

# Thales Luna Network HSM 7

## HSM ADMINISTRATION GUIDE



# Document Information

---

|                     |                               |
|---------------------|-------------------------------|
| <b>Last Updated</b> | 2024-07-10 13:46:27 GMT-04:00 |
|---------------------|-------------------------------|

## **Trademarks, Copyrights, and Third-Party Software**

Copyright 2001-2024 Thales Group. All rights reserved. Thales and the Thales logo are trademarks and service marks of Thales and/or its subsidiaries and are registered in certain countries. All other trademarks and service marks, whether registered or not in specific countries, are the property of their respective owners.

## **Disclaimer**

All information herein is either public information or is the property of and owned solely by Thales Group and/or its subsidiaries who shall have and keep the sole right to file patent applications or any other kind of intellectual property protection in connection with such information.

Nothing herein shall be construed as implying or granting to you any rights, by license, grant or otherwise, under any intellectual and/or industrial property rights of or concerning any of Thales Group's information.

This document can be used for informational, non-commercial, internal, and personal use only provided that:

- > The copyright notice, the confidentiality and proprietary legend and this full warning notice appear in all copies.
- > This document shall not be posted on any publicly accessible network computer or broadcast in any media, and no modification of any part of this document shall be made.

Use for any other purpose is expressly prohibited and may result in severe civil and criminal liabilities.

The information contained in this document is provided "AS IS" without any warranty of any kind. Unless otherwise expressly agreed in writing, Thales Group makes no warranty as to the value or accuracy of information contained herein.

The document could include technical inaccuracies or typographical errors. Changes are periodically added to the information herein. Furthermore, Thales Group reserves the right to make any change or improvement in the specifications data, information, and the like described herein, at any time.

Thales Group hereby disclaims all warranties and conditions with regard to the information contained herein, including all implied warranties of merchantability, fitness for a particular purpose, title and non-infringement. In no event shall Thales Group be liable, whether in contract, tort or otherwise, for any indirect, special or consequential damages or any damages whatsoever including but not limited to damages resulting from loss of use, data, profits, revenues, or customers, arising out of or in connection with the use or performance of information contained in this document.

Thales Group does not and shall not warrant that this product will be resistant to all possible attacks and shall not incur, and disclaims, any liability in this respect. Even if each product is compliant with current security standards in force on the date of their design, security mechanisms' resistance necessarily evolves according to the state of the art in security and notably under the emergence of new attacks. Under no circumstances, shall Thales Group be held liable for any third party actions and in particular in case of any successful attack against systems or equipment incorporating Thales products. Thales Group disclaims any liability with respect to security for direct, indirect, incidental or consequential damages that result from any use of its products. It is further stressed

that independent testing and verification by the person using the product is particularly encouraged, especially in any application in which defective, incorrect or insecure functioning could result in damage to persons or property, denial of service, or loss of privacy.

All intellectual property is protected by copyright. All trademarks and product names used or referred to are the copyright of their respective owners. No part of this document may be reproduced, stored in a retrieval system or transmitted in any form or by any means, electronic, mechanical, chemical, photocopy, recording or otherwise without the prior written permission of Thales Group.

## **Regulatory Compliance**

This product complies with the following regulatory regulations. To ensure compliancy, ensure that you install the products as specified in the installation instructions and use only Thales-supplied or approved accessories.

### **USA, FCC**

This equipment has been tested and found to comply with the limits for a “Class B” digital device, pursuant to part 15 of the FCC rules.

### **Canada**

This class B digital apparatus meets all requirements of the Canadian interference-causing equipment regulations.

### **Europe**

This product is in conformity with the protection requirements of EC Council Directive 2014/30/EU. This product satisfies the CLASS B limits of EN55032.

# CONTENTS

|   |    |
|---|----|
| Preface: About the HSM Administration Guide .....   | 10 |
| Customer Release Notes .....  | 10 |
| Audience .....  | 10 |
| Document Conventions .....  | 11 |
| Support Contacts .....  | 13 |
| Chapter 1: Secure Transport Mode .....  | 14 |
| When STM is enabled on the HSM .....  | 14 |
| Recovering an HSM From Secure Transport Mode .....  | 15 |
| Placing an HSM In Secure Transport Mode .....   | 16 |
| Chapter 2: Multifactor Quorum Authentication .....  | 18 |
| Multifactor Quorum Authentication Architecture .....  | 19 |
| Comparing Password and Multifactor Quorum Authentication .....  | 19 |
| PED keys .....  | 20 |
| PED key Types and Roles .....   | 20 |
| Shared PED key Secrets .....  | 22 |
| PINs .....  | 23 |
| Quorum Split Secrets (M of N) .....   | 23 |
| Updated Luna PED Behavior Notes .....   | 25 |
| New-series Luna PED Behavior Notes .....  | 25 |
| Updating or Rolling Back Multifactor Quorum-Authenticated HSM Firmware .....                            | 26 |
| Luna PED Received Items .....   | 26 |
| Other Required Multifactor Quorum-Authentication Items .....  | 28 |
| Luna PED Hardware Functions .....   | 28 |
| Physical Features .....   | 29 |
| Keypad Functions .....  | 30 |
| Modes of Operation .....  | 30 |
| Luna PED with Newer CPU (External Power Supply Now Optional) .....                                      | 31 |
| Local PED Setup .....   | 32 |
| Setting Up a Local PED Connection .....   | 32 |
| PED Actions .....   | 33 |
| Secure Local PED .....  | 33 |
| Secure Communication Between the Local PED and Luna Network HSM 7s With Firmware 7.7.0 and Newer .....  | 34 |
| About Remote PED .....  | 34 |
| Remote PED Architecture .....   | 34 |
| Remote PED Connections .....  | 36 |
| Secure Communication Between the Remote PED and Luna Network HSM 7s With Firmware 7.7.0 and Newer ..... | 38 |

|   |    |
|---|----|
| Secure Communication Between the Remote PED and Luna Network HSM 7s With Firmware 7.4.2 and Older ..... | 38 |
| PEDServer Configuration File .....  | 39 |
| Initializing the Remote PED Vector and Creating an Orange Remote PED key .....                          | 40 |
| Installing PEDserver and Setting Up the Remote Luna PED .....   | 43 |
| Opening a Remote PED Connection .....   | 44 |
| HSM-Initiated Remote PED .....  | 45 |
| To launch PEDserver .....   | 45 |
| To open a Remote PED connection from the Luna Network HSM 7 appliance .....                             | 46 |
| To open a Remote PED connection from a client workstation .....   | 48 |
| PED-Initiated Remote PED .....  | 49 |
| To open a PED-initiated Remote PED connection .....   | 49 |
| PED-initiated Remote PED for Client (lunacm) .....  | 51 |
| Ending or Switching the Remote PED Connection .....   | 53 |
| Configuring PED Timeout Settings .....  | 54 |
| Configuring PED Inactivity Timeout .....  | 54 |
| Configuring PED key Interaction Timeout .....   | 55 |
| Configuring Luna PED Operation Timeout .....  | 55 |
| Remote PED Troubleshooting .....  | 55 |
| Updating External Supply-Powered Luna PED Firmware .....  | 60 |
| Files Included in the Upgrade Package .....   | 60 |
| Preparing for the Update .....  | 60 |
| Updating the Luna PED Firmware .....  | 61 |
| Troubleshooting .....   | 63 |
| Updating USB-Powered Luna PED Firmware .....  | 64 |
| Preparing for the Upgrade .....   | 64 |
| Upgrading the Luna PED Firmware to Version 2.9.0 (or newer) .....                                       | 65 |
| Multifactor Quorum PED key Management .....   | 66 |
| Creating PED keys .....   | 66 |
| Performing Multifactor Quorum Authentication .....  | 72 |
| Consequences of Losing PED keys .....   | 74 |
| Blue HSM SO PED key .....   | 74 |
| Red HSM Domain PED key .....  | 75 |
| Orange Remote PED Vector PED key .....  | 75 |
| Blue Partition SO PED key .....   | 75 |
| Red Partition Domain PED key .....  | 75 |
| Black Crypto Officer PED key .....  | 75 |
| Gray Crypto User PED key .....  | 76 |
| White Audit User PED key .....  | 76 |
| Identifying the PED key Secret .....  | 76 |
| Duplicating Existing PED keys .....   | 77 |
| Changing the PED key Secret .....   | 78 |
| Blue HSM SO PED key .....   | 78 |
| Red HSM Domain PED key .....  | 79 |
| Orange Remote PED Vector PED key .....  | 79 |
| Blue Partition SO PED key .....   | 79 |
| Red Partition Domain PED key .....  | 79 |

|   |     |
|---|-----|
| Black Crypto Officer PED key .....  | 80  |
| Gray Crypto User PED key .....  | 80  |
| White Audit User PED key .....  | 81  |
| PEDserver and PEDclient .....   | 81  |
| The PEDserver Utility .....   | 81  |
| The PEDclient Utility .....   | 82  |
| pedserver .....   | 83  |
| pedserver -appliance .....  | 84  |
| pedserver -appliance delete .....   | 85  |
| pedserver -appliance list .....   | 86  |
| pedserver -appliance register .....   | 87  |
| pedserver mode .....  | 88  |
| pedserver -mode config .....  | 89  |
| pedserver -mode connect .....   | 91  |
| pedserver -mode disconnect .....  | 92  |
| pedserver -mode show .....  | 93  |
| pedserver -mode start .....   | 95  |
| pedserver -mode stop .....  | 97  |
| pedserver -regen .....  | 98  |
| pedclient .....   | 98  |
| pedclient -mode assignid .....  | 100 |
| pedclient -mode config .....  | 101 |
| pedclient -mode deleteid .....  | 103 |
| pedclient -mode releaseid .....   | 104 |
| pedclient -mode setid .....   | 105 |
| pedclient -mode show .....  | 106 |
| pedclient -mode start .....   | 107 |
| pedclient -mode stop .....  | 109 |
| pedclient -mode testid .....  | 110 |
| <br>  |     |
| Chapter 3: Audit Logging .....  | 111 |
| Audit Logging Features .....  | 111 |
| Audit limitations and Controlled tamper recovery state .....                              | 116 |
| The Audit Role .....  | 116 |
| Audit Log Secret .....  | 117 |
| Audit Log Records .....   | 118 |
| Audit Log Message Format .....  | 119 |
| Timestamping .....  | 120 |
| Log Capacity .....  | 121 |
| NTLS is stopped but log still records LUNA_OPEN_SESSION/LUNA_CLOSE_SESSION messages ..... | 121 |
| Audit Logging General Advice and Recommendations .....                                    | 121 |
| Logging In as Auditor .....   | 124 |
| Configuring and Using Audit Logging .....   | 125 |
| Configuring Audit Logging .....   | 125 |
| Copying Log Files Off the Appliance .....   | 128 |
| Exporting the Audit Logging Secret and Importing to a Verifying HSM .....                 | 129 |
| Audit Role Authentication Considerations .....  | 130 |

|   |     |
|---|-----|
| Remote Audit Logging .....  | 130 |
| Mutual authentication with CA signed certificates .....                     | 131 |
| Example of remote audit logging to same host as syslog (7.8.5 onward) ..... | 133 |
| Changing the Auditor Credentials .....                                      | 139 |
| Audit Log Categories and HSM Events .....                                   | 140 |
| Partition Role IDs .....  | 140 |
| HSM Access .....  | 141 |
| Log External .....  | 142 |
| HSM Management .....  | 142 |
| Key Management .....  | 144 |
| Key Usage and Key First Usage .....   | 145 |
| Per-Key Authorization .....   | 146 |
| Audit Log Management .....  | 146 |
| Audit Log Troubleshooting .....   | 148 |
| <br>  |     |
| Chapter 4: Initializing the HSM .....                                       | 149 |
| Hard versus soft initialization .....                                       | 149 |
| Initializing a New or Factory-reset HSM .....                               | 149 |
| Re-initializing the HSM .....   | 152 |
| <br>  |     |
| Chapter 5: HSM Roles .....  | 153 |
| Logging In as HSM Security Officer .....                                    | 154 |
| Changing the HSM SO Credential .....  | 154 |
| <br>  |     |
| Chapter 6: HSM Capabilities and Policies .....                              | 156 |
| Setting HSM Policies Manually .....   | 170 |
| Setting HSM Policies Using a Template .....                                 | 171 |
| Creating an HSM Policy Template .....                                       | 171 |
| Editing an HSM Policy Template .....  | 172 |
| Applying an HSM Policy Template .....                                       | 173 |
| <br>  |     |
| Chapter 7: Application Partitions .....                                     | 174 |
| Creating or Deleting an Application Partition .....                         | 174 |
| Customizing Partition Sizes .....   | 175 |
| Prerequisites .....   | 175 |
| Creating a Custom-Sized Partition .....                                     | 176 |
| Re-sizing an Existing Partition .....                                       | 176 |
| Creating Multiple Equal Large Partitions .....                              | 177 |
| <br>  |     |
| Chapter 8: Security in Operation .....                                      | 178 |
| Tamper Events .....   | 178 |
| Recovering from a Tamper Event .....  | 179 |
| Security Effects of Administrative Actions .....                            | 180 |
| Overt Security Actions .....  | 180 |
| Actions with Security- and Content-Affecting Outcomes .....                 | 180 |
| Elsewhere .....   | 184 |

|   |            |
|---|------------|
| <b>Chapter 9: Monitoring the HSM</b>                | <b>185</b> |
| HSM Status Values                                   | 185        |
| System Operational and Error Messages               | 186        |
| Performance Monitoring                              | 189        |
| Partition Utilization Metrics                       | 190        |
| Rules of acquisition                                | 190        |
| Availability of Partition Utilization Metrics       | 191        |
| Cryptographic Module and Token Return Codes         | 192        |
| Library Codes                                       | 210        |
| Vendor-Defined Return Codes                         | 215        |
| HSM Alarm Codes                                     | 220        |
| Alarm Generation and Handling                       | 221        |
| FRAM LOG  | 222        |
| List of HSM Alarm Codes                             | 222        |
| HSM Alarm Code Samples                              | 227        |
| Temperature - High Warning                          | 228        |
| Temperature – High Soft Tamper                      | 228        |
| Temperature – High Hard Tamper                      | 228        |
| Hard Tampers During Storage                         | 229        |
| Decommission with power on                          | 230        |
| Decommission with power off                         | 230        |
| Chassis open with power on                          | 230        |
| Chassis open with power off                         | 231        |
| Card removal  | 231        |
| Stored Data Integrity                               | 231        |
| Appliance reports out-of-service (OOS) code 30      | 232        |
| <br>  |            |
| <b>Chapter 10: HSM Updates and Upgrades</b>         | <b>233</b> |
| Updating the Luna HSM Firmware                      | 233        |
| Rolling Back the Luna HSM Firmware                  | 235        |
| Upgrading HSM Capabilities and Partition Licenses   | 236        |
| Upgrade Options                                     | 236        |
| Purchasing an Upgrade License                       | 238        |
| Entitlement Certificate                             | 238        |
| Activating a License on the Thales Licensing Portal | 240        |
| Managing Your Thales Licensing Portal Account       | 244        |
| View Licenses by Product                            | 244        |
| Activate New Entitlements                           | 245        |
| Products  | 246        |
| Orders  | 247        |
| Activations   | 247        |
| Devices   | 249        |
| Applying an Upgrade License on the HSM              | 250        |
| Upgrade Troubleshooting                             | 251        |
| <br>  |            |
| <b>Chapter 11: Functionality Modules</b>            | <b>252</b> |
| FM Deployment Constraints                           | 252        |



|   |            |
|---|------------|
| FMs and FIPS Mode .....   | 253        |
| FMs and High-Availability (HA) .....  | 253        |
| FMs and Backup/Restore/Cloning .....  | 254        |
| FMs and Secure Trusted Channel (STC) .....                                    | 254        |
| FMs and Appliance Re-imaging .....  | 254        |
| FMs and HSM Firmware Rollback .....   | 255        |
| FM Configuration and Remote PED .....   | 255        |
| FM-Enabled HSM Cannot be Verified With CMU .....                              | 255        |
| Key Attributes .....  | 255        |
| No EDDSA or EC_MONTGOMERY Private Keys with C_CreateObject .....              | 255        |
| FM Sample Applications Dependent on General Cryptoki Samples .....            | 255        |
| Memory for FMs .....  | 256        |
| Preparing the Luna Network HSM 7 to Use FMs .....                             | 256        |
| Step 1: Ensure You Have FM-Ready Hardware .....                               | 256        |
| Step 2: Update Your HSM .....   | 257        |
| Step 3: Purchase and Apply the FM Capability License .....                    | 257        |
| Step 4: Apply HSM Policy Settings .....                                       | 257        |
| Building and Signing an FM .....  | 258        |
| Loading an FM Into the HSM Firmware .....                                     | 262        |
| Deleting an FM From the HSM Firmware .....                                    | 263        |
| Recovering the HSM After FM Failure .....                                     | 264        |
| Effects of Administrative Actions on Functionality Modules .....              | 265        |
| <b>Chapter 12: Zeroizing or Resetting the HSM to Factory Conditions .....</b> | <b>267</b> |
| HSM Zeroization .....   | 267        |
| Resetting the Luna Network HSM 7 to Factory Condition .....                   | 268        |
| Comparing Zeroize, Decommission, Re-image, and Factory Reset .....            | 269        |
| Comparison of Destruction/Denial Actions .....                                | 270        |
| Stored Data Integrity .....   | 272        |

# PREFACE: About the HSM Administration Guide

This document describes the operational and administrative tasks you can perform to maintain the functionality and efficiency of your HSMs. It contains the following chapters:

- > ["Secure Transport Mode" on page 14](#)
- > ["Multifactor Quorum Authentication" on page 18](#)
- > ["Audit Logging" on page 111](#)
- > ["Initializing the HSM" on page 149](#)
- > ["HSM Roles" on page 153](#)
- > ["HSM Capabilities and Policies" on page 156](#)
- > ["Application Partitions" on page 174](#)
- > ["Security in Operation" on page 178](#)
- > ["Monitoring the HSM" on page 185](#)
- > ["HSM Updates and Upgrades" on page 233](#)
- > ["Functionality Modules" on page 252](#)
- > ["Zeroizing or Resetting the HSM to Factory Conditions" on page 267](#)

The preface includes the following information about this document:

- > ["Customer Release Notes" below](#)
- > ["Audience" below](#)
- > ["Document Conventions" on the next page](#)
- > ["Support Contacts" on page 13](#)

For information regarding the document status and revision history, see ["Document Information" on page 2](#).

## Customer Release Notes

---

The Customer Release Notes (CRN) provide important information about specific releases. Read the CRN to fully understand the capabilities, limitations, and known issues for each release. You can view the latest version of the CRN at [www.thalesdocs.com](http://www.thalesdocs.com).

## Audience

---

This document is intended for personnel responsible for maintaining your organization's security infrastructure. This includes Luna HSM users and security officers, key manager administrators, and network administrators.

All products manufactured and distributed by Thales are designed to be installed, operated, and maintained by personnel who have the knowledge, training, and qualifications required to safely perform the tasks assigned to them. The information, processes, and procedures contained in this document are intended for use by trained and qualified personnel only.

It is assumed that the users of this document are proficient with security concepts.

## Document Conventions

---

This document uses standard conventions for describing the user interface and for alerting you to important information.

### Notes

Notes are used to alert you to important or helpful information. They use the following format:

**NOTE** Take note. Contains important or helpful information.

### Cautions

Cautions are used to alert you to important information that may help prevent unexpected results or data loss. They use the following format:

**CAUTION!** Exercise caution. Contains important information that may help prevent unexpected results or data loss.

### Warnings

Warnings are used to alert you to the potential for catastrophic data loss or personal injury. They use the following format:

**\*\*WARNING\*\*** Be extremely careful and obey all safety and security measures. In this situation you might do something that could result in catastrophic data loss or personal injury.

## Command syntax and typeface conventions

| Format                     | Convention   |
|----------------------------|--|
| <b>bold</b>                | <p>The bold attribute is used to indicate the following:</p> <ul style="list-style-type: none"> <li>&gt; Command-line commands and options (Type <b>dir /p</b>.)</li> <li>&gt; Button names (Click <b>Save As</b>.)</li> <li>&gt; Check box and radio button names (Select the <b>Print Duplex</b> check box.)</li> <li>&gt; Dialog box titles (On the <b>Protect Document</b> dialog box, click <b>Yes</b>.)</li> <li>&gt; Field names (<b>User Name</b>: Enter the name of the user.)</li> <li>&gt; Menu names (On the <b>File</b> menu, click <b>Save</b>.) (Click <b>Menu</b> &gt; <b>Go To</b> &gt; <b>Folders</b>.)</li> <li>&gt; User input (In the <b>Date</b> box, type <b>April 1</b>.)</li> </ul> |
| <i>italics</i>             | In type, the italic attribute is used for emphasis or to indicate a related document. (See the <i>Installation Guide</i> for more information.)  |
| <variable>                 | In command descriptions, angle brackets represent variables. You must substitute a value for command line arguments that are enclosed in angle brackets.   |
| [optional]<br>[<optional>] | Represent optional <b>keywords</b> or <variables> in a command line description. Optionally enter the keyword or <variable> that is enclosed in square brackets, if it is necessary or desirable to complete the task.   |
| {a b c}<br>{<a> <b> <c>}   | Represent required alternate <b>keywords</b> or <variables> in a command line description. You must choose one command line argument enclosed within the braces. Choices are separated by vertical (OR) bars.  |
| [a b c]<br>[<a> <b> <c>]   | Represent optional alternate keywords or variables in a command line description. Choose one command line argument enclosed within the braces, if desired. Choices are separated by vertical (OR) bars.  |

## Support Contacts

---

If you encounter a problem while installing, registering, or operating this product, please refer to the documentation before contacting support. If you cannot resolve the issue, contact your supplier or [Thales Customer Support](#). Thales Customer Support operates 24 hours a day, 7 days a week. Your level of access is governed by the support plan negotiated between Thales and your organization. Please consult this plan for details regarding your entitlements, including the hours when telephone support is available to you.

### Customer Support Portal

The Customer Support Portal, at <https://supportportal.thalesgroup.com>, is where you can find solutions for most common problems and create and manage support cases. It offers a comprehensive, fully searchable database of support resources, including software and firmware downloads, release notes listing known problems and workarounds, a knowledge base, FAQs, product documentation, technical notes, and more.

**NOTE** You require an account to access the Customer Support Portal. To create a new account, go to the portal and click on the **REGISTER** link.

### Telephone

The support portal also lists telephone numbers for voice contact ([Contact Us](#)).

# CHAPTER 1: Secure Transport Mode

Luna HSM 7 units are shipped from the factory in Secure Transport Mode (STM). The purpose of STM is to provide a logical check on the HSM firmware and critical security parameters (such as configuration, keys, policies, roles, etc.) so that the authorized recipient can determine if these have been altered while the HSM was in transit.

The Secure Transport Mode capability provides an additional layer of protection beyond the physical security controls provided by tamper-evident shipping bags.

Thales sends customers control validation information in two separate emails prior to shipment:

- > **Physical security control validation** - an email containing the serial number of the HSM and the serial number of the associated tamper evident bag that encloses the HSM.
- > **Logical control validation** - an email containing the serial number of each HSM in the shipment, along with the STM Random User String and the STM Verification String associated with each HSM.

Customers can use the logical and physical HSM controls to verify that HSMs shipped from the factory have not been modified in transit. The Thales shipping procedures are designed to prevent a possible man-in-the-middle attack, as attackers would need unobserved direct access to the HSM while in transit, along with simultaneous possession of both the STM Random User String and the STM Verification String for that HSM.

Thales customers can also implement STM when shipping pre-configured HSMs between their office locations or when pre-configured HSMs are to be put into storage. Customers implementing STM have added protection because only the HSM Security Officer can place an initialized HSM into STM, or recover the HSM from STM, further increasing the difficulty of man-in-the-middle attacks.

**CAUTION!** Do not place the HSM into secure transport mode (STM) when there is already an active tamper. Such action would cause a mismatch of the verification string when the HSM is brought out of transport mode. Use [hsm tamper clear](#) to clear a tamper, if one is present, before proceeding with STM.

## When STM is enabled on the HSM

1. The HSM generates a random string of 16 characters and presents that as the "Random User String" (suitable for copying and pasting into an e-mail).
2. The HSM gathers several sources of internal information reflecting the state of the HSM at that time, including a random nonce value generated for this purpose; the nonce value is not displayed, and never exists outside the HSM. This information applies to the HSM card only; STM does not affect appliance functions.
3. The HSM combines these items (the generated Random User String, the HSM state information, and the random nonce value), and produces the Verification String (suitable for copying and pasting into an e-mail).
4. The HSM then enters Secure Transport Mode, such that only limited operations are allowed until the HSM is brought out of STM.

- The HSM can now be shipped from the factory to customers, or customers can place the HSM into storage or ship securely to another location. The HSM and the STM strings should not come together until they are in the possession of the intended recipient.

### STM verification email

As part of the delivery process for your new HSM, Thales Client Services will send you an email containing two 16-digit strings: a **Random User String** and a **Verification String**. You require these strings to verify that your HSM has not been altered while in transit.

**NOTE** If the STM verification process fails due to a lost or incorrect verification string, customers do have the option of proceeding with the recovery of the HSM from STM mode. If the STM verification process fails due to a tamper, customers can also choose to factory-reset the HSM to bring it back to a Factory state, and then re-initialize.

Refer to the **CAUTION** notes below to avoid inadvertently causing a spurious STM recovery failure that would mask whether a real event had occurred.

For information about the various tamper events, see ["Tamper Events" on page 178](#).

## Recovering an HSM From Secure Transport Mode

Only the HSM SO can recover an initialized HSM that has been placed into STM. When the HSM is zeroized, HSM SO log in is not required.

### New HSMs

New HSMs are shipped from the factory in Secure Transport Mode (STM). You must recover from STM before you can initialize the HSM. As part of the delivery of your new HSM, you should have received an email from Thales Client Services containing two 16-digit strings:

- > Random User String: XXXX-XXXX-XXXX-XXXX
- > Verification String: XXXX-XXXX-XXXX-XXXX

### To recover an HSM from STM

- Ensure that you have the two strings that were presented when the HSM was placed into STM, or that were emailed to you if this is a new HSM.
- If the HSM is initialized, log in as the HSM SO (see ["Logging In as HSM Security Officer" on page 154](#)). If this is a new or zeroized HSM, skip to the next step.

**CAUTION!** Be very careful entering the HSM SO authentication. A single failed attempt increments a counter that results in a change of the generated comparison string, which will cause STM verification to fail during Secure Transport Mode recovery.

- Recover from STM, specifying the random user string that was displayed when the HSM was placed in STM, or that was emailed to you if this is a new HSM:

```
lunash:> hsm stm recover -randomuserstring <XXXX-XXXX-XXXX-XXXX>
```

**NOTE** The random user string is for verification purposes only. If you do not require STM validation, or you wish to bypass the STM validation, you can enter a different string to proceed with the recovery of the HSM from STM mode.

4. You are presented with a verification string. **Visually compare** the string with the original verification string that was sent via e-mail (or other means).

If the string matches the original verification string, the HSM has not been used or otherwise altered since STM was enabled, and can be safely re-deployed.

Enter **proceed** to recover from STM.

### If the verification strings do not match

1. Reconfirm that you have entered the correct random user string for your HSM. Enter **quit** if you want to enter the string again.
2. If the verification strings still do not match:
  - If this is a new HSM, enter **quit** to leave the HSM in Secure Transport Mode, and contact Thales Technical Support.
  - Otherwise, if you feel that the verification failure was benign, enter **proceed** to release the HSM from Secure Transport Mode, and decide to either:
    - proceed with using the HSM
    - perform a factory reset and re-initialize the HSM as a safety precaution before proceeding further.

## Placing an HSM In Secure Transport Mode

Only the HSM SO can place an initialized HSM into STM. When the HSM is zeroized, HSM SO log in is not required.

**CAUTION!** Using [Luna HSM Firmware 7.7.1-20](#) or older, before placing a multifactor quorum-authenticated HSM in Secure Transport Mode, ensure that CO, LCO and CU roles are deactivated, using [role deactivate](#) with each role name. For Luna Network HSM 7s, roles must be deactivated for all partitions, from LunaCM in a connected client. Failure to do so can result in mismatch when the generated strings are later compared during Secure Transport Mode recovery.

Using [Luna HSM Firmware 7.7.2](#) or newer, this is not necessary, because placing the HSM in STM logs out and deactivates those roles, and prevents auto-reactivation. The sessions can be logged in and reactivated manually.

### To place an HSM into Secure Transport Mode

1. Log in as the HSM SO (see ["Logging In as HSM Security Officer" on page 154](#)).
2. Back up the contents of all application partitions.  
See [Partition Backup and Restore](#) for details.
3. Enter the following command to place the HSM into STM:

```
lunash:> hsm stm transport
```



4. After confirming the action, you are presented with:

- **Verification String:** <XXXX-XXXX-XXXX-XXXX>
- **Random User String:** <XXXX-XXXX-XXXX-XXXX>

Record both strings. They are required to verify that the HSM has not been altered while in STM.

**CAUTION!** Transmit the verification string and random user string to the receiver of the HSM using a secure method, distinct from the transport of the physical HSM, so that it is not possible for an attacker to have access to both the HSM and the verification codes while the HSM is in STM.

# CHAPTER 2: Multifactor Quorum Authentication

The Luna PIN Entry Device (Luna PED) provides PIN entry and secret authentication to a Luna HSM that requires trusted-path multifactor quorum authentication. The requirement for multifactor quorum or password authentication is configured at the factory, according to the HSM model you selected at time of purchase.

The Luna PED and PED keys are the only means of accessing the multifactor quorum-authenticated HSM's administrative functions. They prevent key-logging exploits on workstations connected to the host HSM, because authentication is delivered directly from the hand-held Luna PED to the HSM via the independent, trusted-path interface. No password is entered via computer keyboard.

**NOTE** If you are updating or have already updated to [Luna HSM Firmware 7.7.0](#) or newer, refer to [Special Considerations for Luna HSM Firmware 7.7.0 and Newer](#) for more information about multifactor quorum authentication.

Luna Network HSM 7 7.x requires [Luna PED Firmware 2.7.1](#) or newer. This firmware is backward-compatible with Luna Network HSM 7 6.x.

This chapter contains the following sections about multifactor quorum authentication:

- > ["Multifactor Quorum Authentication Architecture" on the next page](#)
  - ["Comparing Password and Multifactor Quorum Authentication" on the next page](#)
- > ["PED keys" on page 20](#)
  - ["PED key Types and Roles" on page 20](#)
  - ["Shared PED key Secrets" on page 22](#)
  - ["Domain PED keys" on page 23](#)
  - ["PINs" on page 23](#)
  - ["Quorum Split Secrets \(M of N\)" on page 23](#)
- > ["Luna PED Received Items" on page 26](#)
- > ["Luna PED Hardware Functions" on page 28](#)
- > ["Updating External Supply-Powered Luna PED Firmware" on page 60](#)
- > ["Local PED Setup" on page 32](#)
- > ["About Remote PED" on page 34](#)
- > ["Multifactor Quorum PED key Management" on page 66](#)
- > ["PEDserver and PEDclient" on page 81](#)

## Multifactor Quorum Authentication Architecture

The multifactor quorum authentication architecture consists of the following components:

- > **Luna PED:** a PIN Entry Device with a local or remote connection to the HSM. The PED reads authentication secrets from PED keys on behalf of an HSM or partition (see ["Luna PED Hardware Functions" on page 28](#)).
- > **Authentication secrets:** Cryptographic secrets generated by the HSM and stored on PED keys. These secrets serve as login credentials for the various roles on the HSM. They can be shared among roles, HSMs, and partitions according to your security scheme.
- > **PED keys:** physical USB-connected devices that contain authentication secrets, created by the HSM (see ["PED keys" on the next page](#)). PED keys have the following custom authentication features:
  - **Shared Secrets:** PED keys of the same type can be reused or shared among HSMs or partitions, allowing domain sharing (necessary for HA and backup configurations), legacy-style Security Officer authentication, and other custom configurations. See ["Shared PED key Secrets" on page 22](#).
  - **PINs:** optional PINs associated with specific PED keys, set by the owner of the PED key at the time of creation. PINs offer an extra layer of security for PED keys which could be lost or stolen. See ["PINs" on page 23](#).
  - **M of N Split Key Scheme:** optional configuration which allows a role to split its authentication secret across multiple PED keys, and require a minimum number of those keys for authentication. This scheme can be customized to be as simple or complex as your organization's security policy dictates. See ["Quorum Split Secrets \(M of N\)" on page 23](#).

## Comparing Password and Multifactor Quorum Authentication

The following table describes key differences between password- and multifactor quorum-authenticated HSMs.

|   | Password authentication  | Multifactor Quorum authentication  |
|---|--|--|
| <b>Ability to restrict access to cryptographic keys</b> | <ul style="list-style-type: none"> <li>&gt; Knowledge of role password is sufficient</li> <li>&gt; For backup/restore, knowledge of partition domain password is sufficient</li> </ul> | <ul style="list-style-type: none"> <li>&gt; Ownership of the black Crypto Officer PED key is mandatory</li> <li>&gt; For backup/restore, ownership of both black CO and red domain PED keys is mandatory</li> <li>&gt; The Crypto User role is available to restrict access to read-only, with no key management authority</li> <li>&gt; Option to associate a PIN with any PED key, imposing a two-factor authentication requirement on any role</li> </ul> |
| <b>Dual Control</b>                                     | <ul style="list-style-type: none"> <li>&gt; Not available</li> </ul>   | <ul style="list-style-type: none"> <li>&gt; Quorum (also called MofN split-knowledge secret sharing) requires "M" different holders of portions of the role secret (a quorum) in order to authenticate to an HSM role - can be applied to any, all, or none of the administrative and management operations required on the HSM</li> </ul>   |

|  | Password authentication   | Multifactor Quorum authentication   |
|--|---------------------------|---|
| <b>Key-custodian responsibility</b>                | > Password knowledge only | > Linked to partition password knowledge<br>> Linked to black PED key(s) ownership and optional PIN knowledge               |
| <b>Two-factor authentication for remote access</b> | > Not available           | > Remote PED and orange (Remote PED Vector) PED key deliver highly secure remote management of HSM, including remote backup |

## PED keys

PED keys are USB authentication devices, embedded in a molded plastic body. Each contains a secret, generated by the HSM, that authenticates a role, cloning domain, or remote PED server. This secret is retained until deliberately changed by an authorized user.



The Luna PED does not hold the authentication secrets. They reside only on the portable PED keys.





PED keys are created when an HSM, partition, role, or Remote PED vector is initialized. Each PED key can contain only one authentication secret at a time, but it can be overwritten with a new authentication secret. See ["Multifactor Quorum PED key Management" on page 66](#).




**CAUTION!** Do not subject PED keys to extremes of temperature, humidity, dust, or vibration. Use the included key cap to protect the USB connector.

## PED key Types and Roles

The Luna PED uses PED keys for all credentials. You can apply the appropriate labels included with your PED keys, according to the table below, as you create them.

The PED key colors correspond with the HSM roles described in ["HSM Roles" on page 153](#). The following table describes the keys associated with the various roles:

| Lifecycle                | PED key  | Authentication Secret                  | Function   |
|--------------------------|--|--|--|
| HSM Administration       | <b>Blue</b>  | HSM Security Officer (HSM SO) secret   | Authenticates the HSM SO role. The HSM SO manages provisioning functions and security policies for the HSM.<br><b>Mandatory</b>  |
|                          | <b>Red</b><br>    | HSM Domain or Key Cloning Vector       | Cryptographically defines the set of HSMs that can participate in cloning for backup. See " <a href="#">Domain PED keys</a> " on page 23.<br><b>Mandatory</b>  |
|                          | <b>Orange</b><br> | Remote PED Vector                      | Establishes a connection to a Remote PED server. See * below table.<br><b>Optional</b>   |
| HSM Auditing             | <b>White</b><br>  | Auditor (AU) secret                    | Authenticates the Auditor role, responsible for audit log management. This role has no access to other HSM services.<br><b>Optional</b>  |
| Partition Administration | <b>Blue</b>  | Partition Security Officer (PO) secret | Authenticates the Partition SO role. The PO manages provisioning activities and security policies for the partition.<br><b>NOTE:</b> If you want the HSM SO to also perform Partition SO duties, you can use the same blue key to initialize both roles.<br><b>Mandatory</b> |
|                          | <b>Red</b><br>  | Partition Domain or Key Cloning Vector | Cryptographically defines the set of partitions that can participate in cloning for backup or high-availability. See " <a href="#">Domain PED keys</a> " on page 23.<br><b>Mandatory</b>   |

| Lifecycle           | PED key   | Authentication Secret                     | Function  |
|---------------------|---|---|---|
| Partition Operation | <b>Black</b><br> | Crypto Officer (CO) secret                | Authenticates the Crypto Officer role. The CO can perform both cryptographic services and key management functions on keys within the partition.<br><b>Mandatory</b>  |
|                     | <b>Gray</b><br>  | Limited Crypto Officer (LCO) secret<br>** | Authenticates the Limited Crypto Officer role. The LCO can perform a subset of the actions available to the Crypto Officer.<br><b>Optional (used in eIDAS-compliant schemes)</b>  |
|                     | <b>Gray</b><br>  | Crypto User (CU) secret                   | Authenticates the Crypto User role. The CU can perform cryptographic services using keys already existing within the partition. It can create and back up public objects only.<br><b>NOTE:</b> If administrative separation is not important, you can use a single black key to initialize the Crypto Officer and Crypto User roles and still have two separate challenge secrets to distinguish read-write and read-only role privileges.<br><b>Optional</b> |

\* Orange PED keys (RPK) for use with [Luna HSM Firmware 7.7.0](#) or newer, with enhanced security to address modern threat environments and to comply with updated standards, have increased infrastructure onboard the key. If such an initialized RPK is overwritten to become a different role PED key (example SO), this process that formerly would take about six seconds now takes about 36 seconds.

\*\* No use-case is anticipated that requires both the LCO and the CU roles at the same time (Crypto User for Luna use-cases and Limited Crypto Officer for eIDAS use-cases), so the gray Crypto User stickers should be adequate to identify either role as you manage and distribute PED keys.

## Shared PED key Secrets

The Luna PED identifies the type of authentication secret on an inserted PED key, and secrets of the same type (color designation) can be used interchangeably. During the key creation process, you have the option of reusing an authentication secret from an existing key rather than have the HSM create a new one. This means that you can use the same PED key(s) to authenticate multiple HSMs or partitions. This is useful for:

- > legacy-style authentication schemes, where the HSM SO also functions as the owner of application partitions. This is achieved by using the same blue PED key to initialize the HSM and some or all of the partitions on the HSM.
- > allowing a single HSM SO to manage multiple HSMs, or a single Partition SO to manage multiple partitions
- > ensuring that HSMs/partitions share a cloning domain (see ["Domain PED keys" on the next page](#))
- > allowing a read-write Crypto Officer role and a read-only Crypto User role to be managed by the same user

It is not necessary for partitions in an HA group to share the same blue Partition SO key. Only the red cloning domain key must be identical between HA group members.

**NOTE** Using a single PED key secret to authenticate multiple roles, HSMs, or partitions is less secure than giving each its own PED key. Refer to your organization's security policy for guidance.

### Domain PED keys

A red domain PED key holds the key-cloning vector (the domain identifier) that allows key cloning between HSMs and partitions, and is therefore the PED key most commonly shared between HSMs or partitions. Cloning is a secure method of copying cryptographic objects between HSMs and partitions, required for backup/restore and within HA groups. It ensures that keys copied between HSMs or partitions are:

- > strongly encrypted
- > copied only between HSMs and partitions that share a cloning domain.

For more information about cloning domains, see [Domain Planning](#).

**NOTE** An HSM or partition can be a member of only one domain, decided at initialization. A domain can only be changed by re-initializing the HSM. Partition domains may not be changed after initialization.

### PINs

The Luna PED allows the holder of a PED key to set a numeric PIN, 4-48 characters long, to be associated with that PED key. This PIN must then be entered on the Luna PED keypad for all future authentication. The PIN provides two-factor authentication and ensures security in case a key is lost or stolen.

PINs can be set only at the time of key creation, and can be changed only by changing the secret on the PED key. Duplicate keys made at the time of creation can have different PINs, allowing multiple people access to the role (see "[Creating PED keys](#)" on page 66). Copies made later are true copies with the same PIN, intended as backups for one person (see "[Duplicating Existing PED keys](#)" on page 77). Duplicates of the PED key all have the same PIN.

If you are using an M of N configuration, each member of the M of N keyset may set a different PIN.

**CAUTION!** Forgetting a PIN is equivalent to losing the key entirely; you can no longer authenticate the role, domain, or RPV. See "[Consequences of Losing PED keys](#)" on page 74.

### Quorum Split Secrets (M of N)

The Luna PED can split an authentication secret among multiple PED key iKeys (up to 16), and require a minimum number of the split keys (a quorum of key-holders) to authenticate the role. This provides a customizable layer of security by requiring multiple trusted people (sometimes called the quorum) to be present for authentication to the role. The key splits are presented to the Luna PED and combined inside the Luna HSM firmware to authenticate the role.

This can be likened to a club, or a board of directors, or a legislature, with some arbitrary number of members. You don't need all members present, to make a decision or perform an action, but you do not want a single person to be able to arbitrarily make decisions or take action affecting everyone. So your security rules set out a number of participants - a quorum - who must be assembled in order to perform certain actions

For example, you could decide (or your security policy could dictate) that at least three trusted people must be present for changes to the HSM policies or for client partition assignments. To accommodate illness, vacations, business travel, or any other reasons that a key-holder might not be present at the HSM site, it is advisable to split the authentication secret among more than three people. If you decide on a five-key split, you would specify M of N for the HSM SO role, or for the cloning domain, or any other role/function, to be 3 of 5. That is, the pool of individual holders of splits of that role secret is five persons, and from among them, a quorum of three must be available to achieve authentication (any three in this 3 of 5 scenario, but cannot be the same key presented more than once during an authentication attempt).

In this example scenario, the HSM SO authentication secret is split among five blue PED key iKeys, and at least three of those keys must be presented to the Luna PED to log in as HSM SO. The PED enforces your quorum rule.

This feature can be used to customize the level of security and oversight for all actions requiring multifactor quorum authentication. You can elect to apply a quorum (M of N split-secret) scheme to all roles and secrets, to some of them, or to none of them. If you do choose to use M of N, you can set different M and N values for each role or secret. Please note the following recommendations:

- > M = N is not recommended; if one of the key holders is unavailable, you cannot authenticate the role.
- > M = 1 is not recommended; it is no more secure than if there were no splits of the secret - a single person can unlock the role without oversight. If you want multiple people to have access to the role, it is simpler to create multiple copies of the PED key.

**NOTE** Using an M of N split secret can greatly increase the number of PED keys you require. Ensure that you have enough blank or rewritable PED keys on hand before you begin backing up your M of N scheme.

More keys means that some actions:

- > initialization
- > organization-mandated "password" change or roll-over

can require longer to complete and might risk Luna PED timeout. In that case, the options are to increase the PED timeout value in the config file, or become very organized and adept at getting all participants to quickly perform their pin-change tasks.

### Activated Partitions and Quorum (M of N)

For security reasons, the HSM and its servers are often kept in a locked facility, and accessed under specific circumstances, directly or by secure remote channel. To accommodate these security requirements, the Crypto Officer and Crypto User roles can be Activated (to use a secondary, alpha-numeric login credential to authenticate - Partition Policy 22), allowing applications to perform cryptographic functions without having to present a black or gray PED key (see [Activation on Multifactor Quorum-Authenticated Partitions](#)). In this case, if the HSM is rebooted for maintenance or loses power due to an outage, the cached authentication secret is erased and the role must be reactivated (by logging in the role via LunaCM and presenting the requisite M



number, or quorum, of PED keys) before normal operations can resume. A further measure called Auto-Activation (Partition Policy 23) can cache the authenticated state as long as two hours, allowing automatic, hands-off resumption of operation.

If Auto-Activation is not allowed, or if it is common for your devices to experience outages greater than two hours in duration, you can invoke Remote PED operation and perform PED operations from a location that is distant from the HSM, and possibly more convenient for your authentication secret key holders to convene. See ["About Remote PED" on page 34](#).

## Updated Luna PED Behavior Notes

USB-powered and DC-powered Luna PEDs can be updated to [Luna PED Firmware 2.9.0](#) and [Luna PED Firmware 2.7.4](#) respectively.

- > Updated Luna PEDs support new communications security protocols for compliance with evolving standards. For more information about these changes, refer to the following sections:
  - ["Secure Communication Between the Local PED and Luna Network HSM 7s With Firmware 7.7.0 and Newer" on page 34](#)
  - ["Secure Communication Between the Remote PED and Luna Network HSM 7s With Firmware 7.7.0 and Newer" on page 38](#)
- > A Luna HSM at [Luna HSM Firmware 7.7.0](#) or newer requires connection with an updated Luna PED.
  - If you are updating to [Luna HSM Firmware 7.7.0](#) or newer, refer to [Special Considerations for Luna HSM Firmware 7.7.0 and Newer](#), [Luna PED Firmware 2.9.0](#), and [Luna PED Firmware 2.7.4](#) *before* proceeding with the update.
  - For more information about PED behavior on Luna HSMs that contain V0 or V1 partitions, refer to [Multifactor Quorum Authentication](#).
- > PEDs with [Luna PED Firmware 2.7.4](#) or [Luna PED Firmware 2.9.0](#) or newer can also function with the following HSMs:
  - HSMs with firmware 5.x and 6.x that will not be updated with the new PED communication protocols.
  - HSMs with firmware 7.x that have yet to be updated for compliance with current eIDAS/Common Criteria and NIST standards.

## New-series Luna PED Behavior Notes

All of the following points apply to the newer-series PED (firmware versions 2.8.0, 2.8.1, or 2.9.0).

- > If a PED is connected via USB to a version 7.x HSM (whether that HSM is installed in a host computer or is embedded in a Luna Network HSM 7 appliance), if the server housing the HSM is booted from a power-off condition, the PED display might come up blank. The PED must be reset.
- > If a new-series PED is powered via USB from a 7.x HSM, and the HSM is reset, the PED will become unresponsive. The PED must be reset.
- > If a PED is connected via USB to a PED server (for Remote PED), if the server is booted from a power-off condition, the PED display might come up blank OR the PED might be unresponsive to the PED server. The PED must be reset.
- > A new-series PED will be unresponsive after a 7.x HSM firmware update or rollback, and/or the display might come up blank. The PED must be reset.

- > In environments where the user is switching RPED connections to the same PED between a Luna Network HSM 7 with [Luna HSM Firmware 7.7.0](#) and one with firmware older than 7.7.0, the following error may occur after receiving a prompt to present the orange PED key:
- PED\_ERROR when running [Luna HSM Client 10.3.0](#) or newer.
  - DEVICE\_ERROR when running [Luna HSM Client 10.2.0](#) or older.

The user may need to clear the RPK from the PED's cache before attempting to switch connection to the non-7.7.0 HSM by pressing the < key, or repeat the command after encountering the error.

References to resetting the PED mean cycling the power. This can be done by disconnecting and reconnecting the USB cable.

A new-series PED, powered by a 7.x HSM over USB retains the AC power socket of the older-series model. If an AC power block is plugged into the power socket of the PED, this will reset the PED.

## Updating or Rolling Back Multifactor Quorum-Authenticated HSM Firmware

After a version 7.x HSM is updated to [Luna HSM Firmware 7.7.0](#) (or newer), or rolled back to an earlier firmware version, a USB-connected PED should be power cycled. Also restart the PED after any appliance reboot. Without this action, attempted operations against the HSM can result in "device error".



## Luna PED Received Items

This chapter describes the items you received with your Luna PED device. For instructions on setting up the PED, see "[Multifactor Quorum Authentication](#)" on page 18.

### Basic Luna PED Order Items

The following items are included with your Luna PED. All are required for a successful installation.

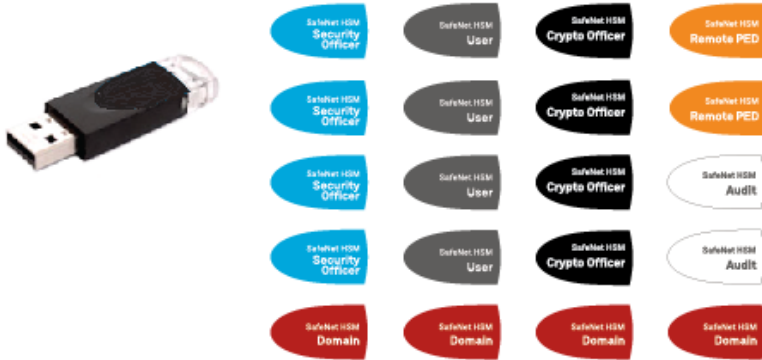
| Qty | Item   |
|-----|--|
| 1   | <b>Luna PED</b> (with <a href="#">Luna PED Firmware 2.7.1</a> or newer)<br> |

| Qty | Item   |
|-----|--|
| 1   | <p data-bbox="248 268 1473 331"><b>Power Supply</b> kit with replaceable mains plug modules for international use (employed when the PED is operated in Remote PED mode)</p> <div data-bbox="292 342 1434 468"><p><b>NOTE</b> If your PED has <a href="#">Luna PED Firmware 2.8.0</a> or newer, it contains refreshed internal hardware and is powered by USB connection. Refreshed PEDs are not shipped with the external power supply, as they do not need it.</p></div>  A photograph showing the components of a power supply kit. It includes a black power adapter with a power cord, a black power cord with a Mini B connector, and several interchangeable mains plug modules in different shapes and colors (black, white, and grey). |
| 1   | <p data-bbox="248 1010 1158 1041"><b>Cable, USB 2.0, Type A to Mini B connectors</b> (for Remote PED operation).</p>  A photograph of a black USB 2.0 cable. One end has a standard Type A USB connector, and the other end has a Mini B connector.   |

| Qty | Item   |
|-----|--|
| 1   | <b>Cable, Data, 9-pin, Micro-D to Micro-D connectors</b> (for local PED operation prior to HSM firmware versions 7.x.).<br> |

## Other Required Multifactor Quorum-Authentication Items

The following required items may be shipped with your Luna PED, or ordered separately.

| Qty | Item   |
|-----|--|
| 1   | <b>Set of PED keys and Labels</b><br><br>Your order may include a set of PED keys and peel-and-stick labels. |

## Luna PED Hardware Functions

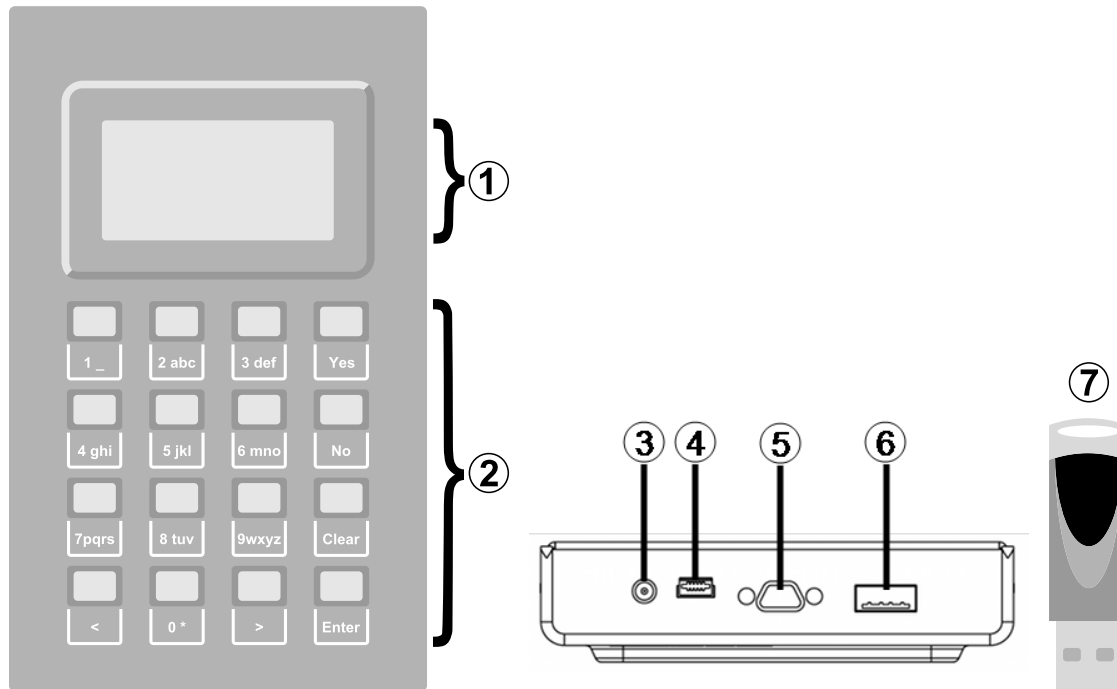
The Luna PED reads authentication secrets from PED keys on behalf of an HSM or partition. This section contains the following information about the Luna PED device:

- > ["Physical Features" on the next page](#)
- > ["Keypad Functions" on page 30](#)
- > ["Modes of Operation" on page 30](#)

- > ["Admin Mode Functions" on page 31](#)
- > ["Luna PED with Newer CPU \(External Power Supply Now Optional\)" on page 31](#)

## Physical Features

The Luna PED is illustrated below, with important features labeled.



|   |   |
|---|---|
| 1 | Liquid Crystal Display (LCD), 8 lines.  |
| 2 | Keypad for command and data entry. See <a href="#">"Keypad Functions" on the next page</a> .  |
| 3 | DC power connector. Not used for PED version 2.8 and above. *   |
| 4 | USB mini-B connector. Used for connecting to the HSM and for file transfer to or from the PED. <a href="#">Luna PED Firmware 2.8.0</a> and above is powered by this USB connection. |
| 5 | Micro-D subminiature (MDSM) connector. Not used for Luna release 7.x.   |
| 6 | USB A-type connector for PED keys.  |
| 7 | PED key. Keys are inserted in the PED key connector (item 6).   |

\* Luna PEDs with [Luna PED Firmware 2.8.0](#) and newer are powered by any USB 2.x or 3.x connection, and do not have an external DC power supply. The PED driver must be installed on the connected computer. If the Luna PED is connected to a hub or to a computer without the driver, then the PED display backlight illuminates, but no PED menu is presented.)

## Keypad Functions

The Luna PED keypad functions are as follows:

| Key                 | Function   |
|---------------------|--|
| <b>Clear</b>        | <ul style="list-style-type: none"> <li>&gt; Clear the current entry, such as when entering a PIN</li> <li>&gt; Hold the key down for five seconds to reset the PED during an operation. This applies only if the PED is engaged in an operation or is prompting for action. There is no effect when no command has been issued or when a menu is open</li> </ul> |
| <b>&lt;</b>         | <ul style="list-style-type: none"> <li>&gt; <b>Backspace:</b> clear the most recent digit you typed on the PED</li> <li>&gt; <b>Exit:</b> return to the previous PED menu</li> </ul>   |
| <b>&gt;</b>         | <ul style="list-style-type: none"> <li>&gt; <b>Log:</b> displays the most recent PED actions (since entering Local or Remote Mode)</li> </ul>  |
| <b>Numeric keys</b> | <ul style="list-style-type: none"> <li>&gt; Select numbered menu items</li> <li>&gt; Input PINs</li> </ul>   |
| <b>Yes and No</b>   | <ul style="list-style-type: none"> <li>&gt; Respond to Yes or No questions from the PED</li> </ul>   |
| <b>Enter</b>        | <ul style="list-style-type: none"> <li>&gt; Confirm an action or entry</li> </ul>  |

## Modes of Operation

The Luna PED can operate in four different modes, depending on the type of HSM connection you want to use:

- > **Local PED-SCP:** This mode is reserved for legacy Luna 6.x HSMs that use an MDSM connector between the PED and the HSM. It does not apply to Luna 7.x. Initial HSM configuration must be done in Local PED mode. See "[Local PED Setup](#)" on [page 32](#) for instructions.
- > **Admin:** This mode is for upgrading the Luna PED device firmware, diagnostic tests, and PED key duplication. See "[Admin Mode Functions](#)" on the [next page](#) for the functions available in this mode.
- > **Remote PED:** In this mode, the PED is connected to a remote workstation and authenticated to the HSM with an orange PED key containing a Remote PED Vector (RPV) secret. This mode allows the Luna Network HSM 7 to be located in a data center or other location restricting physical access. See "[About Remote PED](#)" on [page 34](#) for more information.
- > **Local PED-USB:** In this mode, the PED is connected directly to the HSM card with a USB mini-B to USB-A connector cable. Initial HSM configuration must be done in Local PED mode.

If the Luna PED is connected to an interface when it is powered up, it automatically detects the type of connection being used and switches to the appropriate mode upon receiving the first command from the HSM.

### Changing Modes

If you change your PED configuration without disconnecting the PED from power, you must select the correct mode from the main menu.

## To change the Luna PED's active mode

1. Press the < key to navigate to the main menu.

```
Select Mode
1 Local PED-SCP
4 Admin
7 Remote PED
0 Local PED-USB

PED V.2.7.1-5
```

The main menu displays all the available modes, as well as the PED's current firmware version.

2. Press the corresponding number on the keypad for the desired mode.

**NOTE** The Luna PED must be in **Local PED-USB** mode when connected to a Luna Network HSM 7 7 card, or LunaSH/LunaCM will return an error (CKR\_DEVICE\_ERROR) when you attempt authentication.

### Admin Mode Functions

In this mode, you can upgrade the Luna PED device software, run diagnostic tests, and duplicate PED keys without having the Luna PED connected to an HSM. Press the corresponding number key to select the desired function.

```
Admin mode...
1 PED Key
5 Backup Devices
7 Software Update
9 Self Test

< EXIT
```

- > **PED Key:** allows you to identify the secret on an inserted PED key, or duplicate the key, without having the Luna PED connected to an HSM.
- > **Backup Devices:** Not applicable to Luna 7.x.
- > **Software Update:** requires a PED software file and instructions sent from Thales.
- > **Self Test:** test the PED's functionality. Follow the on-screen instructions to test button functions, display, cable connections, and the ability to read PED keys. The PED returns a PASS/FAIL report once it concludes the test.

## Luna PED with Newer CPU (External Power Supply Now Optional)

A refresh of PED hardware (December 2017) was made necessary by suppliers discontinuing some original components. One of the replaced parts was the CPU, which necessitated a new line of PED firmware, incompatible with the previous versions.

The older PED was shipped with an AC adapter.

The newer PED has the same socket, for connection to an AC adapter, but an adapter/power-block is not shipped with the PED. You can purchase one locally if desired, but the new-CPU PED is reliably powered via USB.

The following points apply to the new-CPU PED - versions 2.8, 2.8.1, 2.9.0 - (that is, any released new CPU PED firmware version)

- > when connected over USB to a Luna PCIe HSM 7 or Luna Network HSM 7, if the server housing the HSM card is booted from power off - the PED display might come up blank. The PED must be reset. Reset = power cycle
- > when connected via USB to a server (but not directly to the HSM card), if the server is booted from power off - the PED display may come up blank OR unresponsive to PED server; the PED must be reset.
- > when powered by the HSM over USB, if an AC power block is then connected, the PED resets.
- > when powered by an AC power block, and also plugged into the HSM's USB port, then if the AC power block is disconnected, the PED will power off.
- > the new-CPU PED will be unresponsive after HSM firmware update or rollback, and the display might come up blank; the PED must be reset.
- > if the new-CPU PED is powered via the USB connection on the HSM, and the HSM is reset, the PED becomes unresponsive; the PED must be reset.
- > if the new-CPU PED is connected to AC and to the HSM's USB connector, if the server housing the HSM is power cycled (not the PED), the PED will not be unresponsive when the server and the HSM are back online; nevertheless, the PED must be reset.

"The PED must be reset" means that the PED must be power cycled by unplugging/replugging the USB cable, or by removing/reinserting the cord from the AC power block (if it is in use).

## Local PED Setup

---

A Local PED connection is the simplest way to set up the Luna PED. In this configuration, the PED is connected directly to the HSM card. It is best suited for situations where all parties who need to authenticate credentials have convenient physical access to the HSM. When the HSM is stored in a secure data center and accessed remotely, you must use a Remote PED setup.

### Setting Up a Local PED Connection

The Luna Network HSM 7 administrator can use these directions to set up a Local PED connection. You require:

- > Luna PED with [Luna PED Firmware 2.7.1](#) or newer
- > USB mini-B to USB-A connector cable
- > Luna PED DC power supply (if included with your Luna PED)

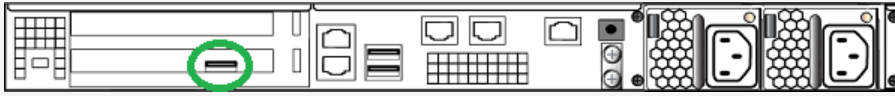
---

#### To set up a Local PED connection

1. Connect the Luna PED to the HSM using the supplied USB mini-B to USB-A connector cable.



**NOTE** To operate in Local PED-USB mode, the Luna PED must be connected directly to the HSM card's USB port, and not one of the other USB connection ports on the appliance.



2. [Luna PED Firmware 2.8.0](#) and newer is powered via the USB connection. If you are using [Luna PED Firmware 2.7.1](#), connect it to power using the Luna PED DC power supply.

As soon as the PED receives power, it performs start-up and self-test routines. It verifies the connection type and automatically switches to the appropriate operation mode when it receives the first command from the HSM.

3. If you prefer to set the operation mode to **Local PED-USB** manually, see ["Changing Modes" on page 30](#).

The Luna PED is now ready to perform authentication for the HSM. You may proceed with setting up or deploying your Luna Network HSM 7. All commands requiring authentication (HSM/partition initialization, login, etc.) will now prompt the user for action on the locally-connected Luna PED.

## PED Actions

There are several things that you can do with the Luna PED at this point:

- > Wait for a PED authentication prompt in response to a LunaSH or LunaCM command (see ["Performing Multifactor Quorum Authentication" on page 72](#))
- > Create copies of your PED keys (see ["Duplicating Existing PED keys" on page 77](#))
- > Change to the Admin Mode to run tests or update PED software (see ["Changing Modes" on page 30](#))
- > Prepare to set up a Remote PED server (see ["About Remote PED" on the next page](#))

## Secure Local PED

PED firmware can be updated to [Luna PED Firmware 2.7.4](#) or newer on a PED with older CPU, and to [Luna PED Firmware 2.9.0](#) or newer on a PED with new CPU.

- > The firmware update is optional for multifactor quorum-authenticated HSMs with firmware versions older than [Luna HSM Firmware 7.7.0](#), and *required* to work with HSMs at [Luna HSM Firmware 7.7.0](#) and newer. This combination complies with an eIDAS-related requirement for an updated secure channel.
- > The updated secure channel for Remote PED operation is now also replicated in the local channel, but because it is local it does not need to be mediated via an orange PED key. The Luna PED, however, sees both local and remote connections as equivalent.

**NOTE** Pressing the "<" key on the Luna PED, to change menus, now warns that the RPV will be invalidated, even though the local connection does not use an orange PED Key. Simply ignore the message.

## Secure Communication Between the Local PED and Luna Network HSM 7s With Firmware 7.7.0 and Newer

Luna HSM Firmware 7.7.0 introduces a level of protection for data that is exchanged between the Local PED (running Luna PED Firmware 2.7.4 or Luna PED Firmware 2.9.0) and Luna Network HSM 7. All exchanged data is protected in the following way:

- > All CSPs exchanged between the Local PED and the Luna Network HSM 7 are protected using an AES-256-KWP CSP wrapping key (CWK).
- > The CWK is established using the One-pass Diffie-Hellman key agreement scheme C(1e, 1s ECDH CDH) with unilateral key confirmation, as defined in *NIST Special Publication 800-56A Revision 3*. The key agreement scheme requires the following:
  - The Luna Network HSM 7 uses a static ECDH key pair. In this case, the HSM generates its own static P-521 ECDH key on startup and the key is assigned a certificate which chains back to the HSM's ECC HOC.
  - The Local PED uses an ephemeral ECDH key pair. In this case, the Local PED generates its ephemeral P-521 ECDH key pair during the key agreement.
- > The SHA-512 based Single-step key derivation function defined in *NIST Special Publication 800-56C Revision 1* is used to derive the CWKs from the shared secret. The derivation function derives separate CWKs for HSM-to-Local PED and Local PED-to-HSM communication.

## About Remote PED

A Remote PED connection allows you to access multifactor quorum-authenticated HSMs that are kept in a secure data center or other remote location where physical access is restricted or inconvenient. This section provides descriptions of the following aspects of Remote PED connections:

- > ["Remote PED Architecture" below](#)
- > ["Remote PED Connections" on page 36](#)
- > ["Secure Communication Between the Remote PED and Luna Network HSM 7s With Firmware 7.7.0 and Newer" on page 38](#)
- > ["Initializing the Remote PED Vector and Creating an Orange Remote PED key" on page 40](#)
- > ["Installing PEDserver and Setting Up the Remote Luna PED" on page 43](#)
- > ["Opening a Remote PED Connection" on page 44](#)
- > ["Ending or Switching the Remote PED Connection" on page 53](#)
- > ["Configuring PED Timeout Settings" on page 54](#)
- > ["Remote PED Troubleshooting" on page 55](#)

## Remote PED Architecture

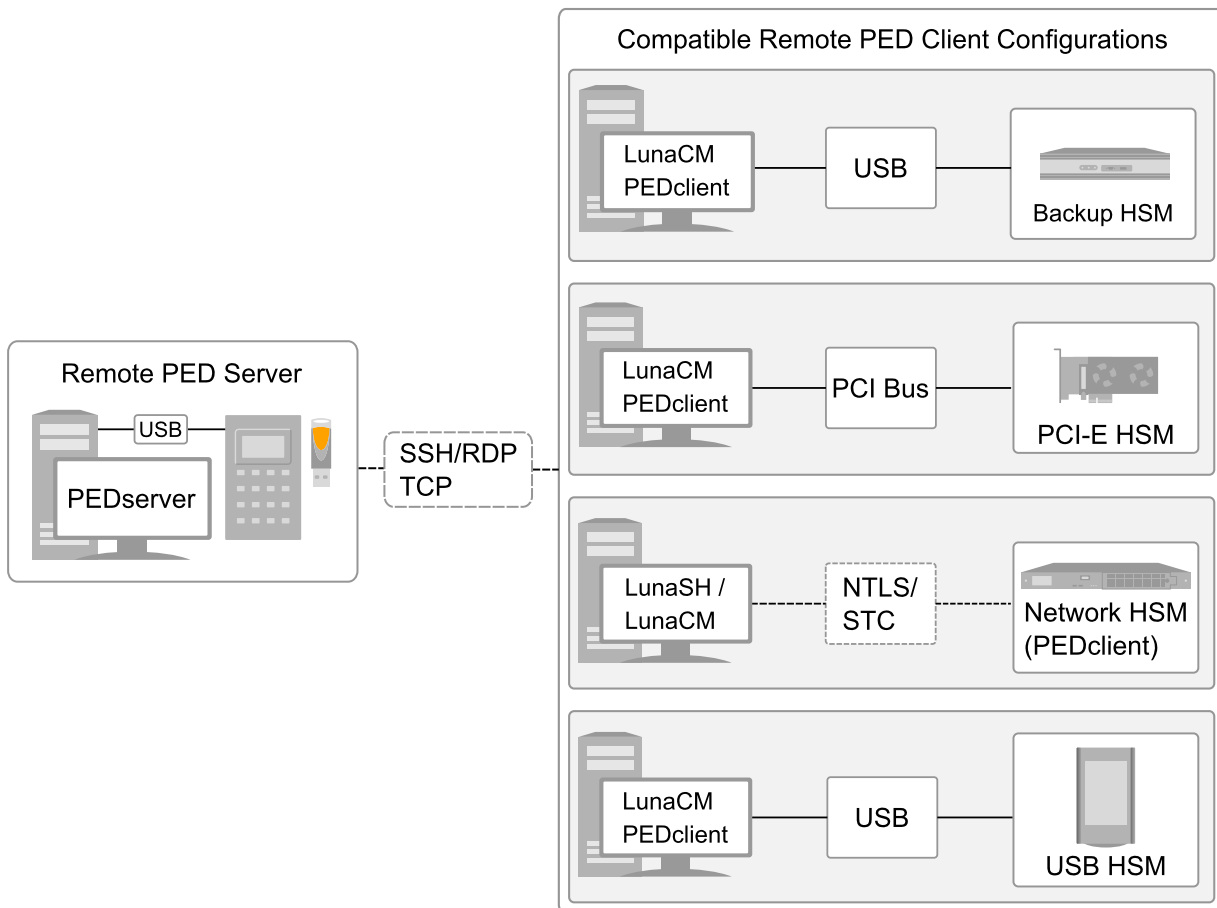
The Remote PED architecture consists of the following components:

- > **Remote PED:** a Luna PED with [Luna PED Firmware 2.7.1](#), connected to a network-connected workstation, powered on, and set to Remote PED mode.

**NOTE** For the enhanced connection security and NIST SP 800-131A Rev.1 compliance implemented with [Luna HSM Firmware 7.7.0](#) and newer, the following Luna PED firmware versions are required:

- > [Luna PED Firmware 2.7.4](#) for PEDs that require the external power block
- > [Luna PED Firmware 2.9.0](#) for USB-powered PEDs

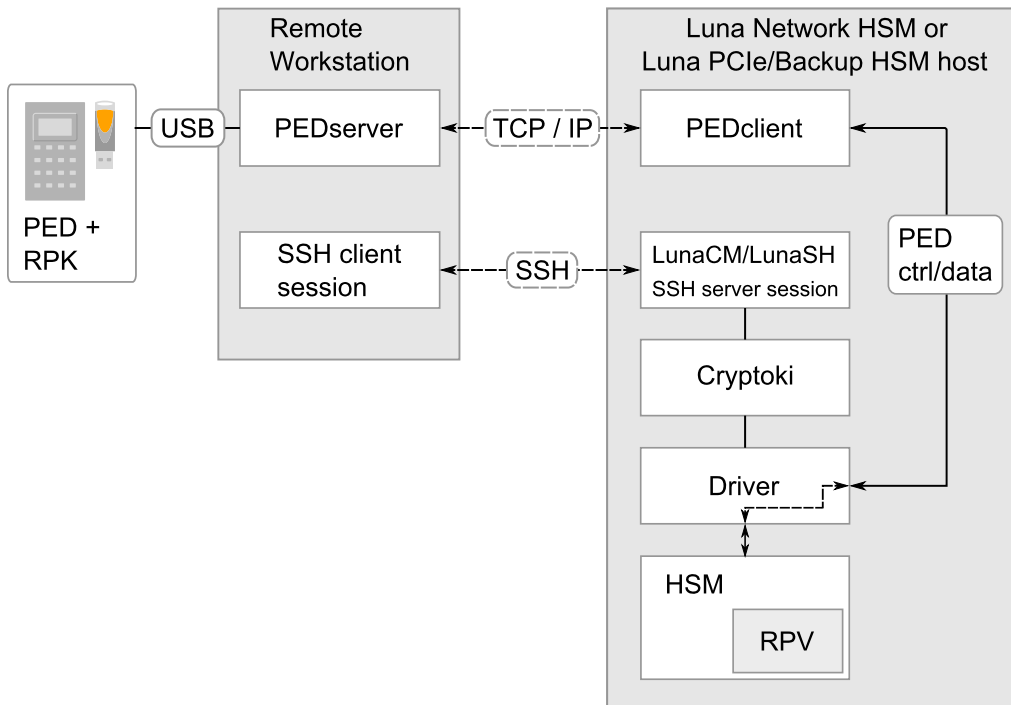
- > **Remote PED Vector (RPV):** a randomly generated, encrypted value used to authenticate between a Remote PED (via PEDserver) and a Luna HSM (via PEDclient).
- > **Remote PED Key (RPK):** an orange PED key containing an RPV (or multiple PED keys with a split RPV in an M of N quorum implementation).
- > **PEDserver:** software that runs on the remote workstation with a USB-connected Luna PED. PEDserver accepts requests from and serves PED actions and data to PEDclient.
- > **PEDclient:** software that requests remote PED services from PEDserver. PEDclient runs on the network-connected system hosting the HSM, which can be one of the following:
  - Host computer with USB-connected Luna Backup HSM, configured for remote backup
  - Host computer with Luna PCIe HSM 7 installed
  - Luna Network HSM 7
  - Host computer with Luna USB HSM 7 connected



## Remote PED Connections

A Luna Network HSM 7 can establish a Remote PED connection with any workstation that meets the following criteria:

- > PEDServer is running
- > a Luna PED with [Luna PED Firmware 2.7.1](#) or newer is connected
- > The orange PED key containing the Remote PED Vector (RPV) for that HSM is available



### Bi-directionality

There are two methods of establishing a Remote PED connection to the HSM:

- > **HSM-initiated:** When the HSM requires authentication, it sends (via PEDclient) a request for PED services to the Remote PED host (which receives the request via PEDserver). This requires that the Luna Network HSM 7 be allowed to initiate external connections, and that the PEDserver IP port remains open. If the Luna Network HSM 7 resides behind a firewall with rules prohibiting these connections, or if your IT policy prohibits opening a port on the Remote PED host, use a PED-initiated connection. See "[HSM-Initiated Remote PED](#)" on page 45.
- > **PED-initiated:** The HSM and Remote PED host exchange and register certificates, creating a trusted connection. This allows the Remote PED host (via PEDserver) to initiate the connection to the Luna Network HSM 7. If you have firewall or other constraints that prevent your HSM from initiating a connection to a Remote PED in the external network, use this connection method. See "[PED-Initiated Remote PED](#)" on page 49.

The following constraints apply to PED-initiated connections:

- > A maximum of 20 Remote PED servers can be registered in PEDclient.
- > A maximum of 80 Luna Network HSM 7 appliances can be registered in PEDserver.

- > If the connection is terminated abnormally (for example, a router switch died), there is no auto-reconnection. PEDserver automatically restarts and runs in HSM-initiated connection mode.
- > When running in PED-initiated connection mode, PEDserver does not listen for new HSM-initiated connections, for security and to simplify usability.

### Priority and Lockout

If a Local PED connection is active and an operation is in progress, a Remote PED connection cannot be initiated until the active Local PED operation is completed. If the Local PED operation takes too long, the Remote PED command may time out.

When a Remote PED connection is active, the Local PED connection is ignored, and all authentication requests are routed to the Remote PED. Attempts to connect to a different Remote PED server are refused until the current connection times out or is deliberately ended. See ["Ending or Switching the Remote PED Connection" on page 53](#).

### One Connection at a Time

Remote PED can provide PED services to only one HSM at a time. To provide PED service to another HSM, you must first end the original Remote PED connection. See ["Ending or Switching the Remote PED Connection" on page 53](#).

### Timeout

Remote PED connections have configurable timeout settings. For more information, refer to ["Configuring PED Timeout Settings" on page 54](#).

Once a partition has been activated and cached the primary authentication (PED key) credential, the Crypto Officer or Crypto User can log in using only the secondary (alphanumeric) credentials and the Remote PED connection can be safely ended until the Partition SO needs to log in again.

### Broken Connections

A Remote PED connection is broken if any of the following events occur:

- > The connection is deliberately ended by the user
- > The connection times out (default: 1800 seconds)
- > Luna PED is physically disconnected from its host
- > VPN or network connection is disrupted
- > You exit Remote PED mode on the Luna PED. If you attempt to change menus, the PED warns:

```
** WARNING **
Exiting now will
invalidate the RPK.
Confirm? YES/NO
```

If the link is broken, as long as the network connection is intact (or is resumed), you can restart PEDserver on the Remote PED host and run **hsm ped connect** in LunaSH or **ped connect** in LunaCM to re-establish the Remote PED link. In a stable network situation, the link will remain available until timeout.

## Secure Communication Between the Remote PED and Luna Network HSM 7s With Firmware 7.7.0 and Newer

Communication between the Remote PED and Luna Network HSM 7 is kept secure before and after RPV initialization.

### Secure Communication Before RPV Initialization

Before the RPV is initialized, data exchanged between the Remote PED and Luna Network HSM 7 is protected using the same method that is used to secure communication between a Local PED and Luna Network HSM 7 (see "[Secure Communication Between the Local PED and Luna Network HSM 7s With Firmware 7.7.0 and Newer](#)" on page 34). However, the SHA-512 based single-step key derivation function defined in *NIST Special Publication 800-56C Revision 1* is used to derive the CWKs from the shared secret, with a password used instead of an RPV.

After the RPV is initialized, the Luna Network HSM 7 and Remote PED re-establish a full secure channel. For more information, see the section below.

### Secure Communication After RPV Initialization

After the RPV is initialized, all communication between the Remote PED and the Luna Network HSM 7 is transmitted within a secure channel that is protected using an AES-256-CTR data encryption key (DEK) and a SHA-512-HMAC data MAC key (DMK). CSPs transmitted within the secure channel are additionally encrypted using an AES-256-KWP CSP wrapping key (CWK). The secure channel is established using the Full Unified C (2e, 2s ECDH CDH) key agreement scheme with bilateral key confirmation, as defined in *NIST Special Publication 800-56A Revision 3*. The key agreement scheme requires each party to use a static ECDH key pair and an ephemeral ECDH key pair. The key pairs are generated in the following ways:

- > The HSM generates its own static P-521 ECDH key on startup. During RPV initialization, the HSM generates a static P-521 ECDH key and loads it onto the RPK along with the RPV (or RPV split is MofN is used). Both static keys are assigned certificates which chains back to the HSM's ECC HOC.
- > During the key agreement, the Luna Network HSM 7 and Remote PED both generate their ephemeral P-521 ECDH key pair.

As part of the key agreement, the SHA-512 based single-step key derivation function defined in *NIST Special Publication 800-56C Revision 1* is used to combine the shared secret, the RPV, and the derived the secure channel protection keys; that is, the DEK, DMK, and CWK. The derivation function derives separate keys (DEK, DMK, and CWK) for HSM-to-Remote PED and Remote PED-to-HSM communication.

The RPV ensures mutual authentication of both end points and the HSM's static ECDH key ensures additional authentication of the HSM.

## Secure Communication Between the Remote PED and Luna Network HSM 7s With Firmware 7.4.2 and Older

All communication between the Remote PED and the HSM is transmitted within an AES-256 encrypted channel, using session keys based on secrets shared out-of-band. This is considered a very secure query/response mechanism. The authentication conversation is between the HSM and the PED. Authentication data retrieved from the PED keys never exists unencrypted outside of the PED or the HSM. PEDclient and PEDserver provide the communication pathway between the PED and the HSM, and the data remains encrypted along that path.

Once the PED and HSM are communicating, they establish a common Data Encryption Key (DEK). DEK establishment is based on the Diffie-Hellman key establishment algorithm and a Remote PED Vector (RPV), shared between the HSM and the PED via the orange Remote PED Key (RPK). Once a common Diffie-Hellman value is established between the parties via the Diffie-Hellman handshake, the RPV is mixed into the value to create a 256-bit AES DEK on each side. If the PED and the HSM do not hold the same RPV, the resulting DEKs are different and communication is blocked.

Mutual authentication is achieved by exchanging random nonces, encrypted using the derived data encryption key. The authentication scheme operates as follows:

| HSM   | –  | Remote PED   |
|---|--|--|
| Send 8 bytes random nonce, R1, encrypted using the derived encryption key.  | $\{R1 \parallel \text{padding}\}_{Ke} \rightarrow$ |  |
|   | $\leftarrow \{R2 \parallel R1\}_{Ke}$              | Decrypt R1. Generate an 8 byte random nonce, R2. Concatenate R2    R1 and encrypt the result using the derived encryption key. |
| Decrypt R2    R1. Verify that received R1 value is the same as the originally generated value. Re-encrypt R2 and return it to Remote PED. | $\{\text{padding} \parallel R2\}_{Ke} \rightarrow$ | Verify that received R2 value is the same as the originally generated value.   |

Following successful authentication, the random nonce values are used to initialize the feedback buffers needed to support AES-OFB mode encryption of the two communications streams (one in each direction).

Sensitive data in transition between a Luna PED and an HSM is end-to-end encrypted: plaintext security-relevant data is never exposed beyond the HSM and the PED boundaries at any time. The sensitive data is also hashed, using a SHA-256 digest, to protect its integrity during transmission.

## PEDServer Configuration File

PED-initiated Remote PED introduces a pedServer.ini/pedServer.conf file. The **Appliances** section manages registered appliances.

**CAUTION!** Do not edit the pedServer.ini/pedServer.conf file. If you have any issues, contact Thales Technical Support.

```
[Appliances]
ServerCAFile=C:\Program Files\SafeNet\LunaClient\cert\PedServerCAFile.pem
SSLConfigFile=C:\Program Files\SafeNet\LunaClient\openssl.cnf
ServerName00=myHSM
ServerIP00=192.20.11.78
ServerPort00=9697
CommonCertName00=66331
[RemotePed]
AdminPort=1502
BGProcessShutdownTimeoutSeconds=25
BGProcessStartupTimeoutSeconds=10
ExternalAdminIF=0
```

```

ExternalServerIF=1
IdleConnectionTimeoutSeconds=1800
InternalShutdownTimeoutSeconds=10
LogFileError=1
LogFileInfo=1
LogFileName=C:\Program Files\SafeNet\LunaClient\remotePedServerLog.log
LogFileTrace=0
LogFileWarning=1
MaxLogFileSize=4194304
PingInterval=1
PongTimeout=5

RpkSerialNumberQueryTimeout=15
ServerPortValue=1503
SocketReadRspTimeoutSeconds=60
SocketReadTimeoutSeconds=60
SocketWriteTimeoutSeconds=15

```

A new entry in the main `Crystoki.ini/Chrystoki.conf` file points to the location of the `pedServer.ini/pedServer.conf` file.

```

[Ped Server]
PedConfigFile = /usr/safenet/lunaclient/data/ped/config

```

## Initializing the Remote PED Vector and Creating an Orange Remote PED key

The Remote PED (via PEDserver) authenticates itself to the Luna Network HSM 7 with a randomly-generated encrypted value stored on an orange PED key. That secret originates in an HSM, and can be carried to other HSMs via the orange key. An newly-configured HSM either:

- > generates its own RPV secret to imprint on an orange PED key,
- > accepts a pre-existing RPV from a previously imprinted orange PED key, at your discretion.

The orange key proves to the HSM that the Remote PED is authorized to provide authentication for HSM roles. A Luna Network HSM 7 administrator can create this key using one of the following two methods:

- > **Local RPV Initialization:** The RPV is initialized using a Luna PED connected to the USB port on the HSM card. This is the standard method of initializing the RPV.  
See "[Local RPV Initialization](#)" below.
- > **Remote RPV Initialization:** The RPV is initialized using a Luna PED connected to a remote workstation running PEDserver. A one-time numeric password is used to authenticate the Remote PED to the HSM before initializing the RPV. This optional method is useful if the HSM SO has only remote SSH access to the appliance. It is available only if the HSM is in a zeroized state (uninitialized) and your firewall settings allow an HSM-initiated Remote PED connection. If you choose this method, you will set up Remote PED before initializing the RPV ("[Remote RPV Initialization](#)" on page 42).

Continue to "[Installing PEDserver and Setting Up the Remote Luna PED](#)" on page 43.

**NOTE** Generally, the HSM SO creates an orange PED key (and backups), makes a copy for each valid Remote PED server, and distributes them to the Remote PED administrators.

### Local RPV Initialization

If the HSM is already initialized, the HSM SO must log in to complete this procedure. You require:

- > Luna PED with [Luna PED Firmware 2.7.1](#) or newer



- > USB mini-B to USB-A connector cable
- > Luna PED DC power supply (if included with your Luna PED)
- > Blank or reusable orange PED key (or multiple keys, if you plan to make extra copies or use an M of N security scheme). See ["Creating PED keys" on page 66](#) for more information.

**NOTE** Orange PED keys (RPK) for use with [Luna HSM Firmware 7.7.0](#) or newer, with enhanced security to address modern threat environments and to comply with updated standards, have increased infrastructure onboard the key. If such an initialized RPK is overwritten to become a different role PED key (example SO), this process that formerly would take about six seconds now takes about 36 seconds.

### To initialize the RPV and create the orange PED key locally

1. If you have not already done so, set up a Local PED connection (see ["Local PED Setup" on page 32](#)).
2. Using a serial or SSH connection, log in to the Luna Network HSM 7 appliance as **admin**.
3. If the HSM is initialized, login as HSM SO (see ["Logging In as HSM Security Officer" on page 154](#)). If not, skip to the next step.  
lunash:> **hsm login**
4. Ensure that you have the orange PED key(s) ready. Initialize the RPV.  
lunash:> **hsm ped vector init**
5. Attend to the Luna PED and respond to the on-screen prompts. See ["Creating PED keys" on page 66](#) for a full description of the key-creation process.

```
SLOT
SETTING RPV...
Would you like to
reuse an existing
keyset?(Y/N)
```

- If you have an orange PED key with an existing RPV that you wish to use for this HSM, press **Yes**.
- If you are creating a new RPV, press **No**.

```
SLOT
SETTING RPV...
Insert a
RPK / Remote
PED Key (ORANGE)
Press ENTER.
```

Continue following the prompts for PIN, M of N, and duplication options.

To continue setting up a Remote PED server, see ["Installing PEDserver and Setting Up the Remote Luna PED" on page 43](#).

## Remote RPV Initialization

When you initialize an RPV with the PED connected locally, you have direct physical control of the operation and its security.

When you initialize an RPV remotely, you must secure the link and the operation with a one-time password. The HSM must be *uninitialized* for this operation.

**NOTE** This feature requires minimum [Luna Network HSM 7 Appliance Software 7.2.0](#) and [Luna HSM Client 7.2.0](#).

Use the following procedure to initialize the RPV. You require:

- > A blank or reusable orange PED key (or multiple keys, if you plan to make extra copies or use an M of N security scheme). See ["Creating PED keys" on page 66](#) for more information.
- > The HSM must be in a zeroized state and the RPV uninitialized.

### To initialize the RPV and create the orange key remotely

1. Open an HSM-initiated Remote PED connection.

```
lunash:> hsm ped connect -ip <PEDserver_IP>
```

The Remote PED connection command prepares to secure the connection and LunaSH does one of the following:

- If you are using [Luna HSM Firmware 7.7.0](#) or newer and [Luna HSM Client 10.3.0](#) or newer, LunaSH presents a randomly-generated 8-digit numeric one-time password that the HSM will use to identify the Remote PED server.

```
Please attend to the PED and enter following password: 18246843
```

```
Command Result : No Error
```

The remote Luna PED prompts you for the one-time password:

```
SLOT
COMPUTE SESSION KEY.

Enter PED Password.

*****
```

- If you are using [Luna HSM Firmware 7.4.2](#) or older and [Luna HSM Client 10.2.0](#) or older, LunaSH returns the following message:

```
Luna PED operation required to connect to Remote PED - use orange PED key(s).
```

```
Enter PED Password:
```

In LunaSH, when prompted to "Enter PED Password" set any 8-digit numeric one-time password that the HSM will use to identify the Remote PED server. The following message is displayed in LunaSH, and the Luna PED prompts you for the password:

```
Luna PED operation required to connect to remote PED - Enter PED password.
```

```
SLOT
COMPUTE SESSION KEY.

Enter PED Password.

*****
```

2. Enter the numeric password on the PIN pad, exactly as you entered it in LunaSH/displayed in LunaSH, and press **Enter**.
3. Ensure that you have the orange PED key(s) ready. Initialize the RPV.

lunash:> **hsm ped vector init**

4. Attend to the Luna PED and respond to the on-screen prompts. See ["Creating PED keys" on page 66](#) for a full description of the key-creation process.

When you have created the orange key, the HSM launches PEDclient and establishes a Remote PED connection using the newly-created RPV.

```
Ped Client Version 2.0.1 (20001)
Ped Client launched in "Release ID" mode.
Callback Server is running..
ReleaseID command passed.
"Release ID" command passed.
Ped Client Version 2.0.1 (20001)
Ped Client launched in "Delete ID" mode.
Callback Server is running..
DeleteID command passed.
"Delete ID" command passed.
```

Command Result : 0 (Success)

You may now initialize the HSM. See ["Initializing the HSM" on page 149](#) for more information.

**NOTE** After creating the orange (Remote PED Vector) key for an HSM using the single-session, one-time password-authenticated PED connection that is used to create the key, the Luna PED prompts for the one-time password when you end the session using **ped disconnect**.

You can ignore the prompt. The PED session is disconnected properly by pressing the Enter key on the Luna PED, without entering the password.

## Installing PEDserver and Setting Up the Remote Luna PED

The PEDserver software, installed on the Remote PED host workstation, allows the USB-connected Luna PED to communicate with remotely-located HSMs. The Remote PED administrator can install PEDserver using the Luna HSM Client installer. You require:

- > Network-connected workstation with compatible operating system (refer to the release notes)
- > Luna HSM Client installer
- > Luna PED with [Luna PED Firmware 2.7.1](#) or newer
- > USB mini-B to USB-A connector cable
- > Luna PED DC power supply if required by your Luna PED hardware

**NOTE** To set up a Remote PED Server on Linux, you require [Luna HSM Client 10.1.0](#) or newer.

## To install PEDserver and the PED driver, and set up the Luna PED

1. Run the Luna HSM Client installer and follow the on-screen instructions, as detailed in [Luna HSM Client Software Installation](#), and select the **Luna Remote PED** option. Any additional installation choices are optional, for the purpose of this procedure.
2. On Windows, if you are prompted to install the driver, accept the installation.
3. On Windows, reboot the computer to ensure that the Luna PED driver is accepted by Windows. This step is not required for Linux or Windows Server operating systems.
4. Connect the Luna PED to a USB port on the host system using the supplied USB mini-B to USB-A connector cable.

Luna PED with [Luna PED Firmware 2.8.0](#) and above is powered via the USB connection. If you are using a Luna PED with [Luna PED Firmware 2.7.1](#), connect it to power using the Luna PED DC power supply.

As soon as the PED receives power, it performs start-up and self-test routines (for PED v2.8 and later, the PED driver must be installed on the connected computer, or the display remains blank). It verifies the connection type and automatically switches to the appropriate operation mode when it receives the first command from the HSM.

To manually set the operation mode to **Remote PED**, see ["Changing Modes" on page 30](#).

5. On Windows, open the Windows **Device Manager** to confirm that the Luna PED is recognized as **PED2**. If it appears as an unrecognized USB device:
  - a. Disconnect the Luna PED from the host USB port.
  - b. Reboot the computer to ensure that the Luna PED driver is accepted by Windows.
  - c. Reconnect the Luna PED.

To continue setting up a Remote PED connection, see ["Opening a Remote PED Connection" below](#).

## Opening a Remote PED Connection

There are two methods of establishing a Remote PED connection to the HSM:

- > **HSM-initiated:** When the HSM requires authentication, it sends (via PEDclient) a request for PED services to the Remote PED host (which receives the request via PEDserver). This requires that the Luna Network HSM 7 be allowed to initiate external connections, and that the PEDserver IP port remains open. If the Luna Network HSM 7 resides behind a firewall with rules prohibiting these connections, or if your IT policy prohibits opening a port on the Remote PED host, use a PED-initiated connection instead.

See ["HSM-Initiated Remote PED" on the next page](#).

- > **PED-initiated:** The HSM and Remote PED host exchange and register certificates, creating a trusted connection. This allows the Remote PED host (via PEDserver) to initiate the connection to the Luna Network HSM 7. If you have firewall or other constraints that prevent your HSM from initiating a connection to a Remote PED in the external network, use this connection method.

See ["PED-Initiated Remote PED" on page 49](#).

**NOTE** For the Luna Network HSM 7, only Luna Shell commands can be used with a *PED-initiated Remote PED connection*. Client-side LunaCM commands such as **partition init** cannot be executed. This means that only administrative personnel, logging in via Luna Shell (lunash:>) can authenticate to the HSM using a PED-initiated Remote PED connection.

To perform actions requiring authentication on Luna Network HSM 7 partitions (that is, from the client side) any Remote PED connection must be launched by the HSM, and the data-center firewall rules must permit such outward initiation of contact.

## HSM-Initiated Remote PED

The HSM/client administrator can use this procedure to establish an HSM-initiated Remote PED connection. The procedure is different depending on whether you are setting up Remote PED for the Luna Network HSM 7 appliance or a client. You require:

- > Administrative access to a network-connected workstation with PEDserver installed and Luna PED connected (see "[Installing PEDserver and Setting Up the Remote Luna PED](#)" on page 43)
- > Administrative access to the Luna Network HSM 7 via SSH (if using Remote PED for HSM-level authentication)
- > Administrative access to a Luna HSM Client workstation with an assigned user partition (if using Remote PED for partition-level authentication)
- > One of the following:
  - Orange PED key with the HSM's RPV (see "[Initializing the Remote PED Vector and Creating an Orange Remote PED key](#)" on page 40)
  - Blank orange PED key (or multiple keys, if you plan to use an M of N scheme)

If you encounter issues, see "[Remote PED Troubleshooting](#)" on page 55.

## To launch PEDserver

1. On Windows, open an Administrator command prompt by right-clicking the Command Prompt icon and selecting **Run as administrator**. This step is not necessary if you are running Windows Server 20xx, as the Administrator prompt is launched by default.

2. Navigate to the Luna HSM Client install directory.

Windows default: **cd C:\Program Files\SafeNet\LunaClient\**

Linux/UNIX default: **cd /usr/safenet/lunaclient**

3. Launch PEDserver. If you are launching PEDserver on an IPv6 network, you must include the **-ip** option.

> "[pedserver -mode start](#)" on page 95 [-ip <PEDserver\_IP>]

```
C:\Program Files\SafeNet\LunaClient>pedserver mode start
Ped Server Version 1.0.6 (10006)
Ped Server launched in startup mode.
Starting background process
Background process started
Ped Server Process created, exiting this process.
```

4. Verify that the service has launched successfully.

> "[pedserver -mode show](#)" on page 93

Note the **Ped2 Connection Status**. If it says **Connected**, PEDserver is able to communicate with the Luna PED.

Note also the server port number (default: **1503**). You must specify this port along with the PEDserver host IP when you open a connection.

```
c:\Program Files\SafeNet\LunaClient>pedserver mode show
Ped Server Version 1.0.6 (10006)
Ped Server launched in status mode.

Server Information:
  Hostname:                DWG9999
  IP:                      0.0.0.0
  Firmware Version:       2.7.1-5
  PedII Protocol Version: 1.0.1-0
  Software Version:       1.0.6 (10006)

  Ped2 Connection Status:  Connected
  Ped2 RPK Count:         0
  Ped2 RPK Serial Numbers (none)

Client Information:       Not Available

Operating Information:
  Server Port:             1503
  External Server Interface: Yes
  Admin Port:             1502
  External Admin Interface: No

  Server Up Time:         190 (secs)
  Server Idle Time:       0 (secs) (0%)
  Idle Timeout Value:    1800 (secs)

  Current Connection Time: 0 (secs)
  Current Connection Idle Time: 0 (secs)
  Current Connection Total Idle Time: 0 (secs) (100%)
  Total Connection Time: 0 (secs)
  Total Connection Idle Time: 0 (secs) (100%)
```

Show command passed.

5. Use **ipconfig** (Windows) or **ifconfig** (Linux) to determine the PEDserver host IP. A static IP is recommended, but if you are connecting over a VPN, you may need to determine the current IP each time you connect to the VPN server.

If you are setting up Remote PED with a Luna Network HSM 7 appliance, see ["To open a Remote PED connection from the Luna Network HSM 7 appliance"](#) below.

If you are setting up Remote PED with a client, see ["To open a Remote PED connection from a client workstation"](#) on page 48.

## To open a Remote PED connection from the Luna Network HSM 7 appliance

1. Open an SSH session to the Luna Network HSM 7 and log in to LunaSH as **admin**.
2. Initiate the Remote PED connection from the Luna Network HSM 7.

```
lunash:> hsm ped connect -ip <PEDserver_IP> -port <PEDserver_port> [-serial <serial#>]
```

**NOTE** The **-serial** option is required only if you are using Remote PED to authenticate a Luna Backup HSM connected to one of the Luna Network HSM 7's USB ports. If a serial number is not specified, the appliance's internal HSM is used.

```
lunash:>hsm ped connect -ip 192.124.106.100 -port 1503
```

Luna PED operation required to connect to Remote PED - use orange PED key(s).

- If you have not yet initialized the RPV, and the HSM is not in initialized state, LunaSH prompts you to enter a password.

```
Enter PED Password:
```

See "[Remote RPV Initialization](#)" on page 42 for this procedure.

- If you already initialized the RPV, the Luna PED prompts for the orange PED key.

```
SLOT
COMPUTE SESSION KEY.
Insert a
RPK / Remote
PED Key (ORANGE)
Press ENTER.
```

Present the orange PED key with the correct RPV. The HSM authenticates the RPV, and control is returned to the LunaSH prompt.

```
Command Result : 0 (Success)
```

The HSM-initiated Remote PED connection is now open.

3. Verify the Remote PED connection by entering a command that requires multifactor quorum authentication.
  - If the HSM is already initialized and you have the blue HSM SO PED key, you can use `lunash:> hsm login`.
  - If the HSM is uninitialized, you can initialize it now with `lunash:> hsm init -label <label>`. Have blank or reusable blue and red PED keys ready (or multiple blue and red keys for M of N or to make multiple copies). See "[Creating PED keys](#)" on page 66 for more information.

**NOTE** The HSM-initiated Remote PED connection eventually times out (default: 1800 seconds), and must be re-initiated each time authentication is required. To simplify this process, you can set a default IP address and/or port for LunaSH to use each time you connect. To drop the Remote PED connection manually, see "[Ending or Switching the Remote PED Connection](#)" on page 53.

4. [OPTIONAL] Set a default IP address and/or port for the Luna Network HSM 7 to look for a configured Remote PED.

```
lunash:> hsm ped set -ip <PEDserver_IP> -port <PEDserver_port>
```

```
lunash:>hsm ped set -ip 192.124.106.100 -port 1503
```

```
Command Result : 0 (Success)
```

With this default address set, the HSM administrator can use `lunash:> hsm ped connect` (without specifying the IP/port) to initiate the Remote PED connection. The orange Luna PED will be required each time.

**NOTE** If you want to use the Remote PED to authenticate a different HSM, you must first drop the current connection. See ["Ending or Switching the Remote PED Connection" on page 53](#).

## To open a Remote PED connection from a client workstation

1. Launch LunaCM on the client.
2. Initiate the Remote PED connection.

```
lunacm:> ped connect -ip <PEDserver_IP> -port <PEDserver_port>
```

```
lunacm:>ped connect -ip 192.124.106.100 -port 1503
```

```
Command Result : No Error
```

3. Issue the first command that requires authentication.

- If the partition is already initialized and you have the blue Partition SO key, log in.

```
lunacm:> role login -name po
```

- If the partition is uninitialized, you can initialize it now. Have blank or reusable blue and red PED keys ready (or multiple blue and red keys for MofN or for multiple copies). See ["Creating PED keys" on page 66](#) for more information on creating PED keys.

```
lunacm:> partition init -label <label>
```

4. The Luna PED prompts for an orange PED key. Present the orange PED key with the correct RPK.

```
SLOT
COMPUTE SESSION KEY.
Insert a
RPK / Remote
PED Key (ORANGE)
Press ENTER.
```

5. The Luna PED prompts for the key associated with the command you issued. Follow the on-screen directions to complete the authentication process.

```
SLOT
SO LOGIN...
Insert a
SO / HSM Admin
PED Key (BLUE)
Press ENTER.
```

**NOTE** The HSM-initiated Remote PED connection eventually times out (default: 1800 seconds), and must be re-initiated each time authentication is required. To simplify this process, you can set a default IP address and/or port for LunaCM to use each time you connect. To drop the Remote PED connection manually, see ["Ending or Switching the Remote PED Connection" on page 53](#).

6. [OPTIONAL] Set a default IP address and/or port for the Luna Network HSM 7 to look for a configured Remote PED.



```
lunacm:> ped set -ip <PEDserver_IP> -port <PEDserver_port>
```

```
lunacm:>ped set -ip 192.124.106.100 -port 1503
```

```
Command Result : 0 (Success)
```

With this default address set, the HSM administrator can use `lunacm:> ped connect` (without specifying the IP/port) to initiate the Remote PED connection. The orange PED key may be required if the RPK has been invalidated on the PED since you last used it.

**NOTE** If you want to use the Remote PED to authenticate a different HSM, you must first drop the current connection. See ["Ending or Switching the Remote PED Connection" on page 53](#).

## PED-Initiated Remote PED

A PED-initiated connection requires the HSM and Remote PED host to exchange and register certificates, creating a trusted connection. This allows the Remote PED host (via PEDserver) to initiate the connection to the Luna Network HSM 7. If you have firewall or other constraints that prevent your HSM from initiating a connection to a Remote PED in the external network, use this connection method. The HSM administrator can use this procedure to set up the connection. You require:

- > Administrative access to a network-connected workstation with PEDserver installed and Luna PED connected (see ["Installing PEDserver and Setting Up the Remote Luna PED" on page 43](#))
- > Orange PED key with the HSM's RPV (see ["Initializing the Remote PED Vector and Creating an Orange Remote PED key" on page 40](#))
- > Administrative access to the Luna Network HSM 7 via SSH

**NOTE** The PED-initiated Remote PED connection procedure requires **admin** access to the appliance via LunaSH, and therefore this method cannot directly provide authentication services for client partitions.

## To open a PED-initiated Remote PED connection

1. On Windows, open an Administrator command prompt on the Remote PED host. (If you are running Windows Server 20xx, the Administrator prompt is launched by default. For any other supported Windows version, right-click the Command Prompt icon and select **Run as administrator**.)
2. Navigate to the Luna HSM Client install directory (**C:\Program Files\SafeNet\LunaClient\** or **/usr/safenet/lunaclient**)
3. You will need the Remote PED host's NTLS certificate. If you have already set up an NTLS client connection to the appliance using LunaCM, you can find the certificate in **C:\Program Files\SafeNet\LunaClient\cert\client\** or **/usr/safenet/lunaclient/cert/client**. If the certificate is not available, you can generate it with the PEDserver utility.

**CAUTION!** If the Remote PED host has registered NTLS partitions on any HSM, regenerating the certificate will cause you to lose contact with your registered NTLS partitions. Use the existing certificate instead.

```
> "pedserver -regen" on page 98 -commonname <name>
```

```
c:\Program Files\SafeNet\LunaClient>pedserver -regen -commonname RemotePED1
Ped Server Version 1.0.6 (10006)
```

```
Are you sure you wish to regenerate the client certificate?
All registered partitions may disappear.
```

```
Are you sure you wish to continue?
```

```
Type 'proceed' to continue, or 'quit' to quit now -> proceed
```

```
Private Key created and written to: C:\Program
Files\SafeNet\LunaClient\cert\client\RemotePED1Key.pem
Certificate created and written to: C:\Program
Files\SafeNet\LunaClient\cert\client\RemotePED1.pem
```

```
Successfully regenerated the client certificate.
```

4. Use **pscp** or **scp** to securely retrieve the Luna Network HSM 7's NTLS certificate. Enter the appliance's admin account password when prompted. Note the period at the end of the command.

```
>pscp admin@<appliance_IP>:server.pem .
```

```
c:\Program Files\SafeNet\LunaClient>pscp admin@192.20.11.78:server.pem .
admin@192.20.11.78's password:
```

```
server.pem | 1 kB | 1.1 kB/s | ETA: 00:00:00 | 100%
```

5. Use **pscp** or **scp** to securely transfer the Remote PED host's NTLS certificate to the Luna Network HSM 7's admin account.

```
>pscp .\cert\client\<certname> admin@<appliance_IP>:
```

```
c:\Program Files\SafeNet\LunaClient>pscp .\cert\client\RemotePED1.pem admin@192.20.11.78:
admin@192.20.11.78's password:
```

```
RemotePED1.pem | 1 kB | 1.1 kB/s | ETA: 00:00:00 | 100%
```

6. Register the Luna Network HSM 7 certificate with PEDserver. Use the mandatory **-name** argument to set a unique name for the appliance. The appliance listens for the SSL connection from PEDserver at the default port **9697**.

```
>"pedserver -appliance register" on page 87 -name <appliance_name> -certificate <cert_filename> -ip
<appliance_IP> -port <port>
```

7. Open an SSH session to the Luna Network HSM 7 and log in to LunaSH as **admin**.

8. Register the PEDserver host certificate.

```
lunash:> hsm ped server register -certificate <certname>
```

```
lunash:>hsm ped server register -certificate RemotePED1.pem
```

```
'hsm ped server register' successful.
```

```
Command Result : 0 (Success)
```

9. Initiate the connection between PEDserver and the Luna Network HSM 7.

```
>"pedserver -mode connect" on page 91 -name <appliance_name>
```

```
c:\Program Files\SafeNet\LunaClient>pedserver mode connect -name myLunaHSM
Ped Server Version 1.0.6 (10006)
```

```
Connecting to myLunaHSM. Please wait..
```

```
Successfully connected to myLunaHSM.
```

10. Using LunaSH, list the available registered Remote PED servers to find the server name (taken from the certificate filename during registration). Select the server you want to use to authenticate credentials for the appliance.

```
lunash:> hsm ped server list
```

```
lunash:> hsm ped select -host <server_name>
```

```
lunash:>hsm ped server list
```

```
Number of Registered PED Server : 1
```

```
    PED Server 1 : CN = RemotePED1
```

```
Command Result : 0 (Success)
```

```
lunash:>hsm ped select -host RemotePED1
```

```
Luna PED operation required to connect to Remote PED - use orange PED key(s).
```

11. The Luna PED prompts for an orange PED key. Present the orange PED key with the correct RPK for the HSM.

```
SLOT
COMPUTE SESSION KEY.
Insert a
RPK / Remote
PED Key (ORANGE)
Press ENTER.
```

The secure network connection is now in place between PEDserver and the appliance. You may now perform any actions that require Remote PED authentication, from lunash. The PED-initiated Remote PED connection does not time out as long as PEDserver is running. If you wish to end the connection in order to connect to a different instance of PEDserver, see ["Ending or Switching the Remote PED Connection" on page 53](#).

## PED-initiated Remote PED for Client (lunacm)

LunaCM, which is a client-side tool, is not able to launch a PED-initiated Remote PED connection if the firewall blocks the initial attempt. LunaCM does not have administrative access to the HSM appliance and is not aware of PED-client settings on the HSM side (such as the port at which the HSM will look for the PED).

If you control two roles, if you are both the HSM SO and the owner/user/PSO of the application partition that is assigned for crypto operations, then you can coordinate actions in Luna Shell (LunaSH command line) and in LunaCM at the client end, to establish a Remote PED connection.

Or, you can do the same if you are the partition owner and are also able to coordinate closely with a person who has administrative access to LunaSH on the HSM appliance.

- > Setup PED-initiated Remote PED connection (refer to the steps above in "[To open a PED-initiated Remote PED connection](#)" on page 49 section).
- > On the Remote PED host, use the lunacm **ped** commands to set the identity of the PedServer to match what you have told the HSM to expect
  - Use **ped set** to provide the IP address and the port number that you determined (or that your colleague determined) in the LunaSH session.

**NOTE** IP address and port number are found in the "Connected PED Server Table:" section of lunash **hsm ped show** command output.

The port number will need to be opened for inbound traffic on the host with that IP address.

- > On the Client (which could also be the Remote PED host, or could be a separate computer/application server), run a command that invokes PED operation, like the **role login** command.
- > The HSM receives the command and looks to the PED (in this case the Remote PED) that has been previously specified in LunaSH.

### Example:

Person with access to **admin** account on the Luna Network HSM 7 verifies that the HSM is expecting a Remote PED connection on a specific port, from a specific IP address -

```
lunash:>hsm ped show
```

<snip>

```
Connected PED Server Table:      PED ID:      4
Server Hostname:                192.168.0.178
Server Port:                    49982
Status:                         Selected
Server Information:
  IP:                            192.168.0.178
  Firmware Version:              2.9.0-2
  PedII Protocol Version:        1.0.1-0
  Software Version:              1.0.6 (10006)
  Ped2 Connection Status:        Connected
  Ped2 Connection Type:          Inbound Connection
  Ped2 RPK Count                 0
  Ped2 RPK Serial Numbers        (none)
```

Show command passed.

```
Command Result : 0 (Success)
```

```
lunash:>
```

If not, see earlier on this page to set up Remote PED.

Person at the PEDserver (which could be the same computer as the partition client, or could be a separate computer, dedicated to being PED server) uses LunaCM to ensure that the PEDserver is using the correct port and IP that the HSM (above) is expecting.

**NOTE** **pedserver\_ip** and **pedserver\_port** below are respectively "IP:" and "Server Port:" fields from the "Connected PED Server Table" section.

```
lunacm:> ped set -ip pedserver_ip -port pedserver_port
lunacm:> ped connect
```

Person who is the PSO of the current slot (which is the desired application partition on the distant Luna Network HSM 7) runs the LunaCM commands that will require the HSM to look for PED interaction.

```
lunacm:> partition init -label 550097_par1 -f
lunacm:> ped connect
lunacm:> role login -n po
lunacm:> ped connect
lunacm:> role init -n co
```

**NOTE** The use of `lunacm:> ped connect` before every partition administrative command is not always necessary, but is a best-practice in unstable network conditions or in situations where network/firewall rules might drop the PEDclient-PEDserver connection frequently or unexpectedly.

If the (re-)connection fails, have the person with "admin" access on the Luna Network HSM 7 re-establish the HSM side of the connection to the PEDserver (expected port and IP) before you issue any more client-side commands that need multifactor quorum authentication.

## Ending or Switching the Remote PED Connection

PEDserver runs on the Remote PED host until explicitly stopped. PEDclient (running on the Luna Network HSM 7) behaves differently depending on the type of Remote PED connection. If you want to connect to a different Remote PED server, or allow another HSM to use the current server, you must manually break the Remote PED connection.

### To end or switch an HSM-initiated Remote PED connection using LunaSH

1. End the Remote PED connection.

```
lunash:> hsm ped disconnect
```

2. You are now able to initiate a connection to a different Remote PED host running PEDserver. You will need to present the orange PED key.

```
lunash:> hsm ped connect -ip <PEDserver_IP> -port <port>
```

**NOTE** Running this command does not change the default Remote PED IP/port you may have previously set. If you want this new Remote PED server to be the default, set it using `lunash:> hsm ped set -ip <PEDserver_IP> -port <port>`.

### To end or switch an HSM-initiated connection using LunaCM

1. End the Remote PED connection.

```
lunacm:> ped disconnect
```

2. You are now able to initiate a connection to a different Remote PED host running PEDserver. You will need to present the orange PED key.

```
lunacm:> ped connect -ip <PEDserver_IP> -port <port>
```

**NOTE** Running this command does not change the default Remote PED IP/port you may have previously set. If you want this new Remote PED server to be the default, set it using `lunacm:> ped set -ip <PEDserver_IP> -port <port>`.

### To end or switch a PED-initiated Remote PED connection

1. End the Remote PED connection with the current host ().  
`lunash:> hsm ped deselect -host <server_name>`
2. Check the available list of Remote PED servers.  
`lunash:> hsm ped server list`  
 If the Remote PED you want to use is not in the list, see ["PED-Initiated Remote PED" on page 49](#).
3. The new Remote PED server must initiate the connection to the appliance.  
 > ["pedserver -mode connect" on page 91](#) -name <appliance\_name>
4. In LunaSH, you are now able to select the new Remote PED server from the available list.  
`lunash:> hsm ped select -host <server_name>`

## Configuring PED Timeout Settings

You can configure the PED timeout settings for your Remote PED connection. This is useful in the following situations:

- > You would like to improve workflows for your HSM roles or enhance the security of your multifactor quorum-authenticated Luna Network HSM 7 deployment by increasing or decreasing the duration of PED inactivity that can elapse until the PED connection breaks.
- > You are using a quorum (M of N split-secret) authentication scheme for your HSM roles and need to increase the time that is available for each required user to present their PED key. For more information about this authentication scheme, refer to ["Quorum Split Secrets \(M of N\)" on page 23](#).
- > You are updating to [Luna HSM Firmware 7.7.0](#) or newer and need to increase the time that is available migrate all your pre-existing orange PED keys. For more information about this migration procedure, refer to [Migrating Existing Orange Remote PED Keys](#).

### Configuring PED Inactivity Timeout

You can increase or decrease the number of seconds of PED inactivity that can elapse before the PED connection breaks. PEDserver and PEDclient both have configurable timeout settings, but the utility that uses the briefer value determines the actual timeout duration.

PED inactivity timeout does not apply to PED-initiated Remote PED connections.

To configure PED inactivity timeout, run `hsm ped timeout set -type rped -seconds <seconds>`.

After configuration, you can verify that the PED inactivity timeout duration has changed by running `hsm ped timeout show`.

## Configuring PED key Interaction Timeout

You can set the amount of time that can elapse without completing PED key requests, before the PED key request ends and must be repeated.

Estimate your actual settings based on the number of keys you are migrating.

To configure PED key interaction timeout, run lunash:> **hsm ped timeout set -type pedk -seconds <seconds>**.

**NOTE** If you decrease the value of **pedk**, the newly set timeout duration only takes effect after running lunash:> **hsm restart**.

After configuration, you can verify that the PED key interaction timeout duration has changed by running **hsm ped timeout show**.

## Configuring Luna PED Operation Timeout

You can set the amount of time that can elapse without completing a Luna PED operation request, before the PED operation ends and must be repeated.

To configure PED key interaction timeout, run lunash:> **hsm ped timeout set -type pedo -seconds <seconds>**.

After configuration, you can verify that the PED key interaction timeout duration has changed by running **hsm ped timeout show**.

## Remote PED Troubleshooting

If you encounter problems at any stage of the Remote PED connection process, the following troubleshooting tips may help resolve the problem:

- > ["Intermittent CKR\\_CALLBACK\\_ERROR: PED Cannot Service its USB Data Channel Fast Enough to Communicate with PEDserver" on the next page](#)
- > ["No Menu Appears on Luna PED Display: Ensure Driver is Properly Installed" on the next page](#)
- > ["RC\\_SOCKET\\_ERROR: PEDserver Requires Administrator Privileges" on the next page](#)
- > ["LUNA\\_RET\\_PED\\_UNPLUGGED: Reconnect HSM-initiated Remote PED Before Issuing Commands" on page 57](#)
- > ["Remote PED Firewall Blocking" on page 57](#)
- > ["Remote PED Blocked Port Access" on page 59](#)
- > ["ped connect Fails if IP is Not Accessible" on page 59](#)
- > ["PEDserver on VPN fails" on page 59](#)
- > ["PED connection Fails with Error: pedClient is not currently running" on page 60](#)

## Intermittent CKR\_CALLBACK\_ERROR: PED Cannot Service its USB Data Channel Fast Enough to Communicate with PEDserver

**NOTE** This issue might occur during Remote PED connections between

- > A Luna Network HSM 7 with [Luna HSM Firmware 7.7.0](#) or newer and a remote workstation with [Luna HSM Client 10.3.0](#) or newer.
- > A Luna Backup HSM 7 with firmware 7.7.1 or newer and a remote workstation with [Luna HSM Client 10.3.0](#) or newer.

The PED might not be able service its USB data channel fast enough to communicate with PEDserver and you will intermittently receive CKR\_CALLBACK\_ERROR.

The following error appears in the PEDserver log file:

```
* ERROR ** 32725 : pedsock_rmtped_write_1_waitack_write_n_waitack failed: 0xffffffff (-1)*
```

If driver log messages are available on your system, the following message may appear where driver logs are reported:

```
kernel: lunaped: read: usb_bulk_msg: rc = -110
```

To avoid this error, throttle communication between the PED and PEDserver by running the following command from a command prompt:

```
pedserver -mode config -set -pedwritelay <int>
```

**NOTE** To resolve this error in most cases, Thales recommends setting the value of **-pedwritelay** to **50**. If you still experience this issue, set **-pedwritelay** to a value higher than **50**. For more information about this option, refer to ["pedserver -mode config" on page 89](#).

## No Menu Appears on Luna PED Display: Ensure Driver is Properly Installed

If the PED driver is not properly installed before connecting the PED to the workstation's USB port, the PED screen does not display the menu. If you encounter this problem, ensure that you have followed the entire procedure at ["Installing PEDserver and Setting Up the Remote Luna PED" on page 43](#).

## RC\_SOCKET\_ERROR: PEDserver Requires Administrator Privileges

If PEDserver is installed in the default Windows directory, it requires Administrator privileges to make changes. If you run PEDserver as an ordinary user, you may receive an error like the following:

```
c:\Program Files\SafeNet\LunaClient>pedserver mode start
Ped Server Version 1.0.6 (10006)
Ped Server launched in startup mode.
Starting background process
Failed to recv query response command: RC_SOCKET_ERROR c0000500
Background process failed to start : 0xc0000500 RC_SOCKET_ERROR
Startup failed. : 0xc0000500 RC_SOCKET_ERROR
```

To avoid this error, when opening a command line for PEDserver operations, right-click the Command Prompt icon and select **Run as Administrator**. Windows Server 20xx opens the Command Prompt as Administrator by default.



**NOTE** If you do not have Administrator permissions on the Remote PED host, contact your IT department or install Luna HSM Client in a non-default directory (outside the **Program Files** directory) that is not subject to permission restrictions.

### **LUNA\_RET\_PED\_UNPLUGGED: Reconnect HSM-initiated Remote PED Before Issuing Commands**

As described in the connection procedures, HSM-initiated Remote PED connections time out after a default period of 1800 seconds (30 minutes). If you attempt authentication via PED after timeout or after the connection has been broken for another reason, the Luna PED will not respond and you will receive an error like this:

```
lunash:>hsm login
```

```
Luna PED operation required to login as HSM Administrator - use Security Officer (blue) PED key.
```

```
Error: 'hsm login' failed. (300142 : LUNA_RET_PED_UNPLUGGED)
```

```
Command Result : 65535 (Luna Shell execution)
```

To avoid this error, re-initiate the connection before issuing any commands requiring authentication via PED:

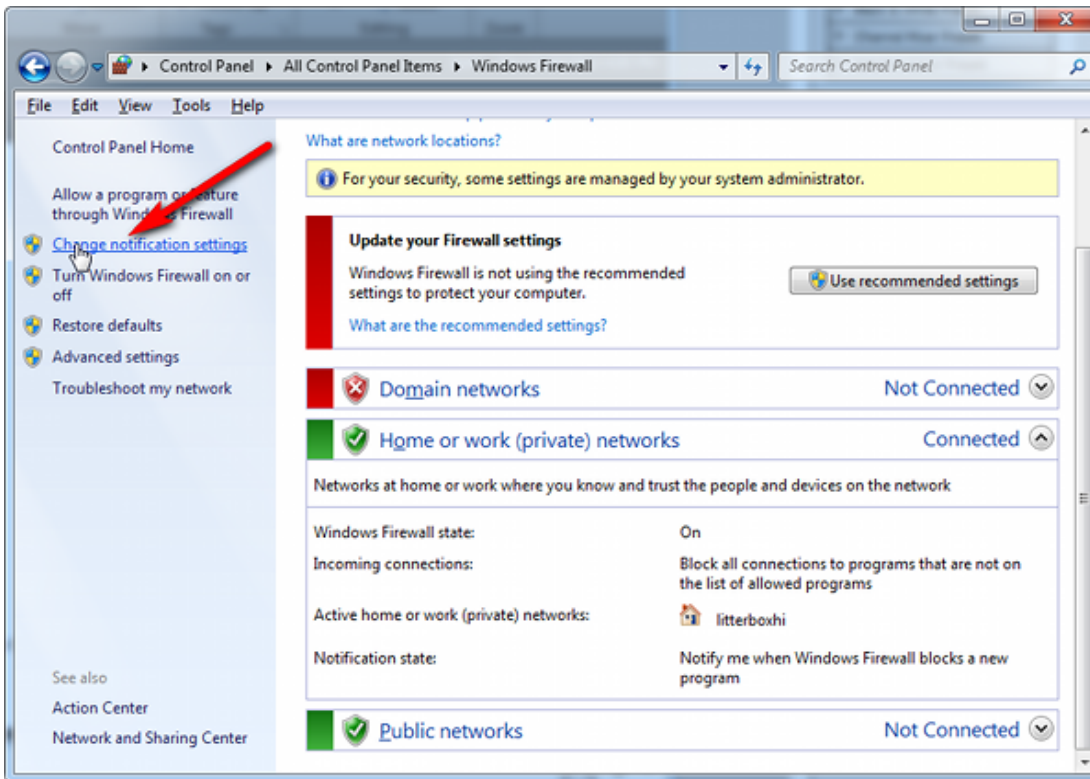
```
lunash:> hsm ped connect -ip <PEDserver_IP> -port <PEDserver_port>
```

```
lunacm:> ped connect -ip <PEDserver_IP> -port <PEDserver_port>
```

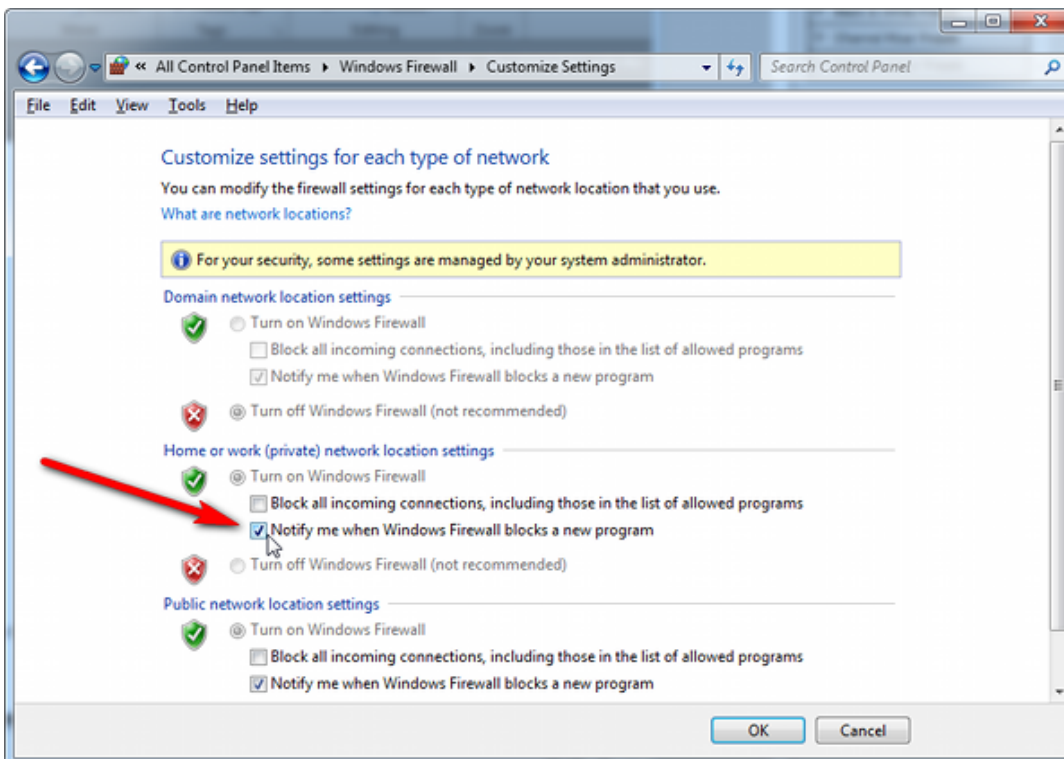
### **Remote PED Firewall Blocking**

If you experience problems while attempting to configure a Luna Remote PED session over VPN, you might need to adjust Windows Firewall settings. If your security policy prohibits changes to Windows Firewall, you can use a PED-initiated connection for HSM SO-level operations. See "[PED-Initiated Remote PED](#)" on page 49.

1. From the Windows Start Menu, select **Control Panel**.
2. Select **Windows Firewall**.
3. Select **Change notification settings**.



4. In the dialog **Customize settings for each type of network**, go to the appropriate section and activate **Notify me when Windows Firewall blocks a new program**.



With notifications turned on, a dialog box appears whenever Windows Firewall blocks a program, allowing you to override the block as Administrator. This allows PEDserver to successfully listen for PEDclient connections.

### Remote PED Blocked Port Access

The network might be configured to block access to certain ports. If ports 1503 (the default PEDserver listening port) and 1502 (the administrative port) are blocked on your network, choose a different port when starting PEDserver, and when using lunacm:> **ped connect** or lunash:> **hsm ped connect** to initiate the Remote PED connection. Contact your network administrator for help.

You might choose to use a port-forwarding jump server, co-located with the Luna Network HSM 7(s) on the datacenter side of the firewall. This can be a low-cost solution for port-blocking issues. It can also be used to implement a PKI authentication layer for Remote PED or other SSH access, by setting up smart-card access control to the jump server.

For example, you can use a standard Ubuntu Server distribution with OpenSSH installed and no other changes made to the standard installation with the following procedure:

1. Connect the Luna PED to a Windows host with Luna HSM Client installed and PEDserver running.
2. Open an Administrator command prompt on the Remote PED host and start the port-forwarding service.

```
>plink -ssh -N -T -R 1600:localhost:1503 <user>@<Ubuntu_server_IP>.
```

3. Login to the appliance as **admin** and open the HSM-initiated connection.

```
lunash:> hsm ped connect -ip <Ubuntu_server_IP> -port 1600
```

The Remote PED host initiates the SSH session, via the Ubuntu jump server, which returns to the Remote PED host running PEDserver.

A variant of this arrangement also routes port 22 through the jump server, which allows administrative access to the Luna Network HSM 7 under the PKI access-control scheme.

### ped connect Fails if IP is Not Accessible

On a system with two network connections, if PEDserver attempts to use an IP address that is not externally accessible, lunacm:>**ped connect** can fail. To resolve this:

1. Ensure that PEDserver is listening on the IP address that is accessible from outside.
2. If not, disable the network connection on which PEDserver is listening.
3. Restart PEDserver and confirm that it is listening on the IP address that is accessible from outside.

### PEDserver on VPN fails

If PEDserver is running on a laptop that changes location, the active network address changes even though the laptop is not shutdown. If you unplugged from working at home, over the corporate VPN, commuted to the office, and reconnected the laptop there, PEDserver is still configured with the address you had while using the VPN. Running **pedserver -mode stop** does not completely clear all settings, so running **pedserver -mode start** again fails with a message like "Startup failed. : 0x0000303 RC\_OPERATION\_TIMED\_OUT". To resolve this problem:

1. Close the current command prompt window.
2. Open a new Administrator command prompt.
3. Verify the current IP address.

```
>ipconfig
```

4. Start PEDserver, specifying the new IP and port number ().
  - > **"pedserver -mode start" on page 95** -ip <new\_IP> -port <port>

### PED connection Fails with Error: pedClient is not currently running

It can happen that the callback server gets shut down, which prevents connections that use it, like Remote PED and remote backup. To resolve this:

1. On the appliance, restart the callback service.
  - lunash:> **service restart cbs**
2. Start the Remote PED connection again (initiated at the PED side or at the HSM side, as appropriate to your network and firewall protocols).

The callback service also restarts when the appliance is rebooted.

## Updating External Supply-Powered Luna PED Firmware

This section describes how to update the firmware on your Luna PED that is powered by a power-block. Refer to [Customer Release Notes](#) for valid update paths.

**NOTE** If your Luna PED is the newer model that is powered by a USB connection (and is not shipped with a power-block), see ["Updating USB-Powered Luna PED Firmware" on page 64](#).

### Files Included in the Upgrade Package

The update package includes the following files. Both files are required to successfully perform the update:

- > Firmware update file for the desired version (<PED\_firmware\_file\_name>.bin, where the version is in the range 2.7.x)
- > if the package contains **LunaPED\_Update.exe** use that; otherwise, download KB0015846 from the Support Portal for a copy of LunaPED\_Update.exe that works with PEDs powered by power block.

### Preparing for the Update

Before you can install the new firmware, you must download the update package to the Windows Luna HSM Client workstation you will use to perform the update, and configure the Luna PED to accept the update.

**CAUTION!** It is strongly recommended that you protect both your computer and Luna PED with an uninterruptible power supply during the upgrade operation. A power failure while any of the file images are being applied to the PED can result in loss of function that might require RMA.

### To prepare your computer for the update

1. Ensure that Luna HSM Client software, including the Remote PED option, is installed on the Windows PC you will use to update the PED. To verify, ensure that the following files/directories are installed:
  - **C:\Program Files\SafeNet\LunaClient\RemotePEDDriver**

- **C:\Program Files\SafeNet\LunaClient\pedserver.exe**
2. The update files are provided in an archive file named for the PED upgrade part number. Extract the files to the Windows Luna HSM Client workstation connected to the Luna PED you are updating.
  3. On your Luna HSM Client workstation, where the PED is physically connected, stop the pedserver and pedclient services before starting the PED update.

**NOTE** If you are updating the PED firmware from version 2.4.x to 2.5.0 or to 2.6.0 on a Windows 10 workstation (recall that the upgrade path is 2.4.0=>2.4.1=>2.5.0=>2.6.0=>2.7.0=>2.7.1=>2.7.4), then use the PEDupdate.exe that is included with the 2.7.x or 2.9.0 PED firmware update and *not* the firmware update package that was included with the Luna Client 6.2.2 package.

4. On your Luna HSM Client workstation, open a command prompt window and move to the directory where you copied the files in the update package.

### To prepare the Luna PED for the firmware update

1. Connect the Luna PED to power (if you have an older PED that is not powered by the USB connection) and connect the USB cable between the Luna PED and your Luna HSM Client workstation.
2. Allow the PED to boot normally until it reaches the default **Local PED mode Awaiting command...**
3. Press the < key to display the **Mode** menu.
4. Verify the currently-installed PED firmware version.

**CAUTION!** If you are updating an older PED (not powered by the USB connection), this procedure requires starting from version **2.6.0-6** or newer. If your PED displays an earlier version, the update will fail and the PED will require RMA. If you have an older version, update the PED to 2.6.0-6 before continuing with this procedure.

5. Select **4** to display the **Admin** menu.
6. Select **7** for **Software Update**.
7. Select **0** to reset the PED and immediately press and hold the < key while the PED is resetting. Continue to hold the < key until the **Select Mode** menu is displayed.
8. Select **USB Mode (4)** when prompted to **Select Mode**. The PED displays **USB Mode**.

## Updating the Luna PED Firmware

During this procedure, each of the **.bin** files is individually uploaded from your computer to the Luna PED, and then saved into permanent memory as the new version of that component. Individual responses are required at the PED to accept and load each file.

**CAUTION!** Complete the following instructions in the order provided, or the PED could be left in an unusable state.

Once you start transferring / uploading a file to the PED, pay attention and promptly respond to the PED messages to acknowledge the upload and then to confirm installation of that new file. The individual PED operations do impose a timeout. However, you can pause before the next file transfer step, as there is no time restriction from one file upload to the next.

### To update the Luna PED firmware

1. In the command prompt window on the Windows Luna HSM Client workstation you prepared to perform the update, execute the following command:

```
> LunaPED_Update.exe <PED_firmware_file_name>.bin
```

**NOTE** If you have both older Luna PEDs (that are powered by a power block), and the newer Luna PEDs (powered by USB connection and addressed in "[Updating USB-Powered Luna PED Firmware](#)" on page 64), then the LunaPED\_Update.exe files for each are different and not interchangeable.

2. On the Luna PED, select **Yes** in response to the prompt: **Software update. Upload Image? YES/NO.**  
Wait approximately six minutes. While transfer is in progress, the command line shows a progress indicator (remaining bytes to transfer), and the PED displays the following message:

```
USB Mode
Software update
Uploading image
```

3. The output of the update command in the Windows command prompt should be similar to the following:

```
LunaPED_Update v2.1.0-1 Nov 25 2013 12:44:48
PED operation is required (to upload image)...
(Sent 3199130 bytes in 327977000 microseconds).
PED operation is required (to save image)...
```

4. If the image has been sent correctly, the PED displays the following message:

```
USB Mode
Software update
** WARNING **
A power failure during save is unsupported!
Save Image? YES/NO
```

Select **Yes** to save the new image.

5. Wait for 20-30 seconds. When the PED displays the following message, press the **Enter** key on the PED keypad to return to USB mode:

```
Software update
Success
Press ENTER
```

6. Unplug all cables from the PED and then reconnect to restart the PED. As the PED starts booting, it should display the following messages:

```
BOOT V.1.0.6-2,
loading PED..
Local PED Mode Awaiting command...
```

7. Press **<** to exit to the **Select Mode** menu. If the update was successful, the new PED version is displayed at the bottom of the PED screen.

8. Your Luna PED is now updated and ready to use. Repeat the procedure for each Luna PED you own.

## Troubleshooting

This section provides guidance for resolving problems you may encounter when updating the PED firmware.

If your update attempt fails with a Receive error (rx error), check if you have Remote PED services running on the computer to which the PED is connected. Issue the command **PedServer -m stop** and restart the update to resolve the problem.

### No Luna PED Prompts

You must attend to the PED when image files are being applied. If no prompts appear on the PED shortly after you issue the **LunaPED\_Update.exe** command, re-check your connections, as follows:

- > The PED power block must be connected to AC power and to the power socket on the PED.
- > A USB connection must exist between a USB port on the sending computer and the USB-mini port on the PED (immediately beside the power socket).
- > The PED must be powered on, and in USB mode.

### Files Uploaded in the Wrong Order

If you attempt to upload the files in the wrong order, the PED performs some verification at the end of a file upload. If the PED displays a message similar to the following, it is a good indication that you uploaded the wrong file first:

```
Failure (VERIFY) (7)
Press Enter
```

You are not given an opportunity to attempt to install/confirm the file if the upload does not verify.

To resolve the issue, restart the process from the beginning of these instructions, ensuring that you follow the sequence in these instructions, taking the upgrade files in the order specified. If that does not correct the problem, contact Technical Support.

### Upgrade Failed Message (or Similar)

If the Luna PED displays an **Upgrade Failed** message, or any message that does not say **Upgrade in Progress** followed by **Upgrade Complete**, before the **Admin** menu appears, stop the upgrade process immediately.

To resolve the issue, you can take the following actions:

- > Reboot the PED by disconnecting and then re-connecting the PED cables. This might clear the problem. If the problem clears, the PED displays a **Nothing to Upgrade** message. In this case, try the update again.
- > If the PED shows **Upgrade in Progress** followed by **Upgrade Failed!** every time you reboot it, contact Customer Support.
- > You can re-upload the file and try again if the upload action failed to complete, or if you failed to acknowledge it on the PED.

## Updating USB-Powered Luna PED Firmware

This section describes how to update the firmware on your Luna PED that is powered by USB connection. Refer to [Customer Release Notes](#) for valid update paths.

To update the Luna PED from [Luna PED Firmware 2.8.0](#) a newer version, follow the steps below.

If your Luna PED is the older type, that was shipped with a power-block, then do not use these instructions; see "[Updating External Supply-Powered Luna PED Firmware](#)" on page 60 instead.

### Preparing for the Upgrade

**CAUTION!** It is strongly recommended that both your computer and Luna PED be protected by an uninterruptible power supply during the upgrade operation. A power failure while any of the file images is being applied to the PED can result in loss of function that might require repair at a Thales facility.

#### Prepare your computer for the upgrade

The needed upgrade files are provided in an archive file named for the PED upgrade part number. At time of writing this instruction, KB0023048 from the Support Portal contained the appropriate firmware and updater files.

1. Extract the files like *ped-2.9.1-0-x-production-itb-real.bin* (or newer if available) and *LunaPED\_Update.exe* contained in the zip file, to the Windows PC that is connected to the Luna PED that you are upgrading.

**NOTE** If you have both older Luna PEDs (that are powered by a power block and addressed on "[Updating External Supply-Powered Luna PED Firmware](#)" on page 60), and the newer Luna PEDs (powered by USB connection and addressed on this page), then the LunaPED\_Update.exe files for each are different and *not interchangeable*.

2. On your Windows PC, open a command prompt window and move to the directory where you copied the files in the upgrade package.

#### Prepare the Luna PED for the firmware upgrade

1. Ensure that the Luna HSM Client, including the Remote PED option, is installed on your Windows PC. To verify, ensure that the following files / directories are installed:
  - C:\Program Files\SafeNet\LunaClient\RemotePEDDriver
  - C:\Program Files\SafeNet\LunaClient\pedserver.exe
2. Connect *the USB data cable between the USB-mini port* on top of the Luna PED and a USB port on your computer.

**NOTE** [Luna PED Firmware 2.8.0](#) and newer is powered by the USB port; a separate power supply to the Luna PED is not provided nor required.

3. Allow the PED to boot normally until it reaches the default "Local PED mode Awaiting command..."
4. Press the < key to display the **Mode** menu.



- Verify the PED version – the bottom line of the PED display should say “PED V.2.8.0”

**CAUTION!** If any other version is shown, stop, acquire a factory shipped Luna PED with [Luna PED Firmware 2.8.0](#), and then return and resume these instructions. If your Luna PED firmware version is older than 2.8.0 (such as 2.6.x) it can only ever be updated to version 2.7.x - see ["Updating External Supply-Powered Luna PED Firmware" on page 60](#) for the relevant update instructions.

- Select **4** to display the **Admin** menu.
- Select **7** for **Software Update**.

## Upgrading the Luna PED Firmware to Version 2.9.0 (or newer)

During this procedure, the .bin file is individually uploaded from your computer to the Luna PED, and then saved into permanent memory as the new version. Individual responses are required at the PED to accept and load the file.

**CAUTION!** Complete the instructions in the order provided, otherwise the Luna PED could be left in an unusable state.

Once you start transferring / uploading a file to the PED, pay attention and promptly respond to the PED messages to acknowledge the upload and then to confirm installation of that new file. *The individual PED operations do impose a timeout.* However, you can pause before the next file transfer step, as there is no time restriction from one file upload to the next.

### Transfer and confirm the Luna PED firmware update

- In a command prompt window, on your Windows PC, from the directory where you copied the files in the upgrade package, execute the following command:  
 Prompt > **LunaPED\_Update.exe ped-2.9.x-y-z-production-itb-real.bin** (where x-y-z are numbers specific to the released build of the firmware)
- At the Luna PED keypad, select **Yes** in response to the prompt.
- The output of the update command in the Windows command prompt should be similar to the following:  

```
LunaPED_Update v3.0.0-1 May 10 2017 22:52:25
PED operation is required (to upload image)...
(Sent xxxxxxxx bytes in xxxxxxxxxxxx microsecs).
PED operation is required (to save image)...
```
- If the image has transferred correctly, Luna PED displays the following message:  

```
USB Mode Software update
** WARNING **
A power failure during save is unsupported!
Save Image? YES/NO"
```
- Select **Yes** to save the new image.
- Wait approximately 20 seconds. The PED displays the following message:

```
USB Mode Software update Success Press ENTER
```

Press the **Enter** key on the PED to continue.

7. Unplug all cables from the PED and then reconnect to restart the PED.
8. As the PED starts booting, it should show "BOOT V.1.1.0-1", then "loading PED...", and then should finish in "Local PED Mode awaiting command..."

If you press "<" to exit to "Select Mode" menu, the bottom of the PED screen should now show "PED V.2.8.1-0" (or "PED V.2.9.0" or a newer version, as one becomes available).

## Done

Luna PED is now updated and ready to use. Repeat the above sequence for each USB-powered Luna PED that you want to upgrade.

## Multifactor Quorum PED key Management

Once you have established a Local or Remote PED connection, you can proceed with initializing roles on the HSM that require multifactor quorum authentication. The procedures in this section will guide you through the Luna PED prompts at each stage of PED key creation, multifactor quorum authentication, and other operations with the Luna PED.

- > ["Creating PED keys" below](#)
  - ["Stage 1: Reusing Existing PED keys" on page 68](#)
  - ["Stage 2: Defining M of N" on page 69](#)
  - ["Stage 3: Setting a PIN" on page 70](#)
  - ["Stage 4: Duplicating New PED keys" on page 71](#)
- > ["Performing Multifactor Quorum Authentication" on page 72](#)
- > ["Consequences of Losing PED keys" on page 74](#)
- > ["Identifying the PED key Secret" on page 76](#)
- > ["Duplicating Existing PED keys" on page 77](#)
- > ["Changing the PED key Secret" on page 78](#)

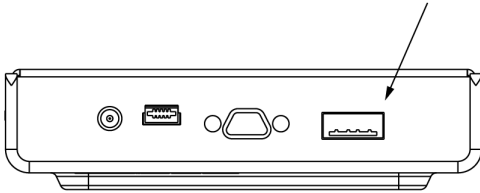
## Creating PED keys

When you initialize an HSM, partition, or role, the Luna PED issues a series of prompts for you to follow to create your PED keys. PED key actions have a timeout setting (default: 200 seconds); ensure that you have everything you need before issuing an initialization command. The requirements for the operation depend on the PED key scheme you have chosen in advance, based on your organization's security policy. Consider these guidelines before you begin:

- > If you are reusing an existing PED key or keyset, the owners of those keys must be present with their keys and PINs ready.
- > If you plan to use an M of N authentication scheme (quorum, or split-secret), all the parties involved must be present and ready to create their authentication split (the initial setup of the quorum and spares). It is advisable for each key holder to create backup duplicates, so you must have a sufficient number of blank or rewritable PED keys ready before you begin.

- > If you plan to make backup duplicates of PED keys, you must have a sufficient number of blank or rewritable PED keys ready.
- > If you plan to use PINs, ensure that they can be privately entered on the Luna PED and memorized, or written down and securely stored.

Whenever the Luna PED prompts you to insert a PED key, use the USB port on the top of the PED:



### To initiate PED key creation

1. Issue one of the following LunaSH or LunaCM commands to initialize the applicable role, domain, or vector.

- **Blue HSM SO and Red HSM Domain PED key:**

```
lunash:> hsm init
```

- **Orange Remote PED Vector PED key:**

```
lunash:> hsm ped vector init
```

- **Blue Partition SO and Red Partition Domain PED keys:**

```
lunacm:> partition init
```

- **Black Crypto Officer PED key:**

```
lunacm:> role init -name co
```

- **Gray Crypto User PED key:**

```
lunacm:> role init -name cu
```

- **White Audit User PED key:**

```
lunash:> audit init
```

The Luna PED responds, displaying:

```
Remote PED mode
Token found
```

**NOTE** The Luna PED screen prompts for a black PED key for any of

- > "User",
- > "Crypto Officer",
- > "Limited Crypto Officer",
- > "Crypto User".

The Luna PED is not aware that the key you present has a black or a gray sticker on it. The colored stickers are visual identifiers for your convenience in keeping track of your PED keys. You differentiate by how you label, and how you use, a given physical key that the Luna PED sees as "black" (once it has been imprinted with a secret).

2. Follow the PED prompts in the following four stages.

### Stage 1: Reusing Existing PED keys

If you want to use a PED key with an existing authentication secret, have the key ready to present to the Luna PED. Reasons for reusing keys may include:

- > You want to use the same blue SO key to authenticate multiple HSMs/partitions
- > You want to initialize a partition in an already-existing cloning domain (to be part of an HA group)

**CAUTION!** The initialization procedure is the only opportunity to set the HSM/partition's cloning domain. It cannot be changed later without reinitializing the HSM, or deleting and recreating the partition. Ensure that you have the correct red key(s) ready.

See ["Shared PED key Secrets" on page 22](#) and ["Domain PED keys" on page 23](#) for more information.

1. The first Luna PED prompt asks if you want to reuse an existing PED key. Press **Yes** or **No** on the keypad to continue.

```
SLOT
SETTING SO PIN...
Would you like to
reuse an existing
keyset? (Y/N)
```

- If you select **No**, skip to ["Stage 2: Defining M of N" on the next page](#).
- If you select **Yes**, the PED prompts you for a key. Insert the key you want to reuse and press **Enter**.

```
SLOT
SETTING SO PIN...
Insert a
SO / HSM Admin
PED Key (BLUE)
Press ENTER.
```

2. If the key has a PIN, the PED prompts you to enter it now. Enter the PIN on the keypad and press **Enter**.

```
SLOT
READING SO PIN...
Enter PED PIN:
*****
```

3. If the key is part of an M of N scheme, the PED prompts you for the next key. You must present enough key splits (M, a.k.a. the quorum) to reconstitute the entire authentication secret.

```
SLOT
READING SO PIN...
Keys read: 01 of 03
Insert another
SO / HSM Admin
PED Key (BLUE)
Press ENTER.
```

4. The PED asks if you want to create a duplicate set of keys. If you are duplicating an M of N keyset, you need a number of blank or rewritable keys equal to N.

```
SLOT
READING SO PIN...
Are you duplicating
this keyset?(Y/N)
Warning: You will
need all N keys!
```

- If you select **No**, the process is complete.
- If you select **Yes**, complete "[Stage 3: Setting a PIN](#)" on the next page for all the duplicate keys you want.

## Stage 2: Defining M of N

If you chose to create a new keyset, the Luna PED prompts you to define the M of N scheme (quorum and pool of splits) for the role, domain, or vector. See "[Quorum Split Secrets \(M of N\)](#)" on page 23 for more information. If you do not want to use M of N (authentication by one PED key), enter a value of **1** for both M and N. Effectively, you have set a "quorum" of one key-holder.

1. The PED prompts you to enter a value for M (the minimum number of split-secret keys required to authenticate the role, domain, or vector - the quorum). Set a value for M by entering it on the keypad and pressing **Enter**. If you are not using an M of N scheme, enter "**1**".

```
SLOT
SETTING SO PIN...
M value? (1-16)

>03
```

2. The PED prompts you to enter a value for N -- the total number of split-secret keys you want to create (the pool of splits from which a quorum will be drawn). Set a value for N by entering it on the keypad and pressing **Enter**. If you are not using an M of N scheme, enter "**1**".

```
SLOT
SETTING SO PIN...
N value? (M-16)

>05
```

3. Continue to "Stage 3: Setting a PIN" below. You must complete stage 3 for each key in the M of N scheme.

### Stage 3: Setting a PIN

If you are creating a new key or M of N split, you have the option of setting a PIN that must be entered by the key owner during authentication. PINs must be 4-48 digits long. Do not use 0 for the first digit. See "PINs" on page 23 for more information.

**CAUTION!** If you forget your PIN, it is the same as losing the PED key entirely; you cannot authenticate the role. See "Consequences of Losing PED keys" on page 74.

1. The PED prompts you to insert a blank or reusable PED key. If you are creating an M of N split, the number of already-created splits is displayed.

```
SLOT
SETTING SO PIN...
Insert a
SO / HSM Admin
PED Key (BLUE)
Press ENTER.
```

```
SLOT
SETTING SO PIN...
Keys write: 03 of 05
Insert another
SO / HSM Admin
PED Key (BLUE)
Press ENTER.
```

2. Insert the PED key and press **Enter**. The PED prompts for confirmation.

```
SLOT
SETTING SO PIN...
** WARNING **
This PED Key is
blank.
Overwrite? YES/NO
```

If the PED key you inserted is not blank, you must confirm twice that you want to overwrite it.

```
SLOT
SETTING SO PIN...
** WARNING **
This PED Key is for
Domain.
Overwrite? YES/NO
```

```
SLOT
SETTING SO PIN...
** WARNING **
Are you sure you
want to overwrite
this PED key? YES/NO
```

3. The PED prompts you for a PIN.
  - If you want to set a PIN, enter it on the keypad and press **Enter**. Enter the PIN again to confirm it.

```
SLOT
SETTING SO PIN...
Enter new PED PIN:
*****█
Confirm new PED PIN:
*****█
```

- If you do not want to set a PIN, press **Enter** twice without entering anything on the keypad. You will not be asked to enter a PIN for this key in the future.

```
SLOT
SETTING SO PIN...
Enter new PED PIN:
█
Confirm new PED PIN:
█
```

4. If there are more keys in the M of N scheme, repeat this stage. Otherwise, continue to "[Stage 4: Duplicating New PED keys](#)" below.

#### Stage 4: Duplicating New PED keys

You now have the option to create duplicates of your newly-created PED key(s). There are two reasons to do this now:

- > If you want more than one person to be able to authenticate a role, you can create multiple keys for that role now, with each person being able to set their own PIN. Duplicates you create later are intended as backups, and will have the same PIN (or none) as the key they are copied from.
- > In case of key loss or theft.

You can make backups now or later. See also "[Duplicating Existing PED keys](#)" on page 77.

1. The next PED prompt asks if you want to create a duplicate keyset (or another duplicate). Press **Yes** or **No** on the keypad to continue.

```
SLOT
SETTING SO PIN...
Are you duplicating
this keyset?(Y/N)
```

```
SLOT
SETTING SO PIN...
Would you like to
make another
duplicate set?(Y/N)
```

- If you select **No**, the key creation process is complete.
  - If you select **Yes**, complete "[Stage 3: Setting a PIN](#)" on the previous page for the duplicate keyset. You can set the same PIN to create a true copy, or set a different PIN for each duplicate.
2. If you specified an M of N scheme, you are prompted to repeat "[Stage 3: Setting a PIN](#)" on the previous page for each M of N split. Otherwise, the key creation process is complete.

## Performing Multifactor Quorum Authentication

When connected, the Luna PED responds to authentication commands in LunaSH or LunaCM. Commands that require PED actions include:

- > Role login commands (blue, black, gray, or white PED keys)
- > Backup/restore commands (red PED keys)
- > Remote PED connection commands (orange PED key)

**NOTE** The Luna PED screen prompts for a black PED key for any of

- > "User",
- > "Crypto Officer",
- > "Limited Crypto Officer",
- > "Crypto User".

The Luna PED is not aware that the key you present has a black or a gray sticker on it. The colored stickers are visual identifiers for your convenience in keeping track of your PED keys. You differentiate by how you label, and how you use, a given physical key that the Luna PED sees as "black" (once it has been imprinted with a secret).

When you issue a command that requires Luna PED interaction, the interface returns a message like the following:

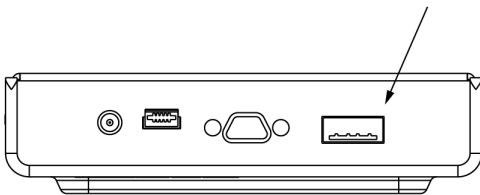
```
lunash:>hsm login
```

Luna PED operation required to login as HSM Administrator - use Security Officer (blue) PED key.

The PED briefly displays the following message before prompting you for the appropriate PED key:

```
Remote PED mode
Token found
```

Whenever the Luna PED prompts you to insert a PED key, use the USB port on the top of the PED:



**CAUTION!** Multiple failed authentication attempts result in zeroization of the HSM or partition, or role lockout, depending on the role. This is a security measure designed to thwart repeated, unauthorized attempts to access cryptographic material. For details, see ["Logging In as HSM Security Officer" on page 154](#) or [Logging In to the Application Partition](#).



## To perform multifactor quorum authentication with the Luna PED

1. The PED prompts for the corresponding PED key. Insert the PED key (or the first M of N split-secret key) and press **Enter**.

```
lunacm:>role login -name po
```

Please attend to the PED.

```
SLOT
SO LOGIN...
Insert a
SO / HSM Admin
PED Key (BLUE)
Press ENTER.
```

- If the key you inserted has an associated PIN, continue to step 2.
- If the key you inserted has no PIN, but it is an M of N split, skip to step 3.
- Otherwise, authentication is complete and the Luna PED returns control to the command interface.

Command Result : No Error

2. The PED prompts for the PIN. Enter the PIN on the keypad and press **Enter**.

```
SLOT
SO LOGIN...
Enter PED PIN:
*****■
```

- If the key you inserted is an M of N split, continue to step 3.
- Otherwise, authentication is complete and the PED returns control to the command interface.

Command Result : No Error

3. The PED prompts for the next M of N split-secret key. Insert the next PED key and press **Enter**.

```
SLOT
SO LOGIN...
Keys read: 01 of 02
Insert another
SO / HSM Admin
PED Key (BLUE)
Press ENTER.
```

- If the key you inserted has an associated PIN, return to step 2.
- Repeat steps 2 and/or 3 until the requisite M number of keys have been presented to the Luna PED. At this point, authentication is complete and the PED returns control to the command interface.

Command Result : No Error

**NOTE** When authenticating an M of N split secret, the Luna USB HSM 7 cannot tell if an PED key PIN is entered incorrectly until the whole secret is reassembled. Therefore, PIN entry will appear to succeed and the authentication operation will only fail when all M PED keys have been presented.

## Consequences of Losing PED keys

PED keys are the only means of authenticating roles, domains, and RPVs on the multifactor quorum-authenticated Luna Network HSM 7. Losing a keyset effectively locks the user out of that role. Always keep secure backups of your PED keys, including quorum (M of N) split secrets. Forgetting the PIN associated with a key is equivalent to losing the key entirely. Losing a split-secret key is less serious, unless enough splits are lost so that M cannot be satisfied.

If a PED key is lost or stolen, log in with one of your backup keys and change the existing PED key secret immediately, to prevent unauthorized HSM access.

The consequences of a lost PED key with no backup vary depending on the type of secret:

- > ["Blue HSM SO PED key" below](#)
- > ["Red HSM Domain PED key" on the next page](#)
- > ["Orange Remote PED Vector PED key" on the next page](#)
- > ["Blue Partition SO PED key" on the next page](#)
- > ["Red Partition Domain PED key" on the next page](#)
- > ["Black Crypto Officer PED key" on the next page](#)
- > ["Gray Crypto User PED key" on page 76](#)
- > ["White Audit User PED key" on page 76](#)

## Blue HSM SO PED key

If the HSM SO secret is lost, you can no longer perform administrative tasks on the HSM, including partition creation and client assignment. If you use the same blue SO key for your HSM backup partitions, the contents of the HSM SO space are unrecoverable. Take the following steps:

1. Contact all Crypto Officers and have them immediately make backups of their existing partitions at the client.
2. When all important partitions are backed up, execute a factory reset of the HSM.
3. Initialize the HSM and create a new HSM SO secret. Use the original red HSM cloning domain key.
4. Restore the HSM SO space contents from a recent backup, if you have one.
5. If you are using Remote PED, you must recreate the Remote PED Vector (RPV). Reuse the original orange key.
6. Recreate the partitions and reassign them to their respective clients.
7. Partition SOs must initialize the new partitions using their original blue and red key(s), and initialize the Crypto Officer role (and Activation secret, if applicable). Supply the new black CO keys to the Crypto Officers.
8. Crypto Officers must change the login credentials from the new black CO key to their original black keys (and reset the Activation secret password, if applicable).
9. Crypto Officers can now restore all partition contents from backup.

## Red HSM Domain PED key

If the HSM Key Cloning Vector is lost, you can no longer perform backup/restore operations on the HSM SO space(s). If the HSM is factory-reset, the contents of the HSM SO space are unrecoverable. Follow the same procedure as you would if you lost the blue HSM SO key, but you cannot restore the HSM SO space from backup.

## Orange Remote PED Vector PED key

If the Remote PED Vector is lost, create a new one and distribute a copy to the administrator of each Remote PED server. See ["Initializing the Remote PED Vector and Creating an Orange Remote PED key" on page 40](#).

## Blue Partition SO PED key

If the Partition SO secret is lost, you can no longer perform administrative tasks on the partition. Take the following steps:

1. Have the Crypto Officer immediately make a backup of the partition objects.
2. Have the HSM SO delete the partition, create a new one, and assign it to the same client.
3. Initialize the new partition with a new blue Partition SO key and the original red cloning domain key(s).
4. Initialize the Crypto Officer role (and Activation secret, if applicable). Supply the new black CO key to the Crypto Officer.
5. The Crypto Officer must change the login credentials from the new black CO key to their original black key (and reset the Activation secret password, if applicable).
6. The Crypto Officer can now restore all partition contents from backup.

## Red Partition Domain PED key

If the Partition Key Cloning Vector is lost, you can no longer perform backup/restore operations on the partition (s), or make changes to HA groups in that cloning domain. You can still perform all other operations on the partition. Take the following steps:

1. Have the HSM SO create a new partition (or multiple partitions, to replace the entire HA group) and assign it to the same client(s).
2. Initialize the partition(s) with a new cloning domain.
3. Initialize the Crypto Officer role with the original black Crypto Officer key (and Activation password, if applicable).
4. Create objects on the new partition to replace those on the original partition.
5. As soon as possible, change all applications to use the objects on the new partition.
6. When objects on the original partition are no longer in production use, the HSM SO can delete the original partition.

## Black Crypto Officer PED key

If the Crypto Officer secret is lost, you can no longer create objects on the partition, or perform backup/restore operations. You might still be able to use the partition, depending on the following criteria:

### > PIN reset by Partition SO:

- If HSM policy **15: Enable SO reset of partition PIN** is set to **1**, the Partition SO can reset the Crypto Officer secret and create a new black CO key.

```
lunacm:>role resetpw -name co
```

- If this policy is set to **0** (default), the CO is locked out unless other criteria in this list apply.

#### > Partition Activation:

- If the partition is Activated, you can still access it for production using the CO challenge secret. Change your applications to use objects on a new partition as soon as possible.
- If the partition is not Activated, read-only access of essential objects might still be available via the Crypto User role.

#### > Crypto User

- If the Crypto User is initialized, you can use the CU role for read-only access to essential partition objects while you change your applications to use objects on a new partition.

If none of these criteria apply, the contents of the partition are unrecoverable.

## Gray Crypto User PED key

If the Crypto User secret is lost, the Crypto Officer can reset the CU secret and create a new gray key:

```
lunacm:>role resetpw -name cu
```

## White Audit User PED key

If the Audit User secret is lost, you can no longer cryptographically verify existing audit logs or make changes to the audit configuration. The existing logs can still be viewed. Re-initialize the Audit User role on the affected HSMs, using the same white key for HSMs that will verify each other's logs.

## Identifying the PED key Secret

You can use this procedure to identify the type of secret (role, domain, or RPV) stored on an unidentified PED key. This procedure will not tell you:

- > identifying information about the HSM the key is associated with
- > whether the key is part of an M of N scheme, or how many keys are in the set
- > whether the key has a PIN assigned
- > who the key belongs to

You require:

- > Luna PED in Admin Mode (see ["Changing Modes" on page 30](#))
- > the key you want to identify

### To identify the type of secret stored on an existing PED key

1. Insert the PED key you want to identify.
2. From the Admin mode menu, press **1** on the keypad to select the **PED Key** option.

```
Admin mode...
1 PED Key
5 Backup Devices
7 Software Update
9 Self Test
< EXIT
```

- From the PED Key mode menu, press **3** on the keypad to select the **List types** option.

```
PED Key mode
1 Login
3 List types
< EXIT
```

The secret type is identified on-screen.

```
PED Key mode
Found keys:
Domain

Press ENTER.
```

## Duplicating Existing PED keys

During the key creation process, you have the option to create multiple copies of PED keys. If you want to make backups of your keys later, you can use this procedure to copy PED keys. You require:

- > Luna PED in Admin Mode (see ["Changing Modes" on page 30](#))
- > Enough blank or rewritable keys to make your copies

The PED key is duplicated exactly by this process. If there is a PIN assigned, the same PIN is assigned to the duplicate key. If the key is part of a quorum (M of N) scheme, the duplicates may not be used in the same login process to satisfy the M of N requirements. You must also have copies of the other keys in the quorum (M of N) keyset. See ["Quorum Split Secrets \(M of N\)" on page 23](#).

### To duplicate an existing PED key

- Insert the PED key you want to duplicate. Have a blank or rewritable PED key ready.
- From the Admin mode menu, press **1** on the keypad to login to the PED key.

```
PED Key mode
1 Login
3 List types
< EXIT
```

- Press **7** on the keypad and follow the on-screen instructions.

```

PED Key mode
  2 Logout
  3 List types
  7 Duplicate
  < EXIT

```

## Changing the PED key Secret

Use the instructions on this page to change/rotate the secrets on any of the indicated PED iKeys.

From time to time, it might be necessary to change the secret associated with a role on an HSM appliance, a role on an HSM or a partition of an HSM, or a cloning domain secret. Reasons for changing credentials include:

- > Regular credential rotation as part of your organization's security policy
- > Compromise of a role or secret due to loss or theft of a PED key
- > Personnel changes in your organization or changes to individual security clearances
- > Changes to your security scheme (implementing/revoking M of N, PINs, or shared secrets)

The procedure for changing a PED key credential depends on the type of key. Procedures for each type are provided below.

**CAUTION!** If you are changing a multifactor quorum credential that is shared among multiple HSMs/partitions/roles, always keep at least one copy of the old keyset until the affected HSMs/partitions/roles are all changed to the new credential. When changing multifactor quorum credentials, you must always present the old keyset first; do not overwrite your old PED keys until you have no further need for them.

- > "Blue HSM SO PED key" below
- > "Red HSM Domain PED key" on the next page
- > "Orange Remote PED Vector PED key" on the next page
- > "Blue Partition SO PED key" on the next page
- > "Red Partition Domain PED key" on the next page
- > "Black Crypto Officer PED key" on page 80
- > "Gray Crypto User PED key" on page 80
- > "White Audit User PED key" on page 81

### Blue HSM SO PED key

The HSM SO can use this procedure to change the HSM SO credential.

#### To change the blue HSM SO PED key credential

1. In LunaSH, log in as HSM SO.  
lunash:> **hsm login**
2. Initiate the PED key change.

lunash:> **hsm changepw**

3. You are prompted to present the original blue PED key(s) and then to create a new HSM SO keyset. See "Creating PED keys" on page 66.

## Red HSM Domain PED key

It is not possible to change an **HSM's cloning domain** without factory-resetting the HSM and setting the new cloning domain as part of the standard initialization procedure.

**CAUTION!** If you set a different cloning domain for the HSM, you cannot restore the HSM SO space from backup.

## Orange Remote PED Vector PED key

The HSM SO can use this procedure to change the Remote PED Vector (RPV) for the HSM.

### To change the RPV/orange key credential

1. In LunaSH, log in as HSM SO.

lunash:> **hsm login**

2. Initialize the RPV.

lunash:> **hsm ped vector init**

You are prompted to create a new Remote PED key. See "Creating PED keys" on page 66.

3. Distribute a copy of the new orange key to the administrator of each Remote PED server.

## Blue Partition SO PED key

The Partition SO can use this procedure to change the Partition SO credential.

### To change a blue Partition SO PED key credential

1. In LunaCM, log in as Partition SO.

lunacm:> **role login -name po**

2. Initiate the PED key change.

lunacm:> **role changepw -name po**

3. You are prompted to present the original blue key(s) and then to create a new Partition SO keyset. See "Creating PED keys" on page 66.

## Red Partition Domain PED key

If you are using [Luna HSM Firmware 7.7.2](#) and older, it is not possible to change a partition's cloning domain. A new partition must be created and initialized with the desired domain. The new partition will not have access to any of the original partition's backups. It cannot be made a member of the same HA group as the original.

Using [Luna HSM Firmware 7.8.0](#) and newer, each partition can support up to three different cloning domains, allowing your sensitive keys and objects to remain within the cryptographic perimeter of the HSM while:

- > migrating objects from one domain to another
- > splitting domains
- > rotating or rolling-over or refreshing your partition domain secrets as part of mandated periodic changes of credential/authentication, just as you would with passwords for
  - appliance administration (including network, logging, ntp, tamper response, etc.)
  - HSM or partition roles
    - container/partition administrative access
    - client access for crypto operations on keys and objects
  - etc.

---

### To change the domain secret

See [Updating or rotating cloning domain secrets](#).

## Black Crypto Officer PED key

The Crypto Officer can use this procedure to change the Crypto Officer credential.

---

### To change a black Crypto Officer PED key credential

1. In LunaCM, log in as Crypto Officer.  
lunacm:> **role login -name co**
2. Initiate the PED key change.  
lunacm:> **role changepw -name co**
3. You are prompted to present the original black key(s) and then to create a new Crypto Officer keyset. See ["Creating PED keys" on page 66](#).

## Gray Crypto User PED key

The Crypto User can use this procedure to change the Crypto User credential.

---

### To change a gray Crypto User PED key credential

1. In LunaCM, log in as Crypto User.  
lunacm:> **role login-name cu**
2. Initiate the PED key change.  
lunacm:> **role changepw -name cu**
3. You are prompted to present the original gray key(s) and then to create a new Crypto User keyset. See ["Creating PED keys" on page 66](#).



**NOTE** The Luna PED screen prompts for a black PED key for any of

- > "User",
- > "Crypto Officer",
- > "Limited Crypto Officer",
- > "Crypto User".

The Luna PED is not aware that the key you present has a black or a gray sticker on it. The colored stickers are visual identifiers for your convenience in keeping track of your PED keys. You differentiate by how you label, and how you use, a given physical key that the Luna PED sees as "black" (once it has been imprinted with a secret).

## White Audit User PED key

The Audit User can use this procedure to change the Audit User credential.

### To change the white Audit User PED key credential

1. Log into LunaSH as **audit**.
2. Log in as the Audit User.  
lunash:> **audit login**
3. Initiate the PED key change.  
lunash:> **audit changepwd**
4. You are prompted to present the original white key(s) and then to create a new Audit User keyset. See ["Creating PED keys" on page 66](#).

## PEDserver and PEDclient

You can use the **PEDserver** and **PEDclient** utilities to manage your remote PED devices.

### The PEDserver Utility

PEDserver is required to run on any computer that has a Luna Remote PED attached, and is providing PED services.

The PEDserver utility has one function. It resides on a computer with an attached Luna PED (in Remote Mode), and it serves PED operations to an instance of PEDclient that operates on behalf of an HSM. The HSM could be local to the computer that has PEDserver running, or it could be on another HSM host computer at some distant location.

PEDserver can also run in peer-to-peer mode, where the server initiates the connection to the Client. This is needed when the Client (usually Luna Network HSM 7) is behind a firewall that forbids outgoing initiation of connections.

See ["pedserver" on page 83](#).

## The PEDclient Utility

PEDclient is required to run on any host of an HSM that needs to be served by a Remote Luna PED. PEDclient must also run on any host of a Remote Backup HSM that will be serving remote primary HSMs.

The PEDclient utility performs the following functions:

- > It mediates between the HSM where it is installed and the Luna PED where PEDserver is installed, to provide PED services to the requesting HSM(s).
- > It resides on a computer with RBS and an attached Luna Backup HSM, and it connects with another instance of PEDclient on a distant host of an HSM, to provide the link component for Remote Backup Service. See [Configuring a Remote Backup Server](#) for more information.
- > It acts as the logging daemon for HSM audit logs.

**NOTE** PEDclient exists on the Luna Network HSM 7 appliance, but is not directly exposed. Instead, the relevant features are accessed via LunaSH **hsm ped** commands.

Thus, for example, in the case where an administrative workstation or laptop has both a Remote PED and a Remote Backup HSM attached, PEDclient would perform double duty. It would link with a locally-running instance of PEDserver, to convey HSM requests from the locally-connected Backup HSM to the locally-connected PED, and return the PED responses. As well, it would link a locally-running instance of RBS and a distant PEDclient instance to mediate Remote Backup function for that distant HSM's partitions.

See "[pedclient](#)" on page 98.

## pedserver

Use the **pedserver** commands to manage certificates in PEDserver and the appliance, initiate connections between the Luna PED and HSM, and select the PED for HSM operation.

To run PEDserver from the command line, you must specify one of the following three options.

### Syntax

#### pedserver

- appliance
- mode
- regen

| Option     | Description  |
|------------|--|
| -appliance | Registers or deregisters an appliance, or lists the registered appliances. Applies to server-initiated (peer-to-peer) mode only. See <a href="#">"pedserver -appliance" on the next page</a> . |
| -mode      | Specifies the mode that the PED Server will be executed in. See <a href="#">"pedserver mode" on page 88</a> .  |
| -regen     | Regenerates the client certificate. Applies to server-initiated (peer-to-peer) mode only. See <a href="#">"pedserver -regen" on page 98</a> .  |

## pedserver -appliance

---

Registers or deregisters an appliance, or lists the registered appliances. These commands apply to PED-initiated mode only.

### Syntax

#### pedserver -appliance

**delete**  
**list**  
**register**

| Option          | Description   |
|-----------------|---|
| <b>delete</b>   | Deregisters an appliance. See " <a href="#">pedserver -appliance delete</a> " on the next page. |
| <b>list</b>     | Lists the registered appliances. See " <a href="#">pedserver -appliance list</a> " on page 86.  |
| <b>register</b> | Registers an appliance. See " <a href="#">pedserver -appliance register</a> " on page 87        |

---

## pedserver -appliance delete

---

Deregister an appliance certificate from PEDserver.

### Syntax

**pedserver -appliance delete -name <unique name> [-force]**

| Option                     | Description  |
|----------------------------|--|
| <b>-name</b> <unique name> | Specifies the name of the appliance to be deregistered from PEDserver. |
| <b>-force</b>              | Optional parameter. Suppresses any prompts.                            |

### Example

```
C:\Program Files\Safenet\LunaClient>pedServer -appliance delete -name hello -force
```

---

## pedserver -appliance list

---

Displays a list of appliances registered with PEDserver.

### Syntax

**pedserver -appliance list**

### Example

```
C:\Program Files\Safenet\LunaClient>pedServer -appliance list
```

```
>
```

| Server Name | IP Address | Port Number | Certificate Common Name |
|-------------|------------|-------------|-------------------------|
|-------------|------------|-------------|-------------------------|

|       |              |      |           |
|-------|--------------|------|-----------|
| abox  | 192.20.1.23  | 9697 | test2     |
| bbox  | 192.20.12.34 | 9696 | test1     |
| hello | 192.20.1.34  | 9876 | hellocert |

## pedserver -appliance register

Register an appliance certificate with PEDserver.

### Syntax

**pedserver -appliance register -name** <unique name> **-certificate** <appliance certificate file> **-ip** <appliance server IP address> [**-port** <port number>]

| Option   | Description  |
|--|--|
| <b>-name</b> <unique name>                       | Specifies the name of the appliance to be registered to PEDserver.   |
| <b>-certificate</b> <appliance certificate file> | Specifies the full path and filename of the certificate that was retrieved from the appliance.   |
| <b>-ip</b> <appliance server IP address>         | Specifies the IP address of the appliance server.  |
| <b>-port</b> <port number>                       | Optional field. Specifies the port number used to connect to the appliance (directly or indirectly according to network configuration).<br><b>Range:</b> 0-65525 |

### Example

```
C:\Program Files\Safenet\LunaClient>pedServer -appliance register -name hello -certificate the-best-appliance.pem -ip 123.321.123.321 -port 9697
```

## pedserver mode

Specifies the mode that PEDserver will be executed in.

### Syntax

**pedserver -mode**

**config**  
**connect**  
**disconnect**  
**show**  
**start**  
**stop**

| Option            | Description   |
|-------------------|---|
| <b>config</b>     | Modifies or shows existing configuration file settings. See " <a href="#">pedserver -mode config</a> " on the next page.              |
| <b>connect</b>    | Connects to the appliance. See " <a href="#">pedserver -mode connect</a> " on page 91.  |
| <b>disconnect</b> | Disconnects from the appliance. See " <a href="#">pedserver -mode disconnect</a> " on page 92.  |
| <b>show</b>       | Queries if PEDserver is currently running, and gets details about PEDserver. See " <a href="#">pedserver -mode show</a> " on page 93. |
| <b>start</b>      | Starts PEDserver. See " <a href="#">pedserver -mode start</a> " on page 95.   |
| <b>stop</b>       | Shuts down PEDserver. See " <a href="#">pedserver -mode stop</a> " on page 97   |



## pedserver -mode config

Shows and modifies internal PEDserver configuration file settings.

### Syntax

```
pedserver -mode config -name <registered appliance name> -show -set [-port <server port>] [-set][-configfile <filename>] [-admin <admin port number>] [-eserverport <0 or 1>] [-eadmin <0 or 1>] [-idletimeout <int>] [-socketreadtimeout <int>] [-socketwritetimeout <int>] [-internalshutdowntimeout <int>] [-bgprocessstartuptimeout <int>] [-bgprocessshutdowntimeout <int>] [-logfile <filename>] [-loginfo <0 or 1>] [-logwarning <0 or 1>] [-logerror <0 or 1>] [-logtrace <0 or 1>] [-maxlogfilesize <size>] [-pedwritelay <int>] [-pinginterval <int>] [-pingtimeout <int>]
```

| Option                                   | Description   |
|--|---|
| <b>-name</b> <registered appliance name> | Specifies the name of the registered appliance to be configured.                                    |
| <b>-show</b>                             | Displays the contents of the PEDserver configuration file.  |
| <b>-set</b>                              | Updates the PEDserver configuration file to be up to date with other supplied options.              |
| <b>-port</b> <server port>               | Optional. Specifies the server port number.   |
| <b>-configfile</b> <filename>            | Optional. Specifies which PEDserver configuration file to use.                                      |
| <b>-admin</b> <admin port number>        | Optional. Specifies the administration port number.   |
| <b>-eserverport</b> <0 or 1>             | Optional. Specifies if the server port is on "localhost" or listening on the external host name.    |
| <b>-eadmin</b> <0 or 1>                  | Optional. Specifies if the administration is on "localhost" or listening on the external host name. |
| <b>-idletimeout</b> <int>                | Optional. Specifies the idle connection timeout, in seconds.  |
| <b>-socketreadtimeout</b> <int>          | Optional. Specifies the socket read timeout, in seconds.  |
| <b>-socketwritetimeout</b> <int>         | Optional. Specifies socket write timeout, in seconds.   |
| <b>-internalshutdowntimeout</b> <int>    | Optional. Specifies the shutdown timeout for internal services, in seconds.                         |
| <b>-bgprocessstartuptimeout</b> <int>    | Optional. Specifies the startup timeout for the detached process, in seconds.                       |
| <b>-bgprocessshutdowntimeout</b> <int>   | Optional. Specifies the shutdown timeout for the detached process, in seconds.                      |

| Option                        | Description  |
|-------------------------------|--|
| <b>-logfile</b> <filename>    | Optional. Specifies the log file name to which the logger should log messages.   |
| <b>-loginfo</b> <0 or 1>      | Optional. Specifies if the logger should log "info" messages. Set to 0 for no, 1 for yes.  |
| <b>-logwarning</b> <0 or 1>   | Optional. Specifies if the logger should log "warning" messages. Set to 0 for no, 1 for yes.   |
| <b>-logerror</b> <0 or 1>     | Optional. Specifies if the logger should log "error" messages. Set to 0 for no, 1 for yes.   |
| <b>-logtrace</b> <0 or 1>     | Optional. Specifies if the logger should log "trace" messages. Set to 0 for no, 1 for yes.   |
| <b>-maxlogfilesize</b> <size> | Optional. Specifies the maximum log file size in KB.   |
| <b>-pedwritelay</b> <int>     | Optional. Specifies the communications delay over USB between the Luna PED and PEDserver, in microseconds. Default value is 0 and maximum value is 10000.<br>This option is available only if you are using a multifactor quorum-authenticated Luna HSM with <a href="#">Luna HSM Firmware 7.7.0</a> or newer. |
| <b>-pinginterval</b> <int>    | Optional. Specifies the time interval between ping commands, in seconds.   |
| <b>-pingtimeout</b> <int>     | Optional. Specifies timeout of the ping response, in seconds.  |

## Example

```
C:\Program Files\Safenet\LunaClient>pedServer -mode config -name hellohi -show
```

## pedserver -mode connect

Connects to the appliance by retrieving information (IP address, port, PEDserver certificate) from the PEDserver configuration file.

If the running mode is legacy, an error is returned. **pedserver -mode connect** is not a valid command for legacy connections.

The **connect** command will try connecting to PEDclient 20 times before giving up.

### Syntax

**pedserver -mode connect -name** <registered appliance name> [-**configfile** <filename>] [-**logfile** <filename>] [-**loginfo** <0 or 1>] [-**logwarning** <0 or 1>] [-**logerror** <0 or 1>] [-**logtrace** <0 or 1>] [-**maxlogfilesize** <size>]

| Option                                   | Description  |
|--|--|
| <b>-name</b> <registered appliance name> | Specifies the name of the registered appliance to be connected to PEDserver.                 |
| <b>-configfile</b> <filename>            | Optional. Specifies which PEDserver configuration file to use.                               |
| <b>-logfile</b> <filename>               | Optional. Specifies the log file name to which the logger should log messages.               |
| <b>-loginfo</b> <0 or 1>                 | Optional. Specifies if the logger should log "info" messages. Set to 0 for no, 1 for yes.    |
| <b>-logwarning</b> <0 or 1>              | Optional. Specifies if the logger should log "warning" messages. Set to 0 for no, 1 for yes. |
| <b>-logerror</b> <0 or 1>                | Optional. Specifies if the logger should log "error" messages. Set to 0 for no, 1 for yes.   |
| <b>-logtrace</b> <0 or 1>                | Optional. Specifies if the logger should log "trace" messages. Set to 0 for no, 1 for yes.   |
| <b>-maxlogfilesize</b> <size>            | Optional. Specifies the maximum log file size in KB.   |

### Example

```
C:\Program Files\Safenet\LunaClient>pedServer -mode connect -name hellohi
>Connecting to Luna SA. Please wait....
>Successfully connected to Luna SA.
```

## pedserver -mode disconnect

Disconnects PEDserver from the appliance.

If the running mode is legacy, an error is returned. **pedserver -mode disconnect** is not a valid command for legacy connections.

Termination of the connection may take a few minutes.

### Syntax

**pedserver -mode disconnect -name** <registered appliance name> [-**configfile** <filename>] [-**logfile** <filename>] [-**loginfo** <0 or 1>] [-**logwarning** <0 or 1>] [-**logerror** <0 or 1>] [-**logtrace** <0 or 1>] [-**maxlogfilesize** <size>]

| Option                                   | Description  |
|--|--|
| <b>-name</b> <registered appliance name> | Specifies the name of the registered appliance to be disconnected from PEDserver.            |
| <b>-configfile</b> <filename>            | Optional. Specifies which PEDserver configuration file to use.                               |
| <b>-logfile</b> <filename>               | Optional. Specifies the log file name to which the logger should log messages.               |
| <b>-loginfo</b> <0 or 1>                 | Optional. Specifies if the logger should log "info" messages. Set to 0 for no, 1 for yes.    |
| <b>-logwarning</b> <0 or 1>              | Optional. Specifies if the logger should log "warning" messages. Set to 0 for no, 1 for yes. |
| <b>-logerror</b> <0 or 1>                | Optional. Specifies if the logger should log "error" messages. Set to 0 for no, 1 for yes.   |
| <b>-logtrace</b> <0 or 1>                | Optional. Specifies if the logger should log "trace" messages. Set to 0 for no, 1 for yes.   |
| <b>-maxlogfilesize</b> <size>            | Optional. Specifies the maximum log file size in KB.   |

### Example

```
C:\Program Files\Safenet\LunaClient>pedServer -mode disconnect -name hellohi
>Connection to Luna SA terminated.
```

## pedserver -mode show

Queries if PEDserver is currently running, and gets details about PEDserver.

### Syntax

**pedserver -mode show** [-name <registered appliance name>] [-configfile <filename>] [-logfile <filename>] [-loginfo <0 or 1>] [-logwarning <0 or 1>] [-logerror <0 or 1>] [-logtrace <0 or 1>] [-maxlogfilesize <size>]

| Option                            | Description   |
|-----------------------------------|---|
| -name <registered appliance name> | Specifies the name of the registered appliance to be queried. Applies to server-initiated (peer-to-peer) mode only. |
| -configfile <filename>            | Optional. Specifies which PEDserver configuration file to use.  |
| -logfile <filename>               | Optional. Specifies the log file name to which the logger should log messages.                                      |
| -loginfo <0 or 1>                 | Optional. Specifies if the logger should log "info" messages. Set to 0 for no, 1 for yes.                           |
| -logwarning <0 or 1>              | Optional. Specifies if the logger should log "warning" messages. Set to 0 for no, 1 for yes.                        |
| -logerror <0 or 1>                | Optional. Specifies if the logger should log "error" messages. Set to 0 for no, 1 for yes.                          |
| -logtrace <0 or 1>                | Optional. Specifies if the logger should log "trace" messages. Set to 0 for no, 1 for yes.                          |
| -maxlogfilesize <size>            | Optional. Specifies the maximum log file size in KB.  |

### Example

```
C:\Program Files\Safenet\LunaClient>pedServer -mode show -name hellohi
>Ped Server launched in status mode.
  Server Information:
    Hostname:                ABC1-123123
    IP:                      192.10.10.123
    Firmware Version:        2.5.0-1
    PedII Protocol Version:   1.0.1-0
    Software Version:         1.0.5 (10005)
    Ped2 Connection Status:   Connected
    Ped2 RPK Count           1
    Ped2 RPK Serial Numbers   (1a123456789a1234)
  Client Information:        Not Available
  Operating Information:
    Server Port:              1234
    External Server Interface: Yes
    Admin Port:               1235
```

```
External Admin Interface:      No
Server Up Time:                8 (secs)
Server Idle Time:              8 (secs) (100%)
Idle Timeout Value:            1800 (secs)
Current Connection Time:       0 (secs)
Current Connection Idle Time:  0 (secs)
Current Connection Total Idle Time: 0 (secs) (100%)
Total Connection Time:         0 (secs)
Total Connection Idle Time:    0 (secs) (100%)
>Show command passed.
```

## pedserver -mode start

Starts up PEDserver.

### Syntax

```
pedserver -mode start [-name <registered appliance name>] [-ip <server_IP>] [-port <server port>] [-configfile <filename>] [-admin <admin port number>] [-eserverport <0 or 1>] [-eadmin <0 or 1>] [-idletimeout <int>] [-socketreadtimeout <int>] [-socketwritetimeout <int>] [-internalshutdowntimeout <int>] [-bgprocessstartuptimeout <int>] [-bgprocessshutdowntimeout <int>] [-logfile <filename>] [-loginfo <0 or 1>] [-logwarning <0 or 1>] [-logerror <0 or 1>] [-logtrace <0 or 1>] [-maxlogfilesize <size>] [-pinginterval <int>] [-pingtimeout <int>] [-force]
```

| Option                                 | Description  |
|--|--|
| <b>-admin</b> <admin port number>      | Optional. Specifies the administration port number.  |
| <b>-bgprocessshutdowntimeout</b> <int> | Optional. Specifies the shutdown timeout for the detached process, in seconds.   |
| <b>-bgprocessstartuptimeout</b> <int>  | Optional. Specifies the startup timeout for the detached process, in seconds.  |
| <b>-configfile</b> <filename>          | Optional. Specifies which PED Server configuration file to use.  |
| <b>-eadmin</b> <0 or 1>                | Optional. Specifies if the administration is on "localhost" or listening on the external host name.  |
| <b>-eserverport</b> <0 or 1>           | Optional. Specifies if the server port is on "localhost" or listening on the external host name.   |
| <b>-force</b>                          | Optional parameter. Suppresses any prompts.  |
| <b>-idletimeout</b> <int>              | Optional. Specifies the idle connection timeout, in seconds.   |
| <b>-internalshutdowntimeout</b> <int>  | Optional. Specifies the shutdown timeout for internal services, in seconds.  |
| <b>-ip</b> <server_IP>                 | Optional. Specifies the server listening IP address. When <b>running pedserver -mode start</b> on an IPv6 network, you must include this option. |
| <b>-logerror</b> <0 or 1>              | Optional. Specifies if the logger should log "error" messages. Set to 0 for no, 1 for yes.   |
| <b>-logfile</b> <filename>             | Optional. Specifies the log file name to which the logger should log messages.   |
| <b>-loginfo</b> <0 or 1>               | Optional. Specifies if the logger should log "info" messages. Set to 0 for no, 1 for yes.  |

| Option                                   | Description  |
|--|--|
| <b>-logtrace</b> <0 or 1>                | Optional. Specifies if the logger should log "trace" messages. Set to 0 for no, 1 for yes.   |
| <b>-logwarning</b> <0 or 1>              | Optional. Specifies if the logger should log "warning" messages. Set to 0 for no, 1 for yes. |
| <b>-maxlogfilesize</b> <size>            | Optional. Specifies the maximum log file size in KB.   |
| <b>-name</b> <registered appliance name> |  |
| <b>-pinginterval</b> <int>               | Optional. Specifies the time interval between ping commands, in seconds.                     |
| <b>-pingtimeout</b> <int>                | Optional. Specifies timeout of the ping response, in seconds.                                |
| <b>-port</b> <server port>               | Optional. Specifies the server port number.  |
| <b>-socketreadtimeout</b> <int>          | Optional. Specifies the socket read timeout, in seconds.                                     |
| <b>-socketwritetimeout</b> <int>         | Optional. Specifies socket write timeout, in seconds.  |

## Example

```
C:\Program Files\Safenet\LunaClient>pedServer -mode start -name hellohi -force
>Ped Server launched in startup mode.
>Starting background process
>Background process started
>Ped Server Process created, exiting this process.
```



## pedserver -mode stop

Stops PEDserver.

### Syntax

**pedserver -mode stop** [-name <registered appliance name>] [-configfile <filename>] [-socketwritetimeout <int>] [-internalshutdowntimeout <int>] [-bgprocessstartuptimeout <int>] [-bgprocessshutdowntimeout <int>] [-logfile <filename>] [-loginfo <0 or 1>] [-logwarning <0 or 1>] [-logerror <0 or 1>] [-logtrace <0 or 1>] [-maxlogfilesize <size>]

| Option                                   | Description  |
|--|--|
| <b>-name</b> <registered appliance name> | Specifies the name of the registered appliance on which PEDserver will be stopped. Applies to server-initiated (peer-to-peer) mode only. |
| <b>-configfile</b> <filename>            | Optional. Specifies which PEDserver configuration file to use.   |
| <b>-socketreadtimeout</b> <int>          | Optional. Specifies the socket read timeout, in seconds.   |
| <b>-socketwritetimeout</b> <int>         | Optional. Specifies socket write timeout, in seconds.  |
| <b>-internalshutdowntimeout</b> <int>    | Optional. Specifies the shutdown timeout for internal services, in seconds.  |
| <b>-bgprocessstartuptimeout</b> <int>    | Optional. Specifies the startup timeout for the detached process, in seconds.  |
| <b>-bgprocessshutdowntimeout</b> <int>   | Optional. Specifies the shutdown timeout for the detached process, in seconds.   |
| <b>-logfile</b> <filename>               | Optional. Specifies the log file name to which the logger should log messages.   |
| <b>-loginfo</b> <0 or 1>                 | Optional. Specifies if the logger should log "info" messages. Set to 0 for no, 1 for yes.  |
| <b>-logwarning</b> <0 or 1>              | Optional. Specifies if the logger should log "warning" messages. Set to 0 for no, 1 for yes.   |
| <b>-logerror</b> <0 or 1>                | Optional. Specifies if the logger should log "error" messages. Set to 0 for no, 1 for yes.   |
| <b>-logtrace</b> <0 or 1>                | Optional. Specifies if the logger should log "trace" messages. Set to 0 for no, 1 for yes.   |
| <b>-maxlogfilesize</b> <size>            | Optional. Specifies the maximum log file size in KB.   |

### Example

```
C:\Program Files\Safenet\LunaClient>pedServer -mode stop -name hellohi
```

## pedserver -regen

Regenerates the client certificate. This command is available in server-initiated (peer-to-peer) mode only.

Existing links (PEDserver, NTLS or STC) will not be affected until they are terminated. Afterward, the user is required to re-register the client certificate to NTLS and PEDserver.

**NOTE** The **pedserver -regen** command should be used only when there is no Luna HSM Client installed. When Luna HSM Client is installed on the host computer, use the LunaCM command **clientconfig deploy** with the **-regen** option or, if necessary, **vtl createCert**.

### Syntax

**pedserver -regen -commonname <commonname> [-force]**

| Option                             | Description                                 |
|------------------------------------|---|
| <b>-commonname</b><br><commonname> | The client's common name (CN).              |
| <b>-force</b>                      | Optional parameter. Suppresses any prompts. |

### Example

```
C:\Program Files\SafeNet\LunaClient>pedServer -regen -commonname win2016_server -force
Ped Server Version 1.0.6 (10006)
```

```
Private Key created and written to: C:\Program Files\SafeNet\LunaClient\cert\client\win2016_serverKey.pem
```

```
Certificate created and written to: C:\Program Files\SafeNet\LunaClient\cert\client\win2016_server.pem
```

Successfully regenerated the client certificate.

## pedclient

Use the **pedclient** commands to start, stop, and configure the PEDclient service.

### Syntax

**pedclient -mode**

**assignid**  
**config**  
**deleteid**  
**releaseid**  
**setid**  
**show**

**start**  
**stop**  
**testid**

| Option           | Description   |
|------------------|---|
| <b>assignid</b>  | Assigns a PED ID mapping to an HSM. See <a href="#">"pedclient -mode assignid" on the next page.</a>                                |
| <b>config</b>    | Modifies or shows existing configuration file settings. See <a href="#">"pedclient -mode config" on page 101.</a>                   |
| <b>deleteid</b>  | Deletes a PED ID mapping. See <a href="#">"pedclient -mode deleteid" on page 103.</a>   |
| <b>releaseid</b> | Releases a PED ID mapping from an HSM. See <a href="#">"pedclient -mode releaseid" on page 104.</a>                                 |
| <b>setid</b>     | Creates a PED ID mapping. See <a href="#">"pedclient -mode setid" on page 105.</a>  |
| <b>show</b>      | Queries if PEDclient is currently running and gets details about PEDclient. See <a href="#">"pedclient -mode show" on page 106.</a> |
| <b>start</b>     | Starts up PEDclient. See <a href="#">"pedclient -mode start" on page 107.</a>   |
| <b>stop</b>      | Shuts down PEDclient. See <a href="#">"pedclient -mode stop" on page 109.</a>   |
| <b>testid</b>    | Tests a PED ID mapping. See <a href="#">"pedclient -mode testid" on page 110.</a>   |

## pedclient -mode assignid

Assigns a PED ID mapping to a specified HSM.

### Syntax

**pedclient -mode assignid -id <pedid> -id\_serialnumber <serial> [-logfile <filename>] [-loginfo <0 or 1>] [-logwarning <0 or 1>] [-logerror <0 or 1>] [-logtrace <0 or 1>] [-maxlogfilesize <size>] [-locallogger]**

| Option                                 | Description  |
|--|--|
| <b>-id &lt;pedid&gt;</b>               | Specifies the ID of the PED to be assigned.  |
| <b>-id_serialnumber &lt;serial&gt;</b> | Specifies the serial number of the HSM to be linked to the specified PED ID.                 |
| <b>-logfile &lt;filename&gt;</b>       | Optional. Specifies the log file name to which the logger should log messages.               |
| <b>-loginfo &lt;0 or 1&gt;</b>         | Optional. Specifies if the logger should log "info" messages. Set to 0 for no, 1 for yes.    |
| <b>-logwarning &lt;0 or 1&gt;</b>      | Optional. Specifies if the logger should log "warning" messages. Set to 0 for no, 1 for yes. |
| <b>-logerror &lt;0 or 1&gt;</b>        | Optional. Specifies if the logger should log "error" messages. Set to 0 for no, 1 for yes.   |
| <b>-logtrace &lt;0 or 1&gt;</b>        | Optional. Specifies if the logger should log "trace" messages. Set to 0 for no, 1 for yes.   |
| <b>-maxlogfilesize &lt;size&gt;</b>    | Optional. Specifies the maximum log file size in KB.   |
| <b>-locallogger</b>                    | Optional. Specifies that the Remote PED logger should be used, not the IS logging system.    |

### Example

```
C:\Program Files\Safenet\LunaClient>pedClient -mode assignid -id 1234 -id_serialnumber 123456789
```

## pedclient -mode config

Modifies or shows existing configuration file settings.

### Syntax

```
pedclient -mode config -show -set [-eadmin <0 or 1>] [-idletimeout <int>] [-ignoreidletimeout] [-socketreadtimeout <int>] [-socketwritetimeout <int>] [-shutdowntimeout <int>] [-pstartuptimeout <int>] [-pshutdowntimeout <int>] [-logfilename <filename>] [-loginfo <0 or 1>] [-logwarning <0 or 1>] [-logtrace <0 or 1>] [-maxlogfilesize <size>] [-locallogger]
```

| Option                                 | Description  |
|--|--|
| <b>-show</b>                           | Displays the contents of the configuration file.   |
| <b>-set</b>                            | Updates the configuration file to be up to date with other supplied options.   |
| <b>-eadmin &lt;0 or 1&gt;</b>          | Optional. Specifies if the administration port is on "localhost" or on the external host name.   |
| <b>-idletimeout &lt;int&gt;</b>        | Optional. Specifies the idle connection timeout, in seconds.   |
| <b>-ignoreidletimeout</b>              | Optional. Specifies that the idle connection timeout should not apply to the connection established between the PED and HSM during their assignment. |
| <b>-socketreadtimeout &lt;int&gt;</b>  | Optional. Specifies the socket read timeout, in seconds.   |
| <b>-socketwritetimeout &lt;int&gt;</b> | Optional. Specifies the socket write timeout, in seconds.  |
| <b>-shutdowntimeout &lt;int&gt;</b>    | Optional. Specifies the shutdown timeout for internal services, in seconds.  |
| <b>-pstartuptimeout &lt;int&gt;</b>    | Optional. Specifies the startup timeout for the detached process, in seconds.  |
| <b>-pshutdowntimeout &lt;int&gt;</b>   | Optional. Specifies the shutdown timeout for the detached process, in seconds.   |
| <b>-logfilename &lt;filename&gt;</b>   | Optional. Specifies the log file name to which the logger should log messages.   |
| <b>-loginfo &lt;0 or 1&gt;</b>         | Optional. Specifies if the logger should log "info" messages. Set to 0 for no, 1 for yes.  |
| <b>-logwarning &lt;0 or 1&gt;</b>      | Optional. Specifies if the logger should log "warning" messages. Set to 0 for no, 1 for yes.   |
| <b>-logerror &lt;0 or 1&gt;</b>        | Optional. Specifies if the logger should log "error" messages. Set to 0 for no, 1 for yes.   |
| <b>-logtrace &lt;0 or 1&gt;</b>        | Optional. Specifies if the logger should log "trace" messages. Set to 0 for no, 1 for yes.   |

| Option                        | Description   |
|-------------------------------|---|
| <b>-maxlogfilesize</b> <size> | Optional. Specifies the maximum log file size in KB.                                      |
| <b>-locallogger</b>           | Optional. Specifies that the Remote PED logger should be used, not the IS logging system. |

## Example

```
C:\Program Files\Safenet\LunaClient>pedClient -mode config -show
```

## pedclient -mode deleteid

Deletes a PED ID mapping between a specified Luna PED and PEDserver.

### Syntax

**pedclient -mode deleteid -id <PED\_ID> [-logfilename <filename>] [-loginfo <0 or 1>] [-logwarning <0 or 1>] [-logerror <0 or 1>] [-logtrace <0 or 1>] [-maxlogfilesize <size>] [-locallogger]**

| Option                               | Description  |
|--------------------------------------|--|
| <b>-id &lt;PED_ID&gt;</b>            | Specifies the ID of the PED to be deleted from the map.                                      |
| <b>-logfilename &lt;filename&gt;</b> | Optional. Specifies the log file name to which the logger should log messages.               |
| <b>-loginfo &lt;0 or 1&gt;</b>       | Optional. Specifies if the logger should log "info" messages. Set to 0 for no, 1 for yes.    |
| <b>-logwarning &lt;0 or 1&gt;</b>    | Optional. Specifies if the logger should log "warning" messages. Set to 0 for no, 1 for yes. |
| <b>-logerror &lt;0 or 1&gt;</b>      | Optional. Specifies if the logger should log "error" messages. Set to 0 for no, 1 for yes.   |
| <b>-logtrace &lt;0 or 1&gt;</b>      | Optional. Specifies if the logger should log "trace" messages. Set to 0 for no, 1 for yes.   |
| <b>-maxlogfilesize &lt;size&gt;</b>  | Optional. Specifies the maximum log file size in KB.   |
| <b>-locallogger</b>                  | Optional. Specifies that the Remote PED logger should be used, not the IS logging system.    |

### Example

```
C:\Program Files\Safenet\LunaClient>pedClient -mode deleteid -id 1234
```

## pedclient -mode releaseid

Releases a PED ID mapping from the HSM it was assigned to.

### Syntax

**pedclient -mode releaseid -id** <PED\_ID> [-logfilename <filename>] [-loginfo <0 or 1>] [-logwarning <0 or 1>] [-logerror <0 or 1>] [-logtrace <0 or 1>] [-maxlogfilesize <size>] [-locallogger]

| Option                         | Description  |
|--------------------------------|--|
| <b>-id</b> <PED_ID>            | Specifies the ID of the PED to be released.  |
| <b>-logfilename</b> <filename> | Optional. Specifies the log file name to which the logger should log messages.               |
| <b>-loginfo</b> <0 or 1>       | Optional. Specifies if the logger should log "info" messages. Set to 0 for no, 1 for yes.    |
| <b>-logwarning</b> <0 or 1>    | Optional. Specifies if the logger should log "warning" messages. Set to 0 for no, 1 for yes. |
| <b>-logerror</b> <0 or 1>      | Optional. Specifies if the logger should log "error" messages. Set to 0 for no, 1 for yes.   |
| <b>-logtrace</b> <0 or 1>      | Optional. Specifies if the logger should log "trace" messages. Set to 0 for no, 1 for yes.   |
| <b>-maxlogfilesize</b> <size>  | Optional. Specifies the maximum log file size in KB.   |
| <b>-locallogger</b>            | Optional. Specifies that the Remote PED logger should be used, not the IS logging system.    |

### Example

```
C:\Program Files\Safenet\LunaClient>pedClient -mode releaseid -id 1234
```



## pedclient -mode setid

Creates a PED ID mapping between a specified Luna PED and PEDserver.

### Syntax

**pedclient -mode setid -id <PED\_ID> -id\_ip <hostname> -id\_port <port> [-logfile <filename>] [-loginfo <0 or 1>] [-logwarning <0 or 1>] [-logerror <0 or 1>] [-logtrace <0 or 1>] [-maxlogfilesize <size>] [-locallogger]**

| Option                              | Description  |
|-------------------------------------|--|
| <b>-id &lt;PED_ID&gt;</b>           | Specifies the ID of the PED to be mapped.  |
| <b>-id_ip &lt;hostname&gt;</b>      | Specifies the IP address or hostname of the PEDserver to be linked with the PED ID.          |
| <b>-id_port &lt;port&gt;</b>        | Specifies the PED Server port to be linked with the PED ID.                                  |
| <b>-logfile &lt;filename&gt;</b>    | Optional. Specifies the log file name to which the logger should log messages.               |
| <b>-loginfo &lt;0 or 1&gt;</b>      | Optional. Specifies if the logger should log "info" messages. Set to 0 for no, 1 for yes.    |
| <b>-logwarning &lt;0 or 1&gt;</b>   | Optional. Specifies if the logger should log "warning" messages. Set to 0 for no, 1 for yes. |
| <b>-logerror &lt;0 or 1&gt;</b>     | Optional. Specifies if the logger should log "error" messages. Set to 0 for no, 1 for yes.   |
| <b>-logtrace &lt;0 or 1&gt;</b>     | Optional. Specifies if the logger should log "trace" messages. Set to 0 for no, 1 for yes.   |
| <b>-maxlogfilesize &lt;size&gt;</b> | Optional. Specifies the maximum log file size in KB.   |
| <b>-locallogger</b>                 | Optional. Specifies that the Remote PED logger should be used, not the IS logging system.    |

### Example

```
C:\Program Files\Safenet\LunaClient>pedClient -mode setid -id 1234 -id_ip myhostname -id_port 3456
```

## pedclient -mode show

Queries if PEDclient is currently running and gets details about PEDclient.

### Syntax

**pedclient -mode show** [-admin <admin port number>] [-eadmin <0 or 1>] [-socketreadtimeout <int>] [-socketwritetimeout <int>] [-logfilename <filename>] [-loginfo <0 or 1>] [-logwarning <0 or 1>] [-logtrace <0 or 1>] [-maxlogfilesize <size>] [-locallogger]

| Option                            | Description  |
|-----------------------------------|--|
| <b>-admin</b> <admin port number> | Optional. Specifies the administration port number to use.                                     |
| <b>-eadmin</b> <0 or 1>           | Optional. Specifies if the administration port is on "localhost" or on the external host name. |
| <b>-socketreadtimeout</b> <int>   | Optional. Specifies the socket read timeout, in seconds.                                       |
| <b>-socketwritetimeout</b> <int>  | Optional. Specifies the socket write timeout, in seconds.                                      |
| <b>-logfilename</b> <filename>    | Optional. Specifies the log file name to which the logger should log messages.                 |
| <b>-loginfo</b> <0 or 1>          | Optional. Specifies if the logger should log "info" messages. Set to 0 for no, 1 for yes.      |
| <b>-logwarning</b> <0 or 1>       | Optional. Specifies if the logger should log "warning" messages. Set to 0 for no, 1 for yes.   |
| <b>-logerror</b> <0 or 1>         | Optional. Specifies if the logger should log "error" messages. Set to 0 for no, 1 for yes.     |
| <b>-logtrace</b> <0 or 1>         | Optional. Specifies if the logger should log "trace" messages. Set to 0 for no, 1 for yes.     |
| <b>-maxlogfilesize</b> <size>     | Optional. Specifies the maximum log file size in KB.   |
| <b>-locallogger</b>               | Optional. Specifies that the Remote PED logger should be used, not the IS logging system.      |

### Example

```
C:\Program Files\Safenet\LunaClient>pedClient -mode show
```

## pedclient -mode start

Starts up the PEDclient.

### Syntax

```
pedclient -mode start [-winservice] [-eadmin <0 or 1>] [-idletimeout <int>] [-socketreadtimeout <int>] [-socketwritetimeout <int>] [-shutdowntimeout <int>] [-pstartuptimeout <int>] [-pshutdowntimeout <int>] [-logfilename <filename>] [-loginfo <0 or 1>] [-logwarning <0 or 1>] [-logtrace <0 or 1>] [-maxlogfilesize <size>] [-locallogger]
```

| Option                           | Description   |
|----------------------------------|---|
| <b>-winservice</b>               | Starts PEDclient for Windows service. The standard parameters used for <b>pedclient mode start</b> can be used for <b>pedclient mode start -winservice</b> as well. |
| <b>-eadmin</b> <0 or 1>          | Optional. Specifies if the administration port is on "localhost" or on the external host name.  |
| <b>-idletimeout</b> <int>        | Optional. Specifies the idle connection timeout, in seconds.  |
| <b>-socketreadtimeout</b> <int>  | Optional. Specifies the socket read timeout, in seconds.  |
| <b>-socketwritetimeout</b> <int> | Optional. Specifies the socket write timeout, in seconds.   |
| <b>-shutdowntimeout</b> <int>    | Optional. Specifies the shutdown timeout for internal services, in seconds.   |
| <b>-pstartuptimeout</b> <int>    | Optional. Specifies the startup timeout for the detached process, in seconds.   |
| <b>-pshutdowntimeout</b> <int>   | Optional. Specifies the shutdown timeout for the detached process, in seconds.  |
| <b>-logfilename</b> <filename>   | Optional. Specifies the log file name to which the logger should log messages.  |
| <b>-loginfo</b> <0 or 1>         | Optional. Specifies if the logger should log "info" messages. Set to 0 for no, 1 for yes.   |
| <b>-logwarning</b> <0 or 1>      | Optional. Specifies if the logger should log "warning" messages. Set to 0 for no, 1 for yes.  |
| <b>-logerror</b> <0 or 1>        | Optional. Specifies if the logger should log "error" messages. Set to 0 for no, 1 for yes.  |
| <b>-logtrace</b> <0 or 1>        | Optional. Specifies if the logger should log "trace" messages. Set to 0 for no, 1 for yes.  |
| <b>-maxlogfilesize</b> <size>    | Optional. Specifies the maximum log file size in KB.  |

| Option              | Description   |
|---------------------|---|
| <b>-locallogger</b> | Optional. Specifies that the Remote PED logger should be used, not the IS logging system. |

## Example

```
C:\Program Files\Safenet\LunaClient>pedClient -mode start
```

## pedclient -mode stop

Shuts down PEDclient.

### Syntax

**pedclient -mode stop** [-eadmin <0 or 1>] [-socketreadtimeout <int>] [-socketwritetimeout <int>] [-shutdowntimeout <int>] [-pstartuptimeout <int>] [-pshutdowntimeout <int>] [-logfilename <filename>] [-loginfo <0 or 1>] [-logwarning <0 or 1>] [-logtrace <0 or 1>] [-maxlogfilesize <size>] [-locallogger]

| Option                           | Description  |
|----------------------------------|--|
| <b>-eadmin</b> <0 or 1>          | Optional. Specifies if the administration port is on "localhost" or on the external host name. |
| <b>-socketreadtimeout</b> <int>  | Optional. Specifies the socket read timeout, in seconds.                                       |
| <b>-socketwritetimeout</b> <int> | Optional. Specifies the socket write timeout, in seconds.                                      |
| <b>-shutdowntimeout</b> <int>    | Optional. Specifies the shutdown timeout for internal services, in seconds.                    |
| <b>-pstartuptimeout</b> <int>    | Optional. Specifies the startup timeout for the detached process, in seconds.                  |
| <b>-pshutdowntimeout</b> <int>   | Optional. Specifies the shutdown timeout for the detached process, in seconds.                 |
| <b>-logfilename</b> <filename>   | Optional. Specifies the log file name to which the logger should log messages.                 |
| <b>-loginfo</b> <0 or 1>         | Optional. Specifies if the logger should log "info" messages. Set to 0 for no, 1 for yes.      |
| <b>-logwarning</b> <0 or 1>      | Optional. Specifies if the logger should log "warning" messages. Set to 0 for no, 1 for yes.   |
| <b>-logerror</b> <0 or 1>        | Optional. Specifies if the logger should log "error" messages. Set to 0 for no, 1 for yes.     |
| <b>-logtrace</b> <0 or 1>        | Optional. Specifies if the logger should log "trace" messages. Set to 0 for no, 1 for yes.     |
| <b>-maxlogfilesize</b> <size>    | Optional. Specifies the maximum log file size in KB.   |
| <b>-locallogger</b>              | Optional. Specifies that the Remote PED logger should be used, not the IS logging system.      |

### Example

```
C:\Program Files\Safenet\LunaClient>pedClient -mode stop
```

## pedclient -mode testid

Tests a PED ID mapping between a specified Luna PED and PEDserver.

### Syntax

**pedclient -mode testid -id <PED\_ID> [-logfile <filename>] [-loginfo <0 or 1>] [-logwarning <0 or 1>] [-logerror <0 or 1>] [-logtrace <0 or 1>] [-maxlogfilesize <size>] [-locallogger]**

| Option                              | Description  |
|-------------------------------------|--|
| <b>-id &lt;PED_ID&gt;</b>           | Specifies the ID of the PED to be tested.  |
| <b>-logfile &lt;filename&gt;</b>    | Optional. Specifies the log file name to which the logger should log messages.               |
| <b>-loginfo &lt;0 or 1&gt;</b>      | Optional. Specifies if the logger should log "info" messages. Set to 0 for no, 1 for yes.    |
| <b>-logwarning &lt;0 or 1&gt;</b>   | Optional. Specifies if the logger should log "warning" messages. Set to 0 for no, 1 for yes. |
| <b>-logerror &lt;0 or 1&gt;</b>     | Optional. Specifies if the logger should log "error" messages. Set to 0 for no, 1 for yes.   |
| <b>-logtrace &lt;0 or 1&gt;</b>     | Optional. Specifies if the logger should log "trace" messages. Set to 0 for no, 1 for yes.   |
| <b>-maxlogfilesize &lt;size&gt;</b> | Optional. Specifies the maximum log file size in KB.   |
| <b>-locallogger</b>                 | Optional. Specifies that the Remote PED logger should be used, not the IS logging system.    |

### Example

```
C:\Program Files\Safenet\LunaClient>pedClient -mode testid -id 1234
```

# CHAPTER 3: Audit Logging

Each event that occurs on the HSM can be recorded in the HSM event log, allowing you to audit your HSM usage. The HSM event log is viewable and configurable only by the **audit** user role. This **audit** role is disabled by default and must be explicitly enabled.

This chapter describes how to use audit logging to provide security audits of HSM activity. It contains the following sections:

- > ["Audit Logging General Advice and Recommendations" on page 121](#)
- > ["Logging In as Auditor" on page 124](#)
- > ["Configuring and Using Audit Logging" on page 125](#)
- > ["Remote Audit Logging" on page 130](#)
- > ["Changing the Auditor Credentials" on page 139](#)
- > ["Audit Log Categories and HSM Events" on page 140](#)
- > ["Audit Log Troubleshooting" on page 148](#)

## Audit Logging Features

The following list summarizes the functionality of the audit logging feature:

- > Log entries originate from the Luna Network HSM 7 (cryptographic module - the feature is implemented via HSM firmware (rather than in the library), for maximum security.
- > Log origin is assured.
- > Logs and individual records can be validated by any Luna Network HSM 7 that is a member of the same domain.
- > Audit Logging can be performed on password-authenticated and multifactor quorum-authenticated (both FIPS 140-3 level 3) configurations, but these configurations may not validate each other's logs - see the "same domain" requirement, above.

**NOTE** The "same domain" requirement still applies, but with the introduction of Extended Domain Management [ see [Universal Cloning](#) and [Domain Planning](#) ] (Partition Policy 44) in firmware version 7.8.0, you can change/add domains, such that the verifying HSM could be given the same domain as the original logging HSM.

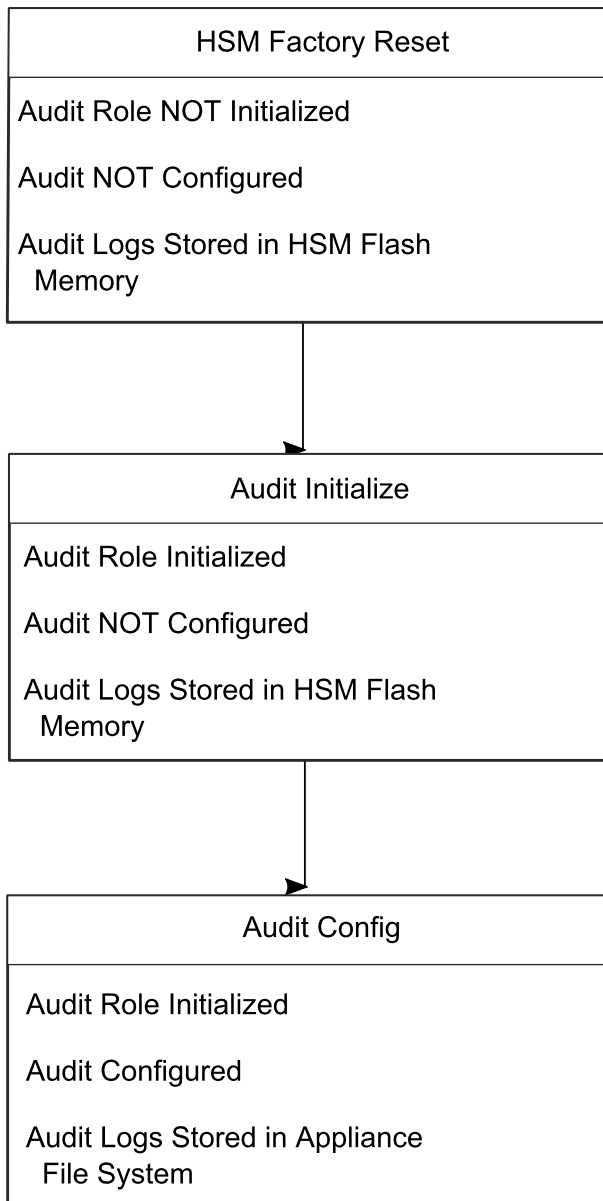
Thus, from Luna HSM firmware version 7.8.0 onward, it is possible

- for a Multifactor Quorum HSM log to be validated by a Password-authenticated HSM or
- for a Password-authenticated HSM log to be validated by a Multifactor Quorum HSM.

- > Each entry includes the following:
  - When the event occurred

- Who initiated the event (the authenticated entity)
  - What the event was
  - The result of the logging event (success, error, etc.)
- > Multiple categories of audit logging are supported, configured by the audit role.
- > Audit management is a separate role - the role creation does not require the presence or co-operation of the Luna Network HSM 7 SO.
- > The category of audit logging is configurable by (and only by) the audit role.
- > Audit log integrity is ensured against the following:
- Truncation - erasing part of a log record
  - Modification - modifying a log record
  - Deletion - erasing of the entire log record
  - Addition - writing of a fake log record
- > The following critical events are logged unconditionally, regardless of the state of the audit role (initialized or not):
- Tamper
  - Decommission
  - Zeroization
  - SO creation
  - Audit role creation



**Note:**

Logs are exported from the HSM's memory to the appliance's hard drive. Only an authenticated Auditor role is allowed to configure or initiate the export function. Therefore, an HSM in the Factory Reset state is **not** allowed to export log files from HSM memory to the appliance file system.

**Note:**

"audit log clear" clears logs only from the appliance file system. It does **not** affect logs stored in the HSM memory. Logs move out of HSM memory to the host file system, only when audit log rotation has been configured by the Auditor - so initialize and configure early to avoid log-entry build-up on the HSM.

**Types of events included in the logs**

The events that are included in the log is configurable by the audit role. The types of events that can be logged include the following:

- > log access attempts (logins)
- > log HSM management (init/reset/etc)
- > key management events (key create/delete)
- > asymmetric key usage (sig/ver)
- > first asymmetric key usage only (sig/ver)

- > symmetric key usage (enc/dec)
- > first symmetric key usage only (enc/dec)
- > log messages from CA\_LogExternal
- > log events relating to log configuration

Each of these events can be logged if they fail, succeed, or both.

### **Event log storage**

When the HSM logs an event, the log is stored on the HSM. The audit user cannot view these log entries. Before a log can be viewed, it must be rotated. Log rotation saves the log entries on the HSM to the HSM appliance, where they can be viewed. Log records are HMACed using an audit log secret to ensure their authenticity. The audit log secret is unique to the HSM where the log was created, and is required to view the HSM event logs. The secret can be exported, allowing you to view and verify the logs on another HSM.

**TIP** Log entries are stored in the cryptographic module (HSM) until they are rotated off. Log entries are not rotated out of the cryptographic module *until* the audit user is initialized and audit logging is configured. By default, even if there is no audit user or configuration, the cryptographic module logs unconditional events within its own memory, like:

- > zeroize
- > decommission
- > hardware tamper
- > card removal
- > etc.

If the crypto module internal space ever fills completely with log records,

- > whether slowly from unconditional logs, or
- > quickly from more volatile high-volume event recording,

...the HSM / cryptographic module would *stop all operations* that were not [audit init](#) and [audit config](#). The HSM would resume providing service only after the audit user cleared the logs.

To avoid that ever happening, configure audit logging to organize log parameters and handling, being sure to set sufficient frequency of rotation for the volume of record generation that you enable.

**Best practice** is to:

- > initialize the audit role as soon as the HSM is first powered on for production [audit init](#)
- > configure the log storage path on the external file system, along with the types of events to log, the rotation interval, etc. [audit config](#)
- > then, initialize the HSM Security Officer (this helps ensure that all messages, demanded by your auditing authority, are captured) [hsm init](#)
- > then, proceed with partition initialization and usage with your application(s)
- > then, *revisit* audit log configuration at regular intervals to tune the balance between
  - desired message types,
  - volume of audited actions normally performed (\*),
  - and so on
- > when you change behavior of the crypto module or change the types of events to audit, be sure to *revisit also* the rotation interval.

[\* Example, you might always want to record the generation of keys, but if usage of those keys is very high-volume (like in some signature use-cases), and thus would generate a high volume of log entries, it might be permissible, and prudent, to log only first-use of any key. Check with the relevant authority.]

### Audit log locations in the HSM appliance

When viewing HSM appliance information (like [status disk](#)), you might see mention of two log-file locations.

- > The folder `/var/audit` receives the HSM audit logs only. This is for HSM events and cryptographic operations. *No* information about host system events is logged here.
- > The folder `/var/log/audit` is for the appliance operating system (host system) audit logs. *No* information about cryptographic operations is logged here.

## Event logging impacts HSM performance

Each audit log record generated requires HSM resources. Configuring event logging to record most, or all, events may have an impact on HSM performance. You may need to adjust your logging configuration to provide adequate logging without significantly affecting performance. By default, only critical events are logged, imposing virtually no load on the HSM.

## Audit limitations and Controlled tamper recovery state

The following conditions apply when HSM Policy "48: Do controlled tamper recovery" is enabled (default setting).

- > Auditor (the Audit role) cannot verify the integrity of audit logs until after recovery from tamper.
- > Auditor cannot be initialized when the HSM is in controlled tamper recovery state.
- > Existing Audit role can login when in controlled tamper recovery state.
- > Existing Audit role cannot make audit config changes when in controlled tamper recovery state.
- > Existing Audit role cannot export the audit secret when in controlled tamper recovery state.

## The Audit Role

The audit logging function is controlled by two roles on Luna Network HSM 7, that must be used together:

- > The "audit" appliance account (use SSH or PuTTY to log in as "audit", instead of "admin", or "operator", or "monitor", etc.)
- > The "audit" HSM account (accessible only if you have logged into the appliance as "audit"; this account must be initialized)

On Luna Network HSM 7, the audit logging is managed by an audit user (an appliance system role), in combination with the HSM audit role, through a set of LunaSH commands. The audit user can perform only the audit-logging related tasks and self-related tasks. Other HSM appliance users, such as admin, operator, and monitor, have no access to the audit logging commands.

A default appliance (LunaSH) audit user is automatically created, but must be enabled. Upon first login, the audit user is asked to change their password. That appliance audit user would need to initialize the HSM audit role first, before being able to administer the audit logging. The Luna Network HSM 7 admin user can create more audit users when necessary.

To simplify configuration,

- > The maximum log file size is capped at 50 MB.
- > The log path is kept internal.
- > The rotation offset is set at 0.

## Audit User on the Appliance

The appliance audit user is a standard user account on Luna Network HSM 7, with default password "PASSWORD" (without the quotation marks). By default, the appliance audit user is disabled. Therefore, you must enable it in LunaSH before it becomes available. See [user enable](#) for the command syntax.

## Audit Role on the HSM

A Luna Network HSM 7 Audit role allows complete separation of Audit responsibilities from the HSM Security Officer (HSM SO), the Crypto Officer(or User), and other HSM roles. If the Audit role is initialized, the HSM and Partition SOs are prevented from working with the log files, and auditors are unable to perform administrative tasks on the HSM. As a general rule, the Audit role should be created before the HSM Security Officer role, to ensure that all important HSM operations (including those that occur during initialization), are captured.

Use the LunaSH command **audit init** to initialize the audit role, as described in [audit init](#).

## Password-authenticated HSMs

For Luna Network HSM 7s with Password Authentication, the auditor role logs into the HSM to perform their activities using a password. After initializing the Audit role on a password-authenticated HSM, log in as the Auditor and set the domain (see [role setdomain](#)). This step is required before setting logging parameters or the log filepath, or importing/exporting audit logs.

## Multifactor Quorum-authenticated HSMs

For Luna Network HSM 7s with multifactor quorum authentication, the auditor role logs into the HSM to perform their activities using the Audit (white) PED key.

## Role Initialization

Creating the Audit role (and imprinting the white PED key for multifactor quorum-authenticated HSMs) does not require the presence or cooperation of the HSM SO.

## Appliance Audit User Available Commands

The Audit role has a limited set of operations available to it, on the HSM, as reflected in the reduced command set available to the "audit" user when logged in to the shell (LunaSH).

```
login as: audit
audit@192.20.11.78's password:
Last login: Fri Mar 31 09:37:53 2020 from 10.124.0.31
```

```
Luna SA 7.7.0 Command Line Shell - Copyright (c) 2001-2020 SafeNet, Inc. All rights reserved.
```

```
lunash:>help
```

The following top-level commands are available:

| Name    | (short) | Description     |
|---------|---------|-----------------|
| help    | he      | Get Help        |
| exit    | e       | Exit Luna Shell |
| hsm     | hs      | > Hsm           |
| audit   | a       | > Audit         |
| my      | m       | > My            |
| network | n       | > Network       |

## Audit Log Secret

The HSM creates a log secret unique to the HSM, computed during the first initialization after manufacture. The log secret resides in flash memory (permanent, non-volatile memory), and is used to create log records that are sent to a log file. Later, the log secret is used to prove that a log record originated from a legitimate HSM and has

not been tampered with.

### Log Secret and Log Verification

The 256-bit log secret which is used to compute the HMACs is stored in the parameter area on the HSM. It is set the first time an event is logged. It can be exported from one HSM to another so that a particular sequence of log messages can be verified by the other HSM. Conversely, it can be imported from other HSMs for verification purpose.

To accomplish cross-HSM verification, the HSM generates a key-cloning vector (KCV, a.k.a. the Domain key) for the audit role when it is initialized. The KCV can then be used to encrypt the log secret for export to the HOST.

To verify a log that was generated on another HSM, assuming it is in the same domain, we simply import the wrapped secret, which the HSM subsequently decrypts; any records that are submitted to the host for verification will use this secret thereafter.

When the HSM exports the secret, it calculates a 32-bit checksum which is appended to the secret before it is encrypted with the KCV.

When the HSM imports the wrapped secret, it is decrypted, and the 32-bit checksum is calculated over the decrypted secret. If this doesn't match the decrypted checksum, then the secret that the HSM is trying to import comes from a system on a different domain, and an error is returned.

To verify a log generated on another HSM, in the same domain, the host passes to the target HSM the wrapped secret, which the target HSM subsequently decrypts; any records submitted to the target HSM for verification use this secret thereafter.

Importing a log secret from another HSM does not overwrite the target log secret because the operation writes the foreign log secret only to a separate parameter area for the wrapped log secret.

**CAUTION!** Once an HSM has imported a wrapped log secret from another HSM, it must export and then re-import its own log secret in order to verify its own logs again.

## Audit Log Records

A log record consists of two fields – the log message and the HMAC for the previous record. When the HSM creates a log record, it uses the log secret to compute the SHA256-HMAC of all data contained in that log message, plus the HMAC of the previous log entry. The HMAC is stored in HSM flash memory. The log message is then transmitted, along with the HMAC of the previous record, to the host. The host has a logging daemon to receive and store the log data on the host hard drive.

For the first log message ever returned from the HSM to the host there is no previous record and, therefore, no HMAC in flash. In this case, the previous HMAC is set to zero and the first HMAC is computed over the first log message concatenated with 32 zero-bytes. The first record in the log file then consists of the first log message plus 32 zero-bytes. The second record consists of the second message plus HMAC1 = HMAC (message1 || 0x0000). This results in the organization shown below.

|         |          |
|---------|----------|
| MSG 1   | HMAC 0   |
|         | ...      |
| MSG n-1 | HMAC n-2 |

|                      |            |
|----------------------|------------|
| MSG n                | HMAC n-1   |
| ...                  |            |
| MSG n+m              | HMAC n+m-1 |
| MSG n+m+1            | HMAC n+m   |
| ...                  |            |
| MSG end              | HMAC n+m-1 |
|                      |            |
| Recent HMAC in NVRAM | HMAC end   |

To verify a sequence of  $m$  log records which is a subset of the complete log, starting at index  $n$ , the host must submit the data illustrated above. The HSM calculates the HMAC for each record the same way as it did when the record was originally generated, and compares this HMAC to the value it received. If all of the calculated HMACs match the received HMACs, then the entire sequence verifies. If an HMAC doesn't match, then the associated record and all following records can be considered suspect. Because the HMAC of each message depends on the HMAC of the previous one, inserting or altering messages would cause the calculated HMAC to be invalid.

The HSM always stores the HMAC of the most-recently generated log message in flash memory. When checking truncation, the host would send the newest record in its log to the HSM; and, the HSM would compute the HMAC and compare it to the one in flash. If it does not match, then truncation has occurred.

## Audit Log Message Format

Each message is a fixed-length, comma delimited, and newline-terminated string. The table below shows the width and meaning of the fields in a message.

| Offset | Length (Chars) | Description                             |
|--------|----------------|---|
| 0      | 10             | Sequence number                         |
| 10     | 1              | Comma                                   |
| 11     | 17             | Timestamp                               |
| 28     | 1              | Comma                                   |
| 29     | 256            | Message text, interpreted from raw data |
| 285    | 1              | Comma                                   |
| 286    | 64             | HMAC of previous record as ASCII-HEX    |





## Log Capacity

The Luna Network HSM 7 appliance has approximately 220 GB of HDD capacity available for storing Audit logs. If you are logging everything the HSM does, this space can fill up completely over time if the Auditor does not periodically export logs off the appliance.

### LOG FULL condition

If you receive `CKR_LOG_FULL`, the log capacity has been reached, and all HSM operations will stop. This is to prevent the HSM from performing unlogged operations. In this condition, most HSM commands will not work; only commands that allow the Auditor to log in, clear the log storage, set the logging configuration, or reset the HSM to factory conditions are permitted.

See "[Copying Log Files Off the Appliance](#)" on page 128 for details of this recovery procedure.

## Configuration Persists Unless Factory Reset is Performed

Audit logging configuration is not removed or reset upon HSM re-initialization or a tamper event. Factory reset or HSM decommission will remove the Audit user and configuration. Logs must be cleared by specific command. Therefore, if your security regime requires decommission at end-of-life, or prior to shipping an HSM, then explicit clearing of HSM logs should be part of that procedure.

This is by design, as part of separation of roles in the HSM. When the Audit role exists, the HSM SO cannot modify the logging configuration, and therefore cannot hide any activity from auditors.

## NTLS is stopped but log still records LUNA\_OPEN\_SESSION/LUNA\_CLOSE\_SESSION messages

`LUNA_OPEN_SESSION` and `LUNA_CLOSE_SESSION` messages continue to appear in the audit logs, even though NTLS is stopped and applications cannot connect.

This is expected: inside the Luna Network HSM 7 appliance, a system state-of-health monitor routinely calls "hsm show", to ensure that the HSM is still functioning. Those calls trigger audit log messages.

## Audit Logging General Advice and Recommendations

The Security Audit Logging feature can produce a significant volume of data. It is expected, however, that Audit Officers will configure it properly for their specific operating environments. The data produced when the feature has been properly configured might be used for a number of reasons, such as:

- > Reconstructing a particular action or set of actions (forensics)
- > Tracing the actions of an application or individual user (accounting)
- > Holding a specific individual accountable for their actions (non-repudiation)

That last point represents the ultimate conclusion of any audit trail – to establish an irrefutable record of the chain of events leading up to a particular incident for the purpose of identifying and holding accountable the individual responsible. Not every organization will want to use security audit to meet the strict requirements of establishing such a chain of events. However, all security audit users will want to have an accurate representation of a particular sequence of events. To ensure that the audit log does contain an accurate representation of events and that it can be readily interpreted when it is reviewed, these basic guidelines should be followed after the audit logging feature has been properly configured:

- > Use a shell script to execute the `lunash:> audit sync` command at least once every 24 hours, provided the host has maintained its connection(s) to its configured NTP server(s).  
For newer firmware versions, that have HSM Policy **57 - Allow sync with host time**, you can initialize the time on the HSM, then set the policy on, to automatically sync the HSM with the local host every 24 hours.
- > Do not allow synchronization with the host's clock if the host has lost connectivity to NTP. This ensures that the HSM's internal clock is not set to a less accurate time than it has maintained internally. In general, the HSM's RTC will drift much less than the host's RTC and will, therefore, be significantly more accurate than the host in the absence of NTP.
- > Review logs at least daily and adjust configuration settings if necessary. It is important that any anomalies be identified as soon as possible and that the logging configuration that has been set is effective. If possible, use the remote logging feature to transmit log data to a Security Information and Event Management (SIEM) system to automatically analyze log data and identify anomalous events.
- > Execute `lunash:> audit log tarlogs` regularly to archive the audit logs and transfer them to a separate machine for long term storage. Also, execute `audit log clear` regularly to free up the audit log disk space on Luna Network HSM 7.
- > Consider installing and configuring a Luna PCIe HSM 7 in (or connected to) the remote log server to act as a "verification engine" for the remote log server. Ensure that the log secret for the operational HSM(s) has been shared with the log server verification HSM.

**NOTE** This is not always possible, unless you are physically copying the logs over from the .tgz archive. Because log records do not necessarily appear on the remote log server immediately, the HMAC might be incorrect. Also, if more than one Luna Network HSM 7 is posting log records to a remote server, this could interfere with record counts.

- > The audit log records are comma-delimited. We recommend that full use be made of the CSV formatting to import records into a database system or spreadsheet tool for analysis, if an SIEM system is not available.
- > The ASCII hex data representing the command and returned values and error code should be examined if an anomaly is detected in log review/analysis. It may be possible to match this data to the HSM's dual-port data. The dual-port, if it is available, will contain additional data that could be helpful in establishing the context surrounding the anomalous event. For example, if an unexpected error occurs it could be possible to identify the trace through the firmware subsystems associated with the error condition. This information would be needed to help in determining if the error was unexpected but legitimate or if it was forced in an attempt to exploit a potential weakness.

An important element of the security audit logging feature is the 'Log External' function. See [Audit Logging](#) for more information. For applications that cannot add this function call, it is possible to use `lunacm:> audit logmsg` within a startup script to insert a text record at the time the application is started.

**NOTE** Audit log and syslog entries are timestamped in UTC format.

## Disk Full

In the event that all the audit disk space is used up, audit logs are written to the HSM's small persistent memory. When the HSM's persistent memory is full, normal crypto commands will fail with "disk full" error.

To resolve that situation, the audit user must:

1. Archive the audit logs on the host side.

2. Move the audit logs to some other location for safe storage.
3. Clear the audit log directory.
4. Restart the callback service.

lunash:> **service restart cbs**

To prevent the "disk full" situation, we recommend that the audit user routinely archive the audit logs and clear the audit log directory.

**CAUTION!** If the HSM is zeroized when a "disk full" condition has occurred, HSM initialization will fail, preventing the user from clearing the logs. This will effectively lock out the appliance and RMA may be necessary.

**TIP** Log entries are stored in the cryptographic module (HSM) until they are rotated off. Log entries are not rotated out of the cryptographic module *until* the audit user is initialized and audit logging is configured. By default, even if there is no audit user or configuration, the cryptographic module logs unconditional events within its own memory, like:

- > zeroize
- > decommission
- > hardware tamper
- > card removal
- > etc.

If the crypto module internal space ever fills completely with log records,

- > whether slowly from unconditional logs, or
- > quickly from more volatile high-volume event recording,

...the HSM / cryptographic module would *stop all operations* that were not [audit init](#) and [audit config](#). The HSM would resume providing service only after the audit user cleared the logs.

To avoid that ever happening, configure audit logging to organize log parameters and handling, being sure to set sufficient frequency of rotation for the volume of record generation that you enable.

**Best practice** is to:

- > initialize the audit role as soon as the HSM is first powered on for production [audit init](#)
- > configure the log storage path on the external file system, along with the types of events to log, the rotation interval, etc. [audit config](#)
- > then, initialize the HSM Security Officer (this helps ensure that all messages, demanded by your auditing authority, are captured) [hsm init](#)
- > then, proceed with partition initialization and usage with your application(s)
- > then, *revisit* audit log configuration at regular intervals to tune the balance between
  - desired message types,
  - volume of audited actions normally performed (\*),
  - and so on
- > when you change behavior of the crypto module or change the types of events to audit, be sure to *revisit also* the rotation interval.

[\* Example, you might always want to record the generation of keys, but if usage of those keys is very high-volume (like in some signature use-cases), and thus would generate a high volume of log entries, it might be permissible, and prudent, to log only first-use of any key. Check with the relevant authority.]

## Logging In as Auditor

Before you can change the audit logging configuration, archive audit logs, or verify audit logs from another HSM, you must log in as Auditor (AU), or relevant commands will fail.

### To log in as Auditor

1. Connect to the appliance via SSH or a serial connection, and log in to LunaSH as **audit** or a custom user with an **audit** role (see [Logging In to LunaSH](#)).
2. Log in to the HSM.

```
lunash:> audit login
```

You are prompted for the Auditor credential.

### Failed Auditor Login Attempts

If you fail three (3) consecutive Auditor login attempts, the Auditor role is locked out for ten minutes.

**NOTE** The system must actually receive some erroneous/false information before it logs a failed attempt; if you merely forget to insert the PED key, or insert the wrong color key, that is not counted as a failed attempt. You must insert an incorrect PED key of the correct type, or enter an incorrect PIN or challenge secret, to fail a login attempt.

## Configuring and Using Audit Logging

This section describes the procedures required to enable audit logging, configure it to specify what is logged and how often the logs are rotated, and how to copy, verify and read the audit logs. It contains the following information:

- > ["Configuring Audit Logging" below](#)
- > ["Copying Log Files Off the Appliance" on page 128](#)
- > ["Exporting the Audit Logging Secret and Importing to a Verifying HSM" on page 129](#)
- > ["Audit Role Authentication Considerations" on page 130](#)

### Configuring Audit Logging

Configure audit logging using the LunaSH **audit** commands.

**NOTE** Audit log and syslog entries are timestamped in UTC format.

**TIP Performance and Audit Logging**

Secure Audit Logging consumes HSM resources, so consider minimizing the intensity of logging that you invoke.

For example, when choosing asymmetric key usage, you have the option to specify event values to record with **-value asymmetric** or **first**.

When choosing symmetric key usage logging you can opt for the corresponding **symmetric** and **symfirst**.

An HMAC is generated for each log, so **"first"** and **"symfirst"** record the first use of a key (asymmetric sig/ver or symmetric enc/dec respectively) and are much more sparing of HSM cycles, and therefore preferred to configuring for a log entry at every individual use of a given key -- unless that level of detailed logging is mandated.

**Prerequisites (HSM SO)**

1. Configure the Luna Network HSM 7 appliance to use the network time protocol (NTP). See [NTP on Luna Network HSM 7](#).
2. Log in to LunaSH as an admin-level user, and enable the audit user. The audit user is necessary to access and work with logs through the LunaSH interface. It is restricted from administrative functions:

```
lunash:> user enable -username audit
```

**To configure audit logging (Auditor)**

1. Using an SSH connection (or a local serial connection), login to LunaSH on the Luna Network HSM 7 appliance as **audit** (not as **admin**), using the password "PASSWORD".

The first time you login as **audit**, you are prompted to change the password to something more secure. To fulfill the purpose of the Audit role, keep the **audit** user's password separate from, and unknown to, the HSM Security Officer:

The audit user sees a reduced subset of commands suitable to the audit role, only, as follows:

| Name       | (short) | Description                            |
|------------|---------|--|
| init       | i       | Initialize the Audit role              |
| changePwd  | ch      | Change Audit User Password or PED Key  |
| login      | logi    | Login as the Audit user                |
| logout     | logo    | Logout the Audit user                  |
| config     | co      | Set Audit Parameters                   |
| sync       | sy      | Synchronize HSM Time to Host Time      |
| show       | sh      | Display the Audit logging info         |
| log        | l       | > Manage Audit Log Files               |
| secret     | se      | > Export/Import Audit Logging Secret   |
| remotehost | r       | > Configure Audit Logging Remote Hosts |

**NOTE** The **audit** user's commands are not available to the **admin** user. The **audit** user has no administrative control over the Luna Network HSM 7 appliance. This is a first layer in the separation of roles. This separation allows a user with no administrative control of the appliance and HSM to have oversight of the HSM logs, while also ensuring that an administrator cannot clear those logs.

- Initialize the **audit** role on the HSM. This enables logging for all subsequent actions performed by the HSM SO and partition user(s):

```
lunash:> audit init
```

- On password-authenticated HSMs, you are prompted for the password.
- On multifactor quorum-authenticated HSMs, you are referred to Luna PED, which prompts you for a blank or rewritable white Audit PED key.

- Now that the **audit** role exists on the HSM, you can configure the auditing function. However, before you can configure audit logging you must log into the HSM as the **audit** role:

```
lunash:> audit login
```

- On password-authenticated HSMs, you are prompted to enter the password for the audit role.
- On multifactor quorum-authenticated HSMs, you are referred to Luna PED, which prompts for the white PED key for the audit role.

**NOTE** You are now logged into the appliance as the **audit** user and into the HSM (within the appliance) as the **audit** role. Both are required. The **audit** commands, including HSM login as the **audit** role do not appear if you are logged in as any other named appliance-level user.

- Synchronize the HSM's clock with the host time (which should also be synchronized with the NTP server) so that all subsequent log records will have a valid and accurate timestamp:

```
lunash:> audit sync
```

- Configure audit logging to specify what you want to log. You can specify the level of audit appropriate for needs of the organization's policy and the nature of the application(s) using the HSM:

```
lunash:> audit config -parameter event -value <event_value>
```

**NOTE** The first time you configure audit logging, we suggest using only the **?** option, to see all the available options in the configuration process.

Security audits can generate a very large amount of data, which consumes HSM processing resources, host storage resources, and makes the job of the Audit Officer quite difficult when it comes time to review the logs. For this reason, ensure that you configure audit logging such that you capture only relevant data, and no more.

For example, the **First Symmetric Key Usage Only** or **First Asymmetric Key Usage Only** category is intended to assist Audit Officers to capture the relevant data in a space-efficient manner for high processing volume applications. On the other hand, a top-level Certificate Authority would likely be required, by policy, to capture all operations performed on the HSM but, since it is typically not an application that would see high volumes, configuring the HSM to audit all events would not impose a significant space and/or performance premium in that situation.

As a further example, `lunash:> audit config -parameter event -value all` will log everything the HSM does. This might be useful in some circumstances, but will quickly fill up log files.

- Configure audit logging to specify how often you want to rotate the logs:

```
lunash:> audit config -parameter rotation -value <value>
```

For example, `lunash:> audit config -parameter rotate -value hourly` would rotate the logs every hour, cutting down the size of individual log files, even in a situation of high-volume event recording, but would increase the number of files to be handled.

## Log Entries

Log entries are made within the HSM, and are written to the currently active log file on the appliance file system. When a log file reaches the rotation trigger, it is closed, and a new file gets the next log entry. The number of log files on the appliance grows according to the logging settings and the rotation schedule that you configured. At any time, you can copy files to a remote computer and then clear the originals from the HSM, if you wish to free the space.

For Luna Network HSM 7, to simplify configuration within its closed and hardened environment, the following rules apply:

- > The maximum log file size is capped at 50 MB.
- > The log path is internal to the Luna Network HSM 7 appliance.
- > The rotation offset is set at 0.

## Copying Log Files Off the Appliance

You can copy the log files off of the appliance for viewing and verification.

### To copy files off the appliance

1. Create an archive of the logs that are ready to archive:

```
lunash:> audit log tarlogs
```

2. View a list of the log files currently saved on the appliance:

```
lunash:> my file list
```

For this example, assume that the list includes a file named **audit.tgz**.

3. On the computer where you wish to capture and store the log files, use **pscp** or **scp** to transfer the file from the appliance:

```
/usr/safenet/lunaclient/logs :> pscp audit@myLunaHSM1:audit.tgz mylunsa1_audit_2014-02-28.tgz
```

Provide the audit user's credentials when prompted. This copies the identified file from the remote Luna Network HSM 7's file system (in the **audit** account) and stores the copy on your local computer file system with a useful name.

4. You can view and parse the plain-text portion of the file.
5. You can verify the authenticity of the retrieved file using a connected HSM to which you have imported the Audit logging secret from the originating Luna Network HSM 7.

6. On the appliance, you can now clear the audit log file system to make space for more audit logs.

```
lunash:> audit log clear
```

7. If you are clearing logs because of a **CKR\_LOG\_FULL** condition, the **cbs** service must also be restarted. The **audit** user is unable to access this command; the **admin** user must log in to LunaSH and restart the service.

```
lunash:> service restart cbs
```



## Exporting the Audit Logging Secret and Importing to a Verifying HSM

You can export the audit log secret from one HSM and import it to another to allow the first HSM's logs to be viewed and verified on the second. The HSMs must share the same authentication method and Audit cloning domain (password string or red PED key). You can verify logs from a Luna PCIe HSM 7 using a Luna Network HSM 7, and vice-versa.

### To export the Audit Logging secret from the HSM and import to the verifying HSM

1. On the Luna Network HSM 7 where HSM audit log files are being created, export the audit logging secret:

```
lunash:> audit secret export
```

The filename is displayed when the secret is exported. You can check the filename with [my file list](#).

2. On a computer connected to both HSMs, use **pscp** or **scp** to transfer the logging secret from the appliance.

- If you are planning to verify logs with a Luna PCIe HSM 7 or Luna USB HSM 7, you can use that HSM's host computer.
- If you are planning to verify logs with a second Luna Network HSM 7, you must transfer the logging secret to a client computer, and then to the second appliance.

```
<client_install_dir>:> pscp audit@<hostname_or_IP>:<log_secret_file> .
```

Then, if transferring to a second Luna Network HSM 7:

```
<client_install_dir>:> pscp <log_secret_file> audit@<hostname_or_IP>:
```

This copies the identified file from the remote Luna Network HSM 7's file system (in the **audit** account) and stores the copy on your local computer file system in the directory from which you issued the command. Provide the audit user's credentials when prompted.

3. Log in to the verifying HSM appliance as the **audit** user. For this example, we will assume that you have already initialized the HSM audit user role, using the same domain/secret as is associated with the source HSM.

- If you are using a Luna Network HSM 7, connect via SSH and log in to LunaSH as the **audit** user:

```
lunash:> audit login
```

- If you are using a Luna PCIe HSM 7 or Luna USB HSM 7, open LunaCM and log in using the Auditor role:

```
lunacm:> role login -name au
```

4. Import the audit logging secret to the HSM.

- Luna Network HSM 7 (LunaSH):

```
lunash:> audit secret import -serialtarget <target_HSM_SN> -serialsource <source_HSM_SN> -file <log_secret_file>
```

- Luna PCIe HSM 7 or Luna USB HSM 7 (LunaCM):

```
lunacm:> audit import file <log_secret_file>
```

5. You can now verify audit log files from the source HSM.

- Luna Network HSM 7 (LunaSH):

```
lunash:> audit log verify -file <audit_log_filename>.log
```

- Luna PCIe HSM 7 or Luna USB HSM 7 (LunaCM):

```
lunacm:> audit verify file <audit_log_filename>.log
```

You might need to provide the full path to the file, depending upon your current environment settings.

## Audit Role Authentication Considerations

- > The audit role PED key or password is a critical property to manage the audit logs. If that authentication secret is lost, the HSM must be factory reset (that is, zeroize the HSM) in order to initialize the audit role again.
- > Multiple bad logins produce different results for the HSM SO and for the audit role, as follows:
  - After 3 bad SO logins, the LUNA\_RET\_SO\_LOGIN\_FAILURE\_THRESHOLD error is returned and the HSM is zeroized.
  - After 3 bad audit logins, the LUNA\_RET\_AUDIT\_LOGIN\_FAILURE\_THRESHOLD error is returned, but the HSM is unaffected. If a subsequent login attempt is executed within 30 seconds, the LUNA\_RET\_AUDIT\_LOGIN\_TIMEOUT\_IN\_PROGRESS error is returned. If you wait for more than 30 seconds and try login again with the correct password, the login is successful.

## Remote Audit Logging

With Luna Network HSM 7, the audit logs can be sent to one or more remote logging servers. Either UDP or TCP protocol can be specified. The default is UDP and port 514. You might choose another port for syslog remote logging or audit remote logging, so that syslog and audit log do not conflict.

**NOTE** You or your network administrator will need to adjust your firewall to pass this traffic (iptables, firewallD, etc.).

Audit logging to the local file system or to a remote server requires that times be synchronized.

**HSM clock management by SO** - The Audit role has always been able to set time, and beginning with [Luna HSM Firmware 7.8.0](#) and newer, clock management can be performed by the HSM SO using `lunash hsm time get` and `hsm time sync` commands. These should be run to initialize the HSM clock time, then HSM Policy **57 - Allow sync with host time** should be set (ON) so that the one-time manual sync operation becomes a daily, automatic event to prevent HSM clock drift outside of parameters; note that it is OFF by default, for backward compatibility.

**NOTE** You can encounter the error CKR\_TIME\_NOT\_INITIALIZED if `lunash hsm time get` and `hsm time sync` commands have not been employed to set the time. As well, you could encounter CKR\_CLOCK\_NOT\_IN\_SYNC if the clocks on source and target HSMs are not within time tolerance for CPv4 cloning operations.

Additionally, other operations need HSM time properly set and synchronized - remote Audit logging, for example, expects tight drift control, to prevent log messages appearing out of order.

Clock synchronization, leading back to trusted time source, is needed on both the source HSM and the target.

## UDP Considerations

If you are using the UDP protocol for logging, the following statements are required in the `/etc/rsyslog.conf` file:

```
$ModLoad imudp
$InputUDPServerRun (PORT)
```

Possible approaches include the following:

> With templates:

```
$template AuditFile, "/var/log/luna/audit_remote.log"
if $syslogfacility-text == 'local3' then ?AuditFile;AuditFormat
```

> Without templates:

```
local3.* /var/log/audit.log;AuditFormat
```

> Dynamic filename:

```
$template DynFile, "/var/log/luna/%HOSTNAME%.log"
if $syslogfacility-text == 'local3' then ?DynFile;AuditFormat
```

**NOTE** The important thing to remember is that the incoming logs go to **local3**, and the port/protocol that is set on the Luna appliance must be the same that is set on the server running rsyslog.

## Example using TCP

The following example illustrates how to setup a remote Linux system to receive the audit logs using TCP:

1. Register the remote Linux system IP address or hostname with the Luna Network HSM 7:

```
lunash:> audit remothost add -host 192.20.9.160 -protocol tcp -port 1660
```

2. Modify the remote Linux system `/etc/rsyslog.conf` file to receive the audit logs:

```
$ModLoad imtcp
$InputTCPServerRun 514
$template AuditFormat, "%msg:F,94:2%\n"
#save log messages from Luna Network HSM 7
local3.* /var/log/luna/audit.log;AuditFormat
```

3. Modify the remote Linux system `/etc/sysconfig/rsyslog` file to receive the remote logs:

```
# Enables logging from remote machines. The listener will listen to the specified port.
SYSLOGD_OPTIONS="-r -m 0"
```

4. Restart the rsyslog daemon on the remote Linux system:

```
# service rsyslog restart
```

5. Monitor the audit logs on the remote Linux system:

```
# tail -f /var/log/luna/audit.log
```

## Mutual authentication with CA signed certificates.

- > The remote log server and the Luna Network HSM 7 appliance each generate a private key and CSR.
- > The remote log server and the Luna Network HSM 7 appliance add the received signed certificates.
- > The remote log server and Luna Network HSM 7 appliance add the CA certificate to their trust store.
- > User configures server information.

**Example: Configure a remote server with mutual authentication, tcp and CA-signed certificates****1. Generate a CSR.**

```
lunash:>audit remotehost cert gen -csr
```

**2. Export the CSR and sign it with the CA certificate.****3. At the CA server receive the CSR, sign the cert from the Luna Network HSM 7 appliance and return it.**

```
[CAserver]# scp operator@192.168.14.93:client_syslog_csr.csr .
[CAserver]# <CAserver-side command(s) to sign the cert>
[CAserver]# scp ca.pem operator@192.168.14.93:
[CAserver]# scp client_sign.pem operator@192.168.14.93:
```

**4. Add the CA certificate to the Luna Network HSM 7 appliance.**

```
lunash:>audit remotehost cert installCA ca.pem
```

```
Attempting to install ca.pem
```

```
CA certificate installed successfully.
```

```
The syslog service needs to be (re)started before a secure connection can be established.
```

```
Command Result : 0 (Success)
```

**5. Import the signed client certificate to the Luna Network HSM 7 appliance and add it.**

```
lunash:>audit remotehost cert install client_sign.pem
```

```
Attempting to install client_sign.pem
```

```
HSM certificate installed successfully.
```

```
The syslog service needs to be (re)started before a secure connection can be enabled.
```

```
Command Result : 0 (Success)
```

**6. Add the remote server configuration.**

```
lunash:>audit remotehost add -host 192.168.140.45 -protocol tcp -port 30007 -mode mutual -tls
```

```
Stopping syslog: [ OK ]
```

```
Starting syslog: [ OK ]
```

```
192.168.140.45 added successfully
```

```
Make sure the rsyslog service on 192.168.140.45 is properly configured to receive the logs
```

```
Command Result : 0 (Success)
```

**7. Execute a command in lunash and ensure that the log entry from the Luna Network HSM 7 appliance is received on the server.**

```
lunash:>audit remotehost list
```

```
Remote logging server(s):
```

```
=====
```

```
[192.168.140.45]:30007, tcp, tls
```

```
Command Result : 0 (Success)
```

...at the server...

```
Jun 21 14:25:37 192.168.141.93 [localhost] hsm[13889]: info : 0 : Command: audit remotehost list : admin : 192.168.106.144/62166
```

## Example of remote audit logging to same host as syslog (7.8.5 onward)

We show the actions of two sessions on the same appliance, to demonstrate remote syslog and remote audit log operating independently (as long as the shared-in-common log server certs and CA are available on the Luna Network HSM 7 appliance).

Recall that the admin user, opening an ssh session to the appliance has access and authority

- > to see and use [\*almost] any host-related commands as well as
- > to log into the cryptographic module to perform tasks as any HSM/crypto-module account for which the appliance admin possesses that role's authentication.

The exception is that the audit user logs into the appliance in its own ssh session and

- > has access to only a very limited set of appliance commands, and
- > can access the cryptographic module only as the HSM audit role, which can perform only audit-related operations within the crypto module.

1. For purpose of illustration, we provide a "clean" start, by having the admin user run a factory reset of the appliance's syslog service.

```
[[aa3312] lunash:>sysconf config factoryReset -service syslog -force  
Force option used. Proceed prompt bypassed.
```

```
Please be patient while the operation is running...  
Resetting service(s) to factory defaults:
```

```
-----  
syslog      :          succeeded
```

```
Command Result : 0 (Success)
```

```
aa3312] lunash:>syslog remotehost list
```

```
Remote logging server(s):  
=====
```

```
Command Result : 0 (Success)
```

So, now, no remote logging is going on, because no remote host is available to send to. Any certs and related configuration for the syslog service are gone.

2. Logging in as audit

```
[aa3312] lunash:>my file list
```

```
Command Result : 0 (Success)
```

```
[aa3312] lunash:>audit remotehost cert status
```

```
CA Certificate: Not Configured
```

```
HSM Certificate: Not Configured
HSM Private Key: Not Configured
```

```
Command Result : 0 (Success)
[aa3312] lunash:>audit remotehost cert gen -csr
```

```
CSR generated successfully.
```

```
Command Result : 0 (Success)
[aa3312] lunash:>my file list
```

```
1021 Jun 10 16:24 client_syslog_csr.csr
```

```
Command Result : 0 (Success)
[aa3312] lunash:>
```

### 3. The server receives the cert signing request, signs, and sends back to Luna Network HSM 7 appliance.

```
[root@aa1239]# scp -O audit@192.168.142.30:client_syslog_csr.csr .
[root@aa1239]# ./signWithCA.sh -f client_syslog_csr.csr -c ca.pem -k ca-key.pem
[root@aa1239]# scp -O client_sign.pem audit@192.168.142.30:
[root@aa1239]# scp -O ca.pem audit@192.168.142.30:
[root@aa1239]# ./setserver.sh -P relp -p 514 -m mutual -c ca -h 192.168142.30 -t
```

### 4. Back at the Luna Network HSM 7 appliance, the **audit** user receives and configures for remote audit logging.

```
[aa3312] lunash:>my file list
```

```
1176 Jun 10 16:26 ca.pem
1131 Jun 10 16:25 client_sign.pem
1021 Jun 10 16:24 client_syslog_csr.csr
```

```
Command Result : 0 (Success)
[aa3312] lunash:>audit remotehost cert status
```

```
CA Certificate: Not Configured
HSM Certificate: Not Configured
HSM Private Key: Configured
```

```
Command Result : 0 (Success)
[aa3312] lunash:>audit remotehost cert installcA ca.pem
```

```
Attempting to install ca.pem
```

```
Stopping syslog: [ OK ]
```

```
Starting syslog: [ OK ]
```

```
CA certificate installed successfully.
```

```
Command Result : 0 (Success)
[aa3312] lunash:>audit remotehost cert status
```

```
CA Certificate: Configured
HSM Certificate: Not Configured
HSM Private Key: Configured
```

```
Command Result : 0 (Success)
```

```
[aa3312] lunash:>audit remotehost cert install client_sign.pem

Attempting to install client_sign.pem

Stopping syslog: [ OK ]

Starting syslog: [ OK ]

HSM certificate installed successfully.

Command Result : 0 (Success)
[aa3312] lunash:>audit remotehost cert status

CA Certificate: Configured
HSM Certificate: Configured
HSM Private Key: Configured

Command Result : 0 (Success)
[aa3312] lunash:>audit remotehost add -host 192.168.140.45 -protocol relp -port 30007 -mode mutual -tls -name server.rsyslog.com

Stopping syslog: [ OK ]

Starting syslog: [ OK ]

192.168.140.45 added successfully
Make sure the rsyslog service on 192.168.140.45 is properly configured to receive the logs

Command Result : 0 (Success)
[aa3312] lunash:>audit remotehost list

Remote logging server(s):
=====

192.168.140.45:30007, relp, tls

Command Result : 0 (Success)
[aa3312] lunash:>

[aa3312] lunash:>audit login -p <audituserpassword>

Command Result : 0 (Success)

[aa3312] lunash:>audit remotehost cert status

CA Certificate: Configured
HSM Certificate: Configured
HSM Private Key: Configured

Command Result : 0 (Success)
[aa3312] lunash:>audit remotehost list

Remote logging server(s):
=====

192.168.140.45:30007, relp, tls
```

```
Command Result : 0 (Success)
[aa3312] lunash:>
```

At this point, remote audit logging is configured to proceed over port 30007.

The recent actions by audit user (the login to the HSM) generate log events that go out via port 30007.

```
2024-06-10T16:29:44.284899-04:00 aa3312 pedClient: ^      2841,24/06/10 20:29:42,S/N 521169
session 3
Access ae105c3103f20cf7 operation LUNA_LOGIN returned RC_OK(0x00000000) roleID=8 container=3

,D6B4FC3651332CC1D319C649B559363FEFC3F9B314A28C394FB4B5FB421F9ACF,190B004082600D003662676600
000000AE105C3103F20CF7D1F30700000000000300000000700000008000000000000000
16:29:47.214958 eno1 In IP (tos 0x0, ttl 64, id 13592, offset 0, flags [DF], proto TCP
(6), length 596)
  192.168.142.30.34242 > aa1239.lab.hsm.30007: Flags [P.], cksum 0x60e8 (correct), seq
1668:2224, ack 136, win 298, length 556
    0x0000:  4500 0254 3518 4000 4006 d448 0a7c 8e1e  E..T5.@.@..H.|..
    0x0010:  0a7c 8c2d 85c2 0202 c76a a769 166d 8be7  .|.-.....j.i.m..
    0x0020:  5018 012a 60e8 0000 1703 0302 2700 0000  P..*`.....'....
```

.... more deleted for space...

## 5. On the same Luna Network HSM 7 appliance, the **admin** user is looking at syslog.

```
[aa3312] lunash:>syslog remotehost cert status
```

```
CA Certificate: Configured
HSM Certificate: Configured
HSM Private Key: Configured
```

```
Command Result : 0 (Success)
```

```
[aa3312] lunash:>syslog remotehost list
```

```
Remote logging server(s):
=====
```

```
Command Result : 0 (Success)
```

```
[aa3312] lunash:>syslog remotehost add -host 192.168.140.45 -protocol tcp -port 30006 -mode
mutual -tls
```

```
Stopping syslog: [ OK ]
```

```
Starting syslog: [ OK ]
```

```
192.168.140.45 added successfully
```

Make sure the rsyslog service on 192.168.140.45 is properly configured to receive the logs

```
Command Result : 0 (Success)
```

```
[aa3312] lunash:>syslog remotehost list
```

```
Remote logging server(s):
=====
```

```
192.168.140.45:30006, tcp, tls
```



```
Command Result : 0 (Success)
[aa3312] lunash:>
```

Syslog for appliance/host events is configured and working on port 300006.

Remote syslog, and the previously configured remote audit logging are sharing the same certs and CA but are operating via different ports on the appliance.

## 6. We could verify by having each user run a command and we could then look at the logs on server aa1239.

First the audit user:

```
[aa3312] lunash:>audit login -p userpin123
```

```
Command Result : 0 (Success)
[aa3312] lunash:>
```

```
2024-06-10T17:03:35.746501-04:00 aa3312 pedClient: ^          3312,24/06/10 21:03:33,S/N 521169
session 3 Access ae105c3103f20cf7 operation LUNA_LOGIN returned RC_OK(0x00000000) roleID=8
container=3
```

```
,82CFC8ED542050F3BCE19EEC5B99C51837567BF9CBF8A355877800CF43A649BE,F00C004082600D00256A676600
000000AE105C3103F20CF7D1F30700000000000300000000700000008000000000000000
```

```
17:03:38.733018 eno1 In IP (tos 0x0, ttl 64, id 19234, offset 0, flags [DF], proto TCP
(6), length 597)
```

```
192.168.142.30.34386 > aa1239.lab.hsm.30007: Flags [P.], cksum 0xfbb5 (correct), seq
89473:90030, ack 8846, win 480, length 557
```

```
0x0000: 4500 0255 4b22 4000 4006 be3d 0a7c 8e1e E..UK"@.@.=.|..
```

```
0x0010: 0a7c 8c2d 8652 0202 7f5d 8f6b 32ba 7abb .|.-.R...].k2.z.
```

```
0x0020: 5018 01e0 fbb5 0000 1703 0302 2800 0000 P.....(...
```

... more, trimmed for space...

Then the appliance admin user:

```
[aa3312] lunash:>syslog remotehost list
```

```
Remote logging server(s):
```

```
=====
```

```
192.168.140.45:30006, tcp, tls
```

```
Command Result : 0 (Success)
[aa3312] lunash:>
```

```
2024-06-10T17:05:00-04:00 aa3312 hsm[18834]: info : 0 : Command: syslog remotehost list :
admin : 10.105.188.126/58071
```

```
192.168.142.30.34012 > aa1239.lab.hsm.30006: Flags [P.], cksum 0xde22 (correct), seq
432:576, ack 1, win 252, length 144
```

```
0x0000: 4500 00b8 19a4 4000 4006 f158 0a7c 8e1e E.....@.@..X.|..
```

```
0x0010: 0a7c 8c2d 84dc 7536 a640 e683 f507 15fb .|.-..u6.@.....
```

```
0x0020: 5018 00fc de22 0000 1703 0300 8b00 0000 P....".....
```

```
0x0030: 0000 0000 0720 5ef1 84ab 843e 6c86 e748 .....^.....>1..H
```

```
0x0040: c601 0b74 d9ee 0a72 2d35 e68d 902b 5c9d ...t...r-5...+\.
```

```
0x0050: 5846 3af6 8b8f 030f 1f16 e647 034f 841e XF:.....G.O..
```

```
0x0060: 49eb 0704 7455 89d4 c1d3 a155 dc34 191c I...tU.....U.4..
```

```
0x0070: 41eb 8fa0 d66e b733 7c64 23f0 c239 86bd A....n.3|d#..9..
```

```
0x0080: 128a 2db0 fc99 5329 879c 24c7 ce8e b546 ..-...S)$.$$$F
```

```
0x0090: a560 42cf 4e70 adac b0ec cb76 09f0 52cc .`B.Np.....v..R.
```

```
0x00a0: 2a7f 0a92 35db 3f61 cd80 c352 4e57 5ccd *...5.?a...RNW\.
```

```
0x00b0: 8aef bla3 4e49 6354 ....NIcT
```

7. Now (only for demonstration purposes), the audit user in their ssh session deletes their remote server configuration (using port 30007).

```
[aa3312] lunash:>audit remotehost delete -host 192.168.140.45 -port 30007
```

```
WARNING! This action will delete the remote server configuration for 192.168.140.45 with
port 30007.
```

```
If you are sure that you wish to proceed, then type 'proceed', otherwise type 'quit'
```

```
> proceed
```

```
Proceeding...
```

```
Stopping syslog: [ OK ]
```

```
Starting syslog: [ OK ]
```

```
Command Result : 0 (Success)
```

```
[aa3312] lunash:>audit remotehost list
```

```
Remote logging server(s):
```

```
=====
```

```
Command Result : 0 (Success)
```

```
[aa3312] lunash:>
```

8. The audit user no longer has remote logging configured. How about the admin user and remote syslogging for appliance (non-crypto module) events?

```
[aa3312] lunash:>syslog remotehost list
```

```
Remote logging server(s):
```

```
=====
```

```
192.168.140.45:30006, tcp, tls
```

```
Command Result : 0 (Success)
```

```
[aa3312] lunash:>
```

Syslog still has its connection, and logs are still being sent via port 30006

```
2024-06-10T17:06:47-04:00 aa3312 hsm[18834]: info : 0 : Command: syslog remotehost list :
admin : 192.168.188.126/58071
```

```
192.168.142.30.34022 > aa1239.lab.hsm.30006: Flags [P.], cksum 0x59f7 (correct), seq
1590:1734, ack 1552, win 252, length 144
```

```
0x0000: 4500 00b8 b6ba 4000 4006 5442 0a7c 8e1e E.....@.@.TB.|..
0x0010: 0a7c 8c2d 84e6 7536 1423 61a4 aba4 9e64 .|.-..u6.#a....d
0x0020: 5018 00fc 59f7 0000 1703 0300 8b00 0000 P...Y.....
0x0030: 0000 0000 02d1 7276 4c90 e88d cb9e a410 .....rvL.....
0x0040: cef1 53a2 95ed 2e37 931d 071b ceb9 5856 ..S....7.....XV
0x0050: cc81 5d97 4d72 9302 4024 9ba3 d3a9 4640 ..].Mr..@$....F@
0x0060: 0d4e 3946 c9b2 b58a 1535 1c08 4a1f 5f59 .N9F.....5..J._Y
0x0070: 22b7 43a3 850b 07a4 1ca7 57fd b428 6157 ".C.....W..(aW
0x0080: 7359 4fe5 0b99 f8b2 6220 3979 9bac b3ec sYO.....b.9y....
0x0090: 8398 91af 6edb ca03 d693 518c 75bd a0bf .....n.....Q.u...
0x00a0: 8256 93a9 0e74 9199 9d05 499f f1f8 4b1d .V...t....I...K.
0x00b0: 6572 a435 b0af 1265 er.5....e
```

```
[aa3312] lunash:>audit login -p userpin123
```

```
Command Result : 0 (Success)
[aa3312] lunash:>
```

```
2024-06-10T17:07:41-04:00 aa3312 hsm[18390]: info : 0 : Command: audit login -password * :
audit : 10.105.188.126/58070
```

```
192.168.142.30.34022 > aa1239.lab.hsm.30006: Flags [P.], cksum 0x2a3e (correct), seq
2118:2262, ack 1552, win 252, length 144
```

```
0x0000: 4500 00b8 b6be 4000 4006 543e 0a7c 8e1e E.....@.@.T>.|..
0x0010: 0a7c 8c2d 84e6 7536 1423 63b4 aba4 9e64 .|.-..u6.#c....d
0x0020: 5018 00fc 2a3e 0000 1703 0300 8b00 0000 P...*>.....
0x0030: 0000 0000 0686 c0ef 967f f629 0582 e004 .....)....
0x0040: 880d 7344 218e d76d 1ec0 5767 fdb3 126e ..sD!..m..Wg...n
0x0050: ab7a 7391 f381 a595 fa12 8df3 88c4 7934 .zs.....y4
0x0060: ad57 d6f7 4039 2030 2def cbf2 2b06 018e .W..@9.0-...+...
0x0070: 7fca 9716 cab5 a23f 37a8 0cd0 5d7f db20 .....?7...]...
0x0080: 56af 8ea8 3ff7 03e1 aa51 2c42 3d64 f33c V...?....Q,B=d.<
0x0090: b327 f771 b7ab e6e5 fad0 c934 6060 994a .'q.....4``.J
0x00a0: 5f7e aeb6 ea49 7485 575e 4ca1 379f 121d _~...It.W^L.7...
0x00b0: 127d 3b6d 945d 7cf5 .};m.}||.
```

And, events (like login) are still being logged via syslog, and out via port 30006, because the certs and CA are available on the appliance, but no more HSM audit logs are being sent via port 30007. Deleting the configuration of one (without removing the certs and CA) does not have any impact on the operation of the other's remote logging.

## Changing the Auditor Credentials

Two auditor credentials can be changed, as needed:

- > the appliance audit role (to authenticate an SSH or serial connection to access appliance-level Luna Shell commands)
- > the HSM audit role (to authenticate to the cryptographic module within the HSM security appliance)

From time to time, it might be necessary to change the secret associated with a role on an HSM appliance, a role on an HSM or a partition of an HSM, or a cloning domain secret. Reasons for changing credentials include:

- > Regular credential rotation as part of your organization's security policy
- > Compromise of a role or secret due to loss or theft of a PED key
- > Personnel changes in your organization or changes to individual security clearances
- > Changes to your security scheme (implementing/revoking M of N, PINs, or shared secrets)

The Auditor can change their own credentials at any time.

To help differentiate the terms used in this context:

- > the *functional position* in your organization is the "auditor";
- > the *credentialed roles*, for
  - the appliance level, controlling Luna Shell (lunash:>) access via ssh or serial connection, and

- the cryptographic module within the HSM security appliance

are both called "audit", but that is two separate levels of access (might be for a single person doing audit configuration and management duties or might be multiple persons, including quorum iKey holders for PED-auth HSMs), and therefore [should be] two different secrets.

### To change/rotate the appliance auditor credential

1. Connect to the appliance via SSH or a serial connection, and log in to LunaSH as **audit** or a custom user with an **audit** role (see [Logging In to LunaSH](#) ).
2. Change the current appliance user's (audit) role password.

```
lunash:>my password set
```

### To change the HSM cryptographic module auditor credential

1. Connect to the appliance via SSH or a serial connection, and log in to LunaSH as **audit** or a custom user with an **audit** role (see [Logging In to LunaSH](#) ).
2. Log into the cryptographic module as the audit HSM role (see "[Logging In as Auditor](#)" on page 124).
3. Change the Auditor credential.

```
lunash:> audit changepwd
```

You are prompted for the current Auditor credential, and then to create a new one.

## Audit Log Categories and HSM Events

This section provides a summary of the audit log categories and their associated HSM events.

### Partition Role IDs

If you are using a Luna Network HSM 7 with [Luna HSM Firmware 7.7.0](#) or newer and [Luna HSM Client 10.3.0](#) or newer, the HSM event log reports events with the following IDs assigned to each partition role:

#### Administrative Partition Role IDs

| Partition Role       | Role ID |
|----------------------|---------|
| Administrator        | 0       |
| HSM Security Officer | 1       |
| Auditor              | 8       |

## Application Partition Role IDs

| Partition Role             | Role ID |
|----------------------------|---------|
| Partition Security Officer | 1       |
| Crypto Officer             | 0       |
| Limited Crypto Officer     | 9       |
| Crypto User                | 5       |

## HSM Access

| HSM Event               | Description  |
|-------------------------|--|
| LUNA_LOGIN              | C_Login.<br>This event must be allowed to proceed even if the result should be logged but cannot (for example, due to a log full condition).       |
| LUNA_LOGOUT             | C_Logout.<br>This event must be allowed to proceed even if the result should be logged but cannot (for example, due to a log full condition).      |
| LUNA_LOGOUT_OTHER       | C_LogoutOther.<br>This event must be allowed to proceed even if the result should be logged but cannot (for example, due to a log full condition). |
| LUNA_MODIFY_OBJECT      | C_SetAttributeValue  |
| LUNA_OPEN_SESSION       | C_OpenSession.<br>This event must be allowed to proceed even if the result should be logged but cannot (for example, due to a log full condition). |
| LUNA_CLOSE_ALL_SESSIONS | C_CloseAllSessions   |
| LUNA_CLOSE_SESSION      | C_CloseSession<br>This event must be allowed to proceed even if the result should be logged but cannot (for example, due to a log full condition). |
| LUNA_OPEN_ACCESS        | CA_OpenApplicationID   |
| LUNA_CLEAN_ACCESS       | CA_Restart, CA_RestartForContainer   |
| LUNA_CLOSE_ACCESS       | CA_CloseApplicationID  |

| HSM Event                         | Description   |
|-----------------------------------|---|
| LUNA_LOAD_CUSTOM_MODULE           | CA_LoadModule   |
| LUNA_LOAD_ENCRYPTED_CUSTOM_MODULE | CA_LoadEncryptedModule  |
| LUNA_UNLOAD_CUSTOM_MODULE         | CA_UnloadModule   |
| LUNA_EXECUTE_CUSTOM_COMMAND       | CA_PerformModuleCall  |
| LUNA_HA_LOGIN                     | CA_HAGetLoginChallenge,<br>CA_HAAnswerLoginChallenge,<br>CA_HALogin,<br>CA_HAAnswerMofNChallenge,<br>HAActivateMofN |

## Log External

| HSM Event         | Description    |
|-------------------|----------------|
| LUNA_LOG_EXTERNAL | CA_LogExternal |

## HSM Management

| HSM Event             | Description  |
|-----------------------|--|
| LUNA_ZEROIZE          | CA_FactoryReset<br>This event is logged unconditionally. |
| LUNA_INIT_TOKEN       | C_InitToken<br>This event is logged unconditionally.     |
| LUNA_SET_PIN          | C_SetPIN   |
| LUNA_INIT_PIN         | C_InitPIN  |
| LUNA_CREATE_CONTAINER | CA_CreateContainer                                       |
| LUNA_DELETE_CONTAINER | CA_DeleteContainer, CA_DeleteContainerWithHandle         |
| LUNA_SEED_RANDOM      | C_SeedRandom   |

| HSM Event                       | Description                     |
|---------------------------------|---------------------------------|
| LUNA_EXTRACT_CONTEXTS           | C_GetOperationState             |
| LUNA_INSERT_CONTEXTS            | C_SetOperationState             |
| LUNA_SELF_TEST                  | C_PerformSelfTest               |
| LUNA_LOAD_CERT                  | CA_SetTokenCertificateSignature |
| LUNA_HA_INIT                    | CA_HAInit                       |
| LUNA_SET_HSM_POLICY             | CA_SetHSMPolicy                 |
| LUNA_SET_DESTRUCTIVE_HSM_POLICY | CA_SetDestructiveHSMPolicy      |
| LUNA_SET_CONTAINER_POLICY       | CA_SetContainerPolicy           |
| LUNA_SET_CAPABILITY             | Internal, for capability update |
| LUNA_CREATE_LOGIN_CHALLENGE     | CA_CreateLoginChallenge         |
| LUNA_REQUEST_CHALLENGE          | CA_SIMInsert, CA_SIMMultiSign   |
| LUNA_PED_INIT_RPV               | CA_InitializeRemotePEDVector    |
| LUNA_PED_DELETE_RPV             | CA_DeleteRemotePEDVector        |
| LUNA_MTK_LOCK                   | Internal, for manufacturing     |
| LUNA_MTK_UNLOCK_CHALLENGE       | Internal, for manufacturing     |
| LUNA_MTK_UNLOCK_RESPONSE        | Internal, for manufacturing     |
| LUNA_MTK_RESTORE                | CA_MTKRestore                   |
| LUNA_MTK_RESPLIT                | CA_MTKResplit                   |
| LUNA_MTK_ZEROIZE                | CA_MTKZeroize                   |
| LUNA_FW_UPGRADE_INIT            | CA_FirmwareUpdate               |
| LUNA_FW_UPGRADE_UPDATE          | CA_FirmwareUpdate               |
| LUNA_FW_UPGRADE_FINAL           | CA_FirmwareUpdate               |
| LUNA_FW_ROLLBACK                | CA_FirmwareRollback             |

| HSM Event               | Description         |
|-------------------------|---------------------|
| LUNA_MTK_SET_STORAGE    | CA_MTKSetStorage    |
| LUNA_SET_CONTAINER_SIZE | CA_SetContainerSize |

## Key Management

| HSM Event  | Description  |
|--|--|
| LUNA_CREATE_OBJECT                                       | C_CreateObject                                     |
| LUNA_COPY_OBJECT   | C_CopyObject                                       |
| LUNA_DESTROY_OBJECT                                      | C_DestroyObject                                    |
| LUNA_DESTROY_MULTIPLE_OBJECTS                            | CA_DestroyMultipleObjects                          |
| LUNA_GENERATE_KEY  | C_GenerateKey                                      |
| LUNA_GENERATE_KEY_PAIR                                   | C_GenerateKeyPair                                  |
| LUNA_WRAP_KEY  | C_WrapKey  |
| LUNA_UNWRAP_KEY  | C_UnwrapKey  |
| LUNA_DERIVE_KEY  | C_DeriveKey  |
| LUNA_GET_RANDOM  | C_GenerateRandom                                   |
| LUNA_CLONE_AS_SOURCE, LUNA_REPLICATE_AS_SOURCE           | CA_CloneAsSource                                   |
| LUNA_CLONE_AS_TARGET_INIT, LUNA_REPLICATE_AS_TARGET_INIT | CA_CloneAsTargetInit                               |
| LUNA_CLONE_AS_TARGET, LUNA_REPLICATE_AS_TARGET           | CA_CloneAsTarget                                   |
| LUNA_GEN_TKN_KEYS  | CA_GenerateTokenKeys                               |
| LUNA_GEN_KCV   | CA_ManualKCV, C_InitPIN, C_InitToken, CA_InitAudit |
| LUNA_SET_LKCV  | CA_SetLKCV   |



| HSM Event               | Description   |
|-------------------------|---|
| LUNA_M_OF_N_GENERATE    | CA_GenerateMofN_Common, CA_GenerateMofN   |
| LUNA_M_OF_N_ACTIVATE    | CA_ActivateMofN   |
| LUNA_M_OF_N_MODIFY      | CA_ActivateMofN   |
| LUNA_EXTRACT            | CA_Extract  |
| LUNA_INSERT             | CA_Insert   |
| LUNA_LKM_COMMAND        | CA_LKMInitiatorChallenge,<br>CA_LKMReceiverResponse,<br>CA_LKMInitiatorComplete,<br>CA_LKMReceiverComplete. |
| LUNA_MODIFY_USAGE_COUNT | CA_ModifyUsageCount   |

## Key Usage and Key First Usage

| HSM Event         | Description    |
|-------------------|----------------|
| LUNA_ENCRYPT_INIT | C_EncryptInit  |
| LUNA_ENCRYPT      | C_Encrypt      |
| LUNA_ENCRYPT_END  | C_EncryptFinal |
| LUNA_DECRYPT_INIT | C_DecryptInit  |
| LUNA_DECRYPT      | C_Decrypt      |
| LUNA_DECRYPT_END  | C_DecryptFinal |
| LUNA_DIGEST_INIT  | C_DigestInit   |
| LUNA_DIGEST       | C_Digest       |
| LUNA_DIGEST_KEY   | C_DigestKey    |
| LUNA_DIGEST_END   | C_DigestFinal  |
| LUNA_SIGN_INIT    | C_SignInit     |
| LUNA_SIGN         | C_Sign         |

| HSM Event               | Description         |
|-------------------------|---------------------|
| LUNA_SIGN_END           | C_SignFinal         |
| LUNA_VERIFY_INIT        | C_VerifyInit        |
| LUNA_VERIFY             | C_Verify            |
| LUNA_VERIFY_END         | C_VerifyFinal       |
| LUNA_SIGN_SINGLEPART    | C_Sign              |
| LUNA_VERIFY_SINGLEPART  | C_Verify            |
| LUNA_WRAP_CSP           | CA_CloneMofN_Common |
| LUNA_M_OF_N_DUPLICATE   | CA_DuplicateMofN    |
| LUNA_ENCRYPT_SINGLEPART | C_Encrypt           |
| LUNA_DECRYPT_SINGLEPART | C_Decrypt           |

## Per-Key Authorization

| HSM Event                        | Description                                 |
|----------------------------------|---|
| LUNA_AUTHORIZE_KEY               | <a href="#">CA_AuthorizeKey</a>             |
| LUNA_SET_AUTHORIZATION_DATA      | <a href="#">CA_SetAuthorizationData</a>     |
| LUNA_RESET_AUTHORIZATION_DATA    | <a href="#">CA_ResetAuthorizationData</a>   |
| LUNA_ASSIGN_KEY                  | <a href="#">CA_AssignKey</a>                |
| LUNA_INCREMENT_FAILED_AUTH_COUNT | <a href="#">CA_IncrementFailedAuthCount</a> |

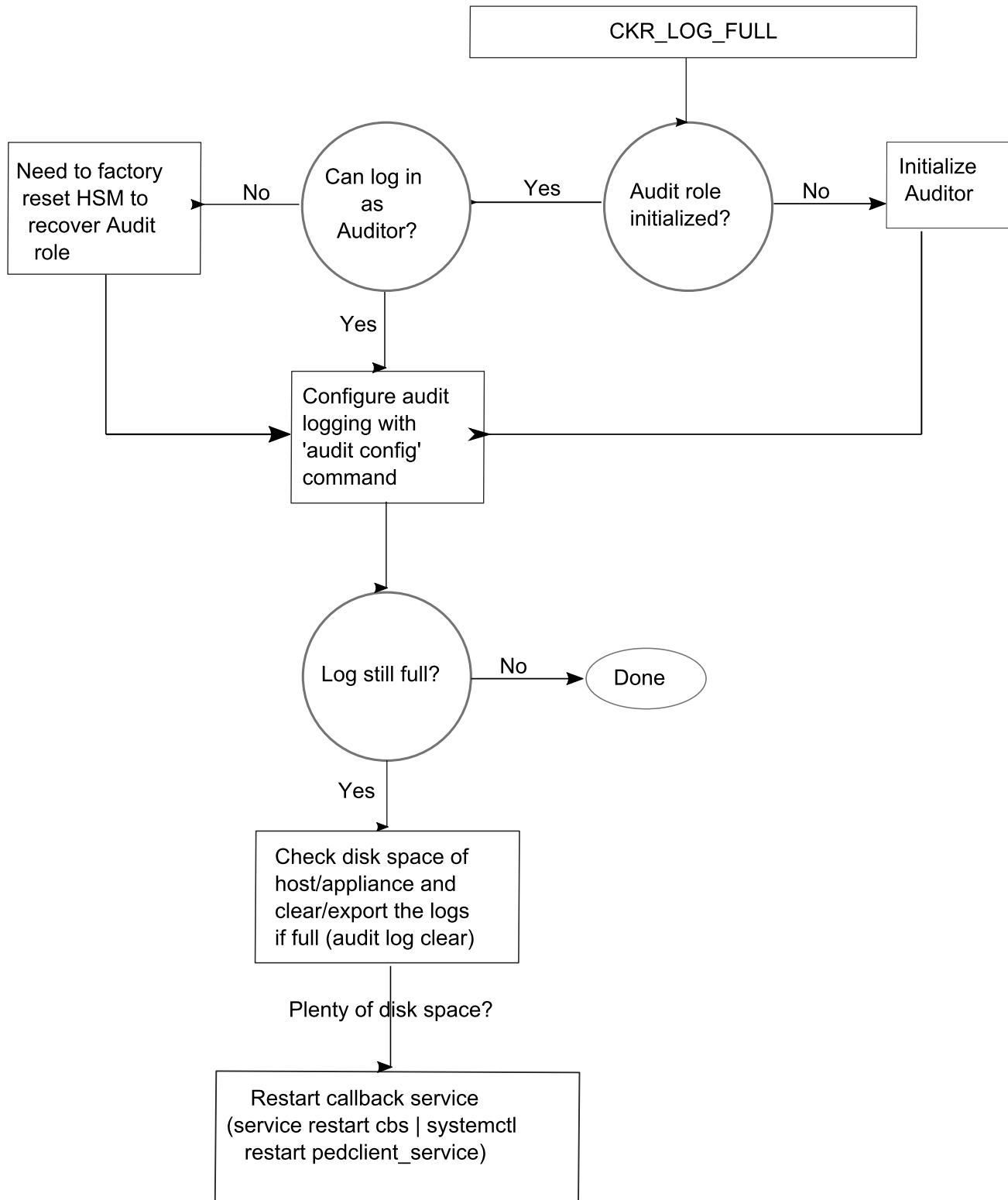
## Audit Log Management

| HSM Event         | Description |
|-------------------|-------------|
| LUNA_LOG_SET_TIME | CA_TimeSync |
| LUNA_LOG_GET_TIME | CA_GetTime  |

| HSM Event                      | Description   |
|--------------------------------|---|
| LUNA_LOG_SET_CONFIG            | CA_LogSetConfig<br>This event must be allowed to proceed even if the result should be logged but cannot (for example, due to a log full condition). |
| LUNA_LOG_GET_CONFIG            | CA_LogGetConfig<br>This event must be allowed to proceed even if the result should be logged but cannot (for example, due to a log full condition). |
| LUNA_LOG_VERIFY                | CA_LogVerify  |
| LUNA_CREATE_AUDIT_CONTAINER ** | CA_InitAudit<br>The event is logged unconditionally.  |
| LUNA_LOG_IMPORT_SECRET         | CA_LogImportSecret  |
| LUNA_LOG_EXPORT_SECRET         | CA_LogExportSecret  |

## Audit Log Troubleshooting

The following sequence might help for problems with audit logging, like "log full."



# CHAPTER 4: Initializing the HSM

Initialization prepares a new HSM for use, or an existing HSM for reuse. You must initialize the HSM before you can generate or store objects, allow clients to connect, or perform cryptographic operations:

- > On a new or factory-reset HSM, initialization sets the HSM SO credentials, the HSM label, and the cloning domain of the HSM Admin partition. This is often referred to as a 'hard' initialization. See ["Initializing a New or Factory-reset HSM"](#) below.
- > On an initialized HSM, re-initialization destroys all existing partitions and objects, but retains the SO credentials and cloning domain. You have the option to change or retain the existing label. This is often referred to as a 'soft' initialization. See ["Re-initializing the HSM"](#) on page 152.

**NOTE** To ensure accurate auditing, perform initialization only after you have set the system time parameters (time, date, time zone, use of NTP (Network Time Protocol)). You can use the `-authtimeconfig` option when initializing the HSM to require HSM SO authorization of any time-related changes once the HSM is initialized.

## Hard versus soft initialization

The following table summarizes the differences between a hard and soft initialization.

| Condition/Effect               | Soft init | Hard init                  |
|--------------------------------|-----------|----------------------------|
| HSM SO authentication required | Yes       | No                         |
| Can set new HSM label          | Yes       | Yes                        |
| Creates new HSM SO identity    | No        | Yes                        |
| Creates new Domain             | No        | Yes                        |
| Destroys partitions            | Yes       | No (none exist to destroy) |
| Destroys objects               | Yes       | No (none exist to destroy) |

## Initializing a New or Factory-reset HSM

**NOTE** New HSMs are shipped in Secure Transport Mode (STM). You must recover the HSM from STM before you can initialize the HSM. See ["Secure Transport Mode"](#) on page 14 for details.

On a new, or factory-reset HSM (using **hsm factoryreset**), the following attributes are set during a hard initialization:

|   |  |
|---|--|
| <b>HSM Label</b>                                  | <p>The label is a string that uniquely identifies this HSM.</p> <p>The HSM label created during initialization must be 1-32 characters in length. If you specify a longer label, it will automatically be truncated to 32 characters. Only alphanumeric characters and the underscore are allowed:</p> <pre>abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789_</pre> <p>For more information, refer to <a href="#">Name, Label, and Password Requirements</a>.</p>  |
| <b>HSM SO credentials</b>                         | <p>For multifactor quorum-authenticated HSMs, you create a new HSM SO (blue) PED key(set) or re-use an existing PED key(set) from an HSM you want to share credentials with. If you are using multifactor quorum authentication, ensure that you have an authentication strategy before beginning. See "<a href="#">Multifactor Quorum Authentication</a>" on page 18.</p> <p>For password-authenticated HSMs, you specify the HSM SO password. For proper security, it should be different from the appliance admin password, and employ standard password-security characteristics.</p> <p>In LunaSH, HSM role passwords must be 8-255 characters in length. The following characters are allowed:</p> <pre>abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789 !@#\$%^&amp;*() -_+=[]{}/:'",.~</pre> <p>The following characters are invalid or problematic and must not be used within passwords:</p> <pre>"&amp;; &lt;&gt; \ `  </pre> <p>Spaces are allowed; to specify a password with spaces, enclose the password in double quotation marks.</p>   |
| <b>Cloning domain for the HSM Admin partition</b> | <p>The cloning domain is a shared identifier that makes cloning possible among a group of HSM partitions. It specifies the security domain (group of HSM partitions) within which the HSM Admin partition can share cryptographic objects through cloning, backup/restore, or in high availability configurations. Note that the HSM Admin partition cloning domain is independent of the cloning domain specified when creating application partitions on the HSM.</p> <p>For multifactor quorum-authenticated HSMs, you create a new Domain (red) PED key(set) or re-use an existing PED key(set) from an HSM you want to be able to clone with.</p> <p>For password-authenticated HSMs, you create a new domain string or re-use an existing string from an HSM you want to be able to clone with.</p> <p>The domain string must be 1-128 characters in length. The following characters are allowed:</p> <pre>abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789 !@#\$%^&amp;*-_+[]{}/:'",.~</pre> <p>The following characters are problematic or invalid and must not be used in a domain string:</p> <pre>"&amp;; &lt;&gt; \ `   ()</pre> <p>Spaces are allowed, as long as the leading character is not a space; to specify a domain string with spaces using the <b>-domain</b> option, enclose the string in double quotation marks.</p> <p>For password-authenticated HSMs, the domain string should match the complexity of the partition password.</p> |

## To initialize a new or factory-reset HSM

1. Log into LunaSH as **admin**. You can use a serial terminal window or SSH connection.

- If Secure Transport Mode is set, you must unlock the HSM before proceeding. New Luna HSMs are shipped from the factory in Secure Transport Mode (STM). STM allows you to verify whether or not an HSM has been tampered while it is not in your possession, such as when it is shipped to another location, or placed into storage. See ["Secure Transport Mode" on page 14](#) for more information.

To recover your HSM from Secure Transport Mode, proceed as follows:

- As part of the delivery process for your new HSM, you should have received an email from Thales Client Services, containing two 16-digit strings, as follows. You will need both of these strings to recover the HSM from STM:

Random User String: XXXX-XXXX-XXXX-XXXX

Verification String: XXXX-XXXX-XXXX-XXXX

- Ensure that you have the Random User String and Verification String that were emailed to you for your new HSM.
  - Enter the following command to recover from STM, specifying the Random User String that was emailed to you for your new HSM:  

```
lunash:> hsm stm recover -randomuserstring <XXXX-XXXX-XXXX-XXXX>
```
  - You are presented with a verification string. If the verification string matches the original verification string emailed to you for your new HSM, the HSM has not been tampered, and can be safely deployed. If the verification string does not match the original verification string emailed to you for your new HSM, the HSM has been tampered while in STM. If the verification strings do not match, contact Thales Technical Support immediately.
  - Enter **proceed** to recover from STM (regardless of whether the strings match or not), or enter **quit** to remain in STM.
- If you are initializing a multifactor quorum-authentication HSM, have the Luna PED connected and ready (via USB, in Local PED-USB mode). If your PED is not in USB mode, see ["Changing Modes" on page 30](#). Alternatively, have a Remote PED instance set up, see ["About Remote PED" on page 34](#).
  - Run the **hsm init** command, specifying a label for your Luna Network HSM 7:  

```
lunash:> hsm init -label <label>
```
  - Respond to the prompts to complete the initialization process:

- on a password-authenticated HSM, you are prompted for the HSM password and for the HSM Admin partition cloning domain string (cloning domains for application partitions are set when the application partitions are initialized).
- on a multifactor quorum-authenticated HSM, you are prompted to attend to the Luna PED to create a new HSM SO (blue) PED key for this HSM, re-use an HSM SO PED key from an existing HSM so that you can also use it to log in to this HSM, or overwrite an existing key with a new authentication secret for use with this HSM. You are also prompted to create, re-use, or overwrite the Domain (red) PED key. You can create MofN quorum keysets and duplicate keys as required. See ["Multifactor Quorum Authentication" on page 18](#) for more information.

## Re-initializing the HSM

On an existing, non-factory-reset HSM, re-initialization clears all existing partitions and objects, but retains the SO credentials and cloning domain. You have the option to change or retain the existing label. Re-initialization is also referred to as a soft init. If you do not want to do a soft init, and also change the SO credentials and cloning domain, you need to use the **hsm factoryreset** command to factory reset the HSM, and then perform the procedure described in "[Initializing a New or Factory-reset HSM](#)" on page 149.

**CAUTION!** Ensure you have backups for any partitions and objects you want to keep, before reinitializing the HSM.

### To re-initialize the HSM (soft init)

1. Log into LunaSH as **admin**. You can use a serial terminal window or SSH connection.
2. Log in as the HSM SO.
3. If Secure Transport Mode is set, you must unlock the HSM before proceeding. See "[Secure Transport Mode](#)" on page 14.
4. If you are initializing a multifactor quorum-authenticated HSM, have the Luna PED connected and ready (via USB, in Local PED-USB mode). If your PED is not in USB mode, see "[Changing Modes](#)" on page 30.
5. Re-initialize the HSM, specifying a label for your Luna Network HSM 7:

```
lunash:> hsm init -label <label>
```



# CHAPTER 5: HSM Roles

The security of an HSM and its cryptographic contents depends on well-controlled access to that HSM. A controlled access policy is defined by:

- > the set of users with valid login credentials for the appliance, the HSM and the application partition
- > the actions each user is allowed to perform when logged in (the user's role)

For example, an access policy that adheres to the PKCS#11 standard requires two roles: the security officer (SO), who administers the user account(s), and the standard user, who performs cryptographic operations. When a user logs in to the HSM, they can perform only those functions that are permitted for their role.

Luna Network HSM 7 divides roles on the HSM according to an enhanced version of the PKCS#11 standard. Configuration, administration, and auditing of the HSM itself is the responsibility of the roles described below. Cryptographic functions take place on the application partition, which has a different set of independent roles (see [Partition Roles](#)).

Personnel holding HSM-level roles access the HSM by logging in to LunaSH via SSH or a serial connection. They must therefore have the appropriate appliance user access for their respective HSM role, to ensure that they can access all LunaSH commands necessary to perform HSM administration tasks.

The HSM-level roles are as follows:

## HSM Security Officer (SO)

The HSM SO handles all administrative and configuration tasks on the HSM, including:

- > Initializing the HSM and setting the SO credential (see ["Initializing the HSM" on page 149](#))
- > Setting and changing global HSM policies (see ["HSM Capabilities and Policies" on page 156](#))
- > Creating/deleting the application partition (see ["Creating or Deleting an Application Partition" on page 174](#))
- > Updating the HSM firmware (see ["Updating the Luna HSM Firmware" on page 233](#))

The HSM SO must have **admin**-level user access to the Luna Network HSM 7 appliance (see [Appliance Users and Roles](#)).

### Managing the HSM Security Officer Role

Refer also to the following procedures to manage the HSM SO role:

- > ["Logging In as HSM Security Officer" on the next page](#)
- > ["Changing the HSM SO Credential" on the next page](#)

## Auditor (AU)

The Auditor is responsible for managing HSM audit logging. These responsibilities have been separated from the other roles on the HSM and application partition so that the Auditor can provide independent oversight of all HSM processes, and no other user, including the HSM SO, can clear those logs. The Auditor's tasks include:

- > Initializing the Auditor role

- > Setting up audit logging on the HSM
- > Configuring the maximum size of audit log files and the time interval for log rotation
- > Archiving the audit logs

The Auditor must have access to the **audit** account on the Luna Network HSM 7 appliance (see [Appliance Users and Roles](#)).

### Managing the Auditor Role

Refer to "Configuring and Using Audit Logging" on page 125 for procedures involving the Auditor role. See also:

- > "Logging In as Auditor" on page 124
- > "Changing the Auditor Credentials" on page 139

## Logging In as HSM Security Officer

Before you can create an application partition or perform other administrative functions on the HSM, you must log in as HSM Security Officer (SO), or administrative commands will fail.

### To log in as HSM SO

1. Connect to the appliance via SSH or a serial connection, and log in to LunaSH as **admin** or a custom user with an **admin** role (see [Logging In to LunaSH](#)).
2. Log in to the HSM.

```
lunash:> hsm login
```

You are prompted for the HSM SO credential.

### Failed HSM SO Login Attempts

If you fail three (3) consecutive HSM SO login attempts, application partitions are destroyed, the HSM is zeroized and all of its contents are rendered unrecoverable. The number is not adjustable. As soon as you authenticate successfully, the counter is reset to zero.

**NOTE** The system must actually receive some erroneous/false information before it logs a failed attempt; if you merely forget to insert the PED key, or insert the wrong color key, that is not counted as a failed attempt. You must insert an incorrect PED key of the correct type, or enter an incorrect PIN or challenge secret, to fail a login attempt.

### Changing the HSM SO Credential

From time to time, it might be necessary to change the secret associated with a role on an HSM appliance, a role on an HSM or a partition of an HSM, or a cloning domain secret. Reasons for changing credentials include:

- > Regular credential rotation as part of your organization's security policy
- > Compromise of a role or secret due to loss or theft of a PED key
- > Personnel changes in your organization or changes to individual security clearances
- > Changes to your security scheme (implementing/revoking M of N, PINs, or shared secrets)

The HSM SO can change their own credential at any time.

There is no way to reset the HSM SO credential except to re-initialize the HSM, zeroizing the contents of the HSM and its application partitions. Resetting a credential requires a higher authority. On the HSM, there is no authority higher than the HSM SO.

---

### To change the HSM SO credential

1. Connect to the appliance via SSH or a serial connection, and log in to LunaSH as **admin** or a custom user with an **admin** role (see [Logging In to LunaSH](#)).
2. Log in as HSM SO (see "[Logging In as HSM Security Officer](#)" on the previous page).
3. Change the HSM SO credential.

```
lunash:> hsm changepw
```

You are prompted for the current HSM SO credential, and then to create a new one.

In LunaSH, HSM role passwords must be 8-255 characters in length. The following characters are allowed:

```
abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789 !@#$%^*()-_+[]{}/:'",.~
```

The following characters are invalid or problematic and must not be used within passwords: "&;<>\'|

Spaces are allowed; to specify a password with spaces, enclose the password in double quotation marks.

# CHAPTER 6: HSM Capabilities and Policies

The HSM can be configured to suit the cryptographic needs of your organization. Configurable functions are governed by the following settings:

- > **HSM Capabilities** are features of HSM functionality, set at manufacture based on the HSM model you selected at time of purchase. You can add new capabilities to the HSM by purchasing and applying capability licenses from Thales (see "[Upgrading HSM Capabilities and Partition Licenses](#)" on page 236). Some capabilities have corresponding modifiable HSM policies.
- > **HSM Policies** are configurable settings that allow the HSM Security Officer to modify the function of their corresponding capabilities. Some policies affect HSM-wide functionality, and others allow further customization of individual partitions by the Partition Security Officer.

The table below describes all Luna Network HSM 7 capabilities, their corresponding policies, and the results of changing their settings. This section contains the following procedures:

- > "[Setting HSM Policies Manually](#)" on page 170
- > "[Setting HSM Policies Using a Template](#)" on page 171

To zeroize the HSM and revert policies to their default values, see "[Resetting the Luna Network HSM 7 to Factory Condition](#)" on page 268.

To zeroize the HSM and keep the existing policy settings, use lunash:> **hsm zeroize**

## Destructive Policies

Some policies affect the security of the HSM. As a security measure, changing those security-affecting policies results in application partitions, or the entire HSM, being zeroized. Among those listed below, such policies are marked as **Destructive**.

| # | HSM Capability   | HSM Policy |
|---|--|------------|
| 0 | <b>Enable PIN-based authentication</b> <ul style="list-style-type: none"><li>&gt; <b>Allowed:</b> The HSM authenticates all users with keyboard-entered passwords.</li><li>&gt; <b>Disallowed:</b> See HSM capability 1 below.</li></ul> | N/A        |

| # | HSM Capability   | HSM Policy  |
|---|--|---|
| 1 | <p><b>Enable PED-based authentication</b></p> <ul style="list-style-type: none"> <li>&gt; <b>Allowed:</b> The HSM authenticates users with secrets stored on physical PED keys, read by a Luna PED. The Crypto Officer and Crypto User roles may also be configured with a secondary, keyboard-entered challenge secret.</li> <li>&gt; <b>Disallowed:</b> See HSM capability 0 above.</li> </ul> | N/A   |
| 2 | <p><b>Performance level</b></p> <p>Numerical value indicates the HSM's performance level, determined by the model you selected at time of purchase:</p> <ul style="list-style-type: none"> <li>&gt; <b>4: Standard</b> performance</li> <li>&gt; <b>8: Enterprise</b> performance</li> <li>&gt; <b>15: Maximum</b> performance</li> </ul>  | N/A   |
| 4 | <p><b>Enable domestic mechanisms &amp; key sizes</b></p> <p>Always <b>allowed</b>. All Luna Network HSM 7s are capable of full-strength cryptography with no US export restrictions.</p>   | N/A   |
| 6 | <p><b>Enable masking</b></p> <p>Always <b>disallowed</b> for HSMs with older firmware. SKS (which uses masking) was not available before <a href="#">Luna HSM Firmware 7.7.0</a>.</p> <p><b>Allowed</b> for Luna Network HSM 7s at <a href="#">Luna HSM Firmware 7.7.0</a> and newer, to support SKS.</p>  | <p><b>Allow masking</b></p> <p><b>Destructive</b></p> <p>If this policy is allowed, see <b>partition policy 3: <a href="#">Allow private key masking</a></b> and <b>partition policy 7: <a href="#">Allow secret key masking</a></b>.</p> |

| # | HSM Capability  | HSM Policy  |
|---|---|---|
| 7 | <p><b>Enable cloning</b></p> <p>Always <b>allowed</b>. All current Luna Network HSM 7s can clone cryptographic objects from one partition to another.</p>   | <p><b>Allow cloning</b></p> <p><b>Destructive</b></p> <ul style="list-style-type: none"> <li>&gt; <b>ON</b> (default): The HSM may clone cryptographic objects from one partition to another. This is required to back up partitions or include them in HA groups. Partition SOs can enable/disable cloning on individual partitions.</li> <li>&gt; <b>OFF</b>: No partition on the HSM may clone cryptographic objects. Partition SOs cannot change this.</li> </ul> |
| 9 | <p><b>Enable full (non-backup) functionality</b></p> <ul style="list-style-type: none"> <li>&gt; <b>Allowed</b>: The HSM is capable of full cryptographic functions.</li> <li>&gt; <b>Disallowed</b>: The HSM is capable of backup functions only.</li> </ul> | N/A   |

| #  | HSM Capability   | HSM Policy   |
|----|--|--|
| 12 | <p><b>Enable non-FIPS algorithms</b><br/>Always <b>allowed</b>. The HSM can use all cryptographic algorithms described in <a href="#">Supported Mechanisms</a>.</p>  | <p><b>Allow non-FIPS algorithms</b><br/><b>Destructive *</b></p> <ul style="list-style-type: none"> <li>&gt; <b>ON</b> (default): The HSM may use all available cryptographic algorithms, meaning all the FIPS-approved algorithms as well as all the non-FIPS algorithms.</li> <li>&gt; <b>OFF</b>: Only algorithms sanctioned by the FIPS 140-2 standard are permitted. The following is displayed in the output from lunash:&gt; <b>hsm show</b>:<br/> <pre>FIPS 140-2 Operation: ===== The HSM is in FIPS 140-2 approved operation mode.</pre> </li> </ul> <div style="border: 1px solid black; padding: 10px; margin-top: 10px;"> <p><b>NOTE</b> When C_GetMechanismInfo is called and the HSM policy “Allow NonFIPS Algorithms” is disabled:</p> <ul style="list-style-type: none"> <li>&gt; If a mechanism has the WRAP flag set and MPE_NO_WRAP, the WRAP flag is <i>not</i> returned by the HSM as part of the mechanism info.</li> <li>&gt; If a mechanism has the SIGN flag set and MPE_NO_SIGN, the SIGN flag is <i>not</i> returned by the HSM as part of the mechanism info.</li> </ul> <p>When the policy is enabled, the HSM returns all the flags that are applicable to the requested mechanism.</p> </div> <p>This policy must be ON for the HSM, in order to allow the non-FIPS choice to be made on a per-partition basis (<a href="#">Luna HSM Firmware 7.7.1</a> and newer) using partition policy 43. If this HSM policy is OFF, then non-FIPS algorithms cannot be permitted on a per-partition basis and partition policy 43 is not available for use.</p> |
| 15 | <p><b>Enable SO reset of partition PIN</b><br/>Always <b>allowed</b>. This capability enables:</p> <ul style="list-style-type: none"> <li>&gt; the Partition SO to reset the password or PED key secret of the Crypto Officer.</li> <li>&gt; the Crypto Officer to reset the password or PED key secret of the Crypto User.</li> </ul> | <p><b>SO can reset partition PIN</b><br/><b>Destructive</b></p> <ul style="list-style-type: none"> <li>&gt; <b>ON</b>: Partition SO may reset the password or PED key secret of a Crypto Officer who has been locked out after too many failed login attempts.</li> <li>&gt; <b>OFF</b> (default): The CO lockout is permanent and the partition contents are no longer accessible. The partition must be re-initialized, and key material restored from a backup device.</li> </ul> <p>See <a href="#">Resetting the Crypto Officer or Crypto User Credential</a>.</p>  |

| #  | HSM Capability   | HSM Policy  |
|----|--|---|
| 16 | <p><b>Enable network replication</b><br/>Always <b>allowed</b>. This capability enables cloning of cryptographic objects over a network. This is required for HA groups, and for partition backup to a remote or client-connected Luna Backup HSM.</p> <div data-bbox="316 541 582 972" style="border: 1px solid #ccc; padding: 5px; margin-top: 10px;"> <p><b>NOTE</b> Luna HSM Firmware 7.8.0 and newer ignores this setting where CPv4 is invoked; that cloning option is always allowed, when the corresponding cloning policies are enabled.</p> </div> | <p><b>Allow network replication</b></p> <ul style="list-style-type: none"> <li>&gt; <b>ON</b> (default): Cloning of cryptographic objects is permitted over a network. Remote and client-connected backup is allowed, and the partition may be used in an HA group.</li> <li>&gt; <b>OFF</b>: Cloning over a network is not permitted. Partition backup is possible to a locally-connected Luna Backup HSM only.</li> </ul> |
| 17 | <p><b>Enable Korean Algorithms</b></p> <ul style="list-style-type: none"> <li>&gt; <b>Allowed</b>: if you have purchased and applied a license for the Korea-specific algorithm set. See <a href="#">"Upgrading HSM Capabilities and Partition Licenses" on page 236</a> to purchase this capability.</li> <li>&gt; <b>Disallowed</b> if you have not applied this license.</li> </ul>   | N/A   |
| 18 | <p><b>FIPS evaluated</b><br/>Always <b>disallowed</b> - deprecated capability. All Luna Network HSM 7s are capable of operating in FIPS Mode.</p> <div data-bbox="272 1591 624 1856" style="border: 1px solid #ccc; padding: 5px; margin-top: 10px;"> <p><b>NOTE</b> This capability is visible (not used) in previous HSM firmware versions, but is removed from <a href="#">Luna HSM Firmware 7.7.0</a> and newer.</p> </div>  | N/A   |



| #  | HSM Capability   | HSM Policy   |
|----|--|--|
| 19 | <b>Manufacturing Token</b><br>Always <b>disallowed</b> . For Thales internal use only.   | N/A  |
| 21 | <b>Enable forcing user PIN change</b><br>Always <b>allowed</b> . This capability forces the Crypto Officer or Crypto User to change the initial role credential created by the Partition SO. | <b>Force user PIN change after set/reset</b><br><ul style="list-style-type: none"> <li>&gt; <b>ON</b> (default): After the Partition SO initializes or resets the Crypto Officer credential, the CO must change the credential before any other actions are permitted. This also applies when the CO initializes/resets the Crypto User role. This policy is intended to enforce the separation of roles on the partition.</li> <li>&gt; <b>OFF</b>: The CO/CU may continue to use the credential assigned by the Partition SO. They can change / rotate the credential at any time, but the change is not forced at first use of the role after role initialization or reset.</li> </ul> See <a href="#">Changing a Partition Role Credential</a> . |
| 22 | <b>Enable portable masking key</b><br>Always <b>allowed</b> - deprecated capability with no application to Luna 7.   | <b>Allow offboard storage</b><br><b>Destructive</b><br>Deprecated policy with no application to Luna 7.<br>Default: <b>ON</b>  |
| 23 | <b>Enable partition groups</b><br>Always <b>disallowed</b> - deprecated capability.  | N/A  |
| 25 | <b>Enable Remote PED usage</b><br>Always <b>allowed</b> on multifactor quorum-authenticated HSMs.<br>Always <b>disallowed</b> on password-authenticated HSMs.                                | <b>Allow Remote PED usage</b><br><ul style="list-style-type: none"> <li>&gt; <b>ON</b> (default): The HSM may authenticate roles using a remotely-located Luna PED server or a locally-installed Luna PED.</li> <li>&gt; <b>OFF</b>: The HSM must use a locally-installed Luna PED to authenticate roles.</li> </ul>   |
| 27 | <b>HSM non-volatile storage space</b><br>Displays the maximum non-volatile storage space (in bytes) on the HSM, determined by the Luna Network HSM 7 model you selected at time of purchase. | N/A  |
| 30 | <b>Enable Unmasking</b><br>Always <b>allowed</b> . This capability enables migration from legacy Luna HSMs that used SIM.  | <b>Allow unmasking</b><br><ul style="list-style-type: none"> <li>&gt; <b>ON</b> (default): Cryptographic objects may be migrated from legacy Luna HSMs that used SIM.</li> <li>&gt; <b>OFF</b>: Migration from legacy HSMs using SIM is not possible.</li> </ul>   |

| #  | HSM Capability   | HSM Policy   |
|----|--|--|
| 33 | <p><b>Maximum number of partitions</b><br/>Displays the maximum number of application partitions that can be created on the HSM. The default maximum is determined by the Luna Network HSM 7 model you selected at time of purchase. On some models, you can upgrade the number of allowable partitions by purchasing additional partition licenses (see <a href="#">"Upgrading HSM Capabilities and Partition Licenses"</a> on page 236).</p> | <p><b>Current maximum number of partitions</b><br/>You can change HSM policy 33 to lower the effective maximum number of partitions below the actual licensed maximum. You cannot, however, lower the maximum below the number of partitions currently existing on the HSM.</p>  |
| 35 | <p><b>Enable Single Domain</b><br/>Always <b>disallowed</b>.</p>   | N/A  |
| 36 | <p><b>Enable Unified PED Key</b><br/>Always <b>disallowed</b>.</p>   | N/A  |
| 37 | <p><b>Enable MofN</b><br/>Always <b>allowed</b> on multifactor quorum-authenticated HSMs.<br/>Always <b>disallowed</b> on password-authenticated HSMs.</p>   | <p><b>Allow MofN</b></p> <ul style="list-style-type: none"> <li>&gt; <b>ON</b> (default): During PED key creation, you have the option to require a quorum to authenticate the role, by splitting the authentication secret among multiple PED keys (see <a href="#">"Quorum Split Secrets (M of N)"</a> on page 23)</li> <li>&gt; <b>OFF</b>: Users do not have the option to split PED key secrets (M and N are automatically set to 1).</li> </ul>  |
| 38 | <p><b>Enable small form factor backup/restore</b><br/>Always <b>disallowed</b>.</p>  | N/A  |
| 39 | <p><b>Enable Secure Trusted Channel</b><br/>Always <b>allowed</b>. This capability enables Secure Trusted Channel (STC) to be used for partition-client connections, and/or to encrypt traffic between the HSM and appliance (see <a href="#">Secure Trusted Channel</a>).</p>   | <p><b>Allow Secure Trusted Channel</b></p> <ul style="list-style-type: none"> <li>&gt; <b>ON</b>: Secure Trusted Channel is enabled for partition-client connections (see <a href="#">Creating a Client-Partition STC Connection</a>). STC can be used to encrypt traffic between the appliance and the HSM (see <a href="#">Using the STC Admin Channel</a>).</li> <li>&gt; <b>OFF</b> (default): All clients must access partitions using NTLS connections.</li> </ul> <p>Not applicable to HSMs at <a href="#">Luna HSM Firmware 7.7.0</a> or newer, where STC is always enabled and is optional to use in any application partition, unless Partition Policy 37 is set to make STC mandatory for that partition.</p> |

| #  | HSM Capability  | HSM Policy   |
|----|---|--|
| 40 | <p><b>Enable decommission on tamper</b><br/>Always <b>allowed</b>. This enables the HSM to be automatically decommissioned if a tamper event occurs (see "<a href="#">Comparing Zeroize, Decommission, Re-image, and Factory Reset</a>" on page 269).</p> | <p><b>Decommission on tamper</b><br/><b>Destructive</b></p> <ul style="list-style-type: none"> <li>&gt; <b>ON</b>: The HSM is decommissioned if a tamper event occurs (see "<a href="#">Tamper Events</a>" on page 178).</li> <li>&gt; <b>OFF</b> (default): The contents of the HSM are not affected by a tamper event.</li> </ul>  |
| 42 | <p><b>Enable partition re-initialize</b><br/>Always <b>disallowed</b>.</p>  | N/A  |
| 43 | <p><b>Enable low level math acceleration</b><br/>Always <b>allowed</b>. This capability enables acceleration of cryptographic functionality for maximum HSM performance.</p>  | <p><b>Allow low-level math acceleration</b></p> <ul style="list-style-type: none"> <li>&gt; <b>ON</b> (default): Provides maximum HSM performance.</li> <li>&gt; <b>OFF</b>: Do not turn this policy off unless instructed by Thales Technical Support.</li> </ul>   |
| 45 | <p><b>Enable Fast-Path</b><br/>Always <b>disallowed</b>.</p>  | N/A  |
| 46 | <p><b>Allow Disabling Decommission</b><br/>Always <b>allowed</b>. This capability enables the HSM SO to disable the decommission button on the HSM.</p>   | <p><b>Disable Decommission</b><br/><b>Destructive</b></p> <ul style="list-style-type: none"> <li>&gt; <b>ON</b>: The decommission button is disabled, preventing decommissioning of the HSM.</li> <li>&gt; <b>OFF</b> (default): Decommission works as described in <a href="#">Decommissioning the HSM Appliance</a>.</li> </ul> <div style="border: 1px solid orange; padding: 5px; margin-top: 10px;"> <p><b>CAUTION!</b> Changing this policy will destroy partitions on the HSM, and they must be recreated. If HSM policy 40 is enabled, you cannot enable this policy (fails with error: CKR_CONFIG_FAILS_DEPENDENCIES). However, attempting to enable it will still destroy HSM partitions.</p> </div> |
| 47 | <p><b>Enable Tunnel Slot</b><br/>Always <b>disallowed</b>.</p>  | N/A  |

| #  | HSM Capability   | HSM Policy  |
|----|--|---|
| 48 | <p><b>Enable Controlled Tamper Recovery</b></p> <p>Always <b>allowed</b>. This capability enables the HSM SO to require tamper events to be explicitly cleared before normal operations can resume.</p>  | <p><b>Do Controlled Tamper Recovery</b></p> <ul style="list-style-type: none"> <li>&gt; <b>ON</b> (default): After a tamper event, the HSM SO must explicitly clear the tamper before the HSM can resume normal operations.</li> <li>&gt; <b>OFF</b>: The HSM must be restarted before it can resume normal operations.</li> </ul> <p>See "<a href="#">Tamper Events</a>" on page 178 for more information.</p> |
| 49 | <p><b>Enable Partition Utilization Metrics</b></p> <p>Always <b>allowed</b>. This capability enables the HSM SO to view (or export to a named file) counters that record how many times specific cryptographic operations have been performed in application partitions since the last counter-reset event. This provides a picture of operational utilization that can be used to guide the (re-)allocation and balancing of partitions and applications, for better service to all users of your partitions.</p> | <p><b>Allow Partition Utilization Metrics</b></p> <ul style="list-style-type: none"> <li>&gt; <b>ON</b>: The HSM SO can view Partition Utilization Metrics.</li> <li>&gt; <b>OFF</b> (default): Partition Utilization Metrics are not available.</li> </ul> <p>See "<a href="#">Partition Utilization Metrics</a>" on page 190 for more information.</p>  |

| #  | HSM Capability   | HSM Policy  |
|----|--|---|
| 50 | <p><b>Enable Functionality Modules</b></p> <p>This capability enables Functionality Modules (FMs) to be loaded to the HSM (see <a href="#">"Functionality Modules" on page 252</a>).</p> <ul style="list-style-type: none"> <li>&gt; <b>Allowed</b> on FM-ready HSMs with <a href="#">Luna HSM Firmware 7.4.0</a> or newer, with the FM capability license installed (see <a href="#">"Preparing the Luna Network HSM 7 to Use FMs" on page 256</a>).</li> <li>&gt; <b>Disallowed</b> on FM-ready HSMs with <a href="#">Luna HSM Firmware 7.4.0</a> or newer, without the FM capability license.</li> </ul> <p>Does not appear on HSMs that are not FM-ready or are running firmware older than <a href="#">Luna HSM Firmware 7.4.0</a>.</p> | <p><b>Allow Functionality Modules Destructive</b></p> <ul style="list-style-type: none"> <li>&gt; <b>ON:</b> With this policy enabled, Functionality Modules may be loaded to the HSM, permitting custom cryptographic operations. Allows use of the <b>ctfm</b> utility and FM-related commands, and the use of Functionality Modules in general with this HSM.</li> </ul> <div style="border: 1px solid #ccc; padding: 10px; margin: 10px 0;"> <p><b>NOTE</b> FIPS compliance requires that objects are never cloned or restored to an HSM using less secure firmware. FIPS 140 validation is performed against the HSM hardware with a specific firmware version.</p> <p>Since the introduction of a Functionality Module changes the firmware, allowing FMs in the HSM removes the HSM from FIPS compliance.</p> <p>For purposes of cloning, an HSM where FMs have <i>ever</i> been allowed is considered less secure than one where FMs have <i>never</i> been allowed. See the Caution below.</p> </div> <p>You can subsequently disable FMs, but future cloning operations will work only with other FM-HOC HSMs.</p> <ul style="list-style-type: none"> <li>&gt; <b>OFF</b> (default): FMs may not be loaded to the HSM.</li> </ul> <div style="border: 1px solid #ccc; padding: 10px; margin: 10px 0;"> <p><b>CAUTION!</b> Enabling FMs (<b>HSM policy 50</b>) introduces changes to Luna HSM functionality, some of which are permanent; they cannot be removed by disabling the policy. FM-enabled status is <b>not</b> reversible by Factory Reset. Refer to <a href="#">"FM Deployment Constraints" on page 252</a> for details before enabling.</p> <p>If you are using Crypto Command Center, ensure that your CCC version supports FM-enabled HSMs before you enable <b>HSM policy 50</b>. Refer to the CCC CRN for details.</p> </div> |

| #  | HSM Capability   | HSM Policy   |
|----|--|--|
| 51 | <p><b>Enable SMFS Auto Activation</b></p> <p>This capability enables the Secure Memory File System (SMFS) to be activated automatically on startup.</p> <ul style="list-style-type: none"> <li>&gt; <b>Allowed</b> on FM-ready HSMs with <a href="#">Luna HSM Firmware 7.4.0</a> or newer, with the FM capability license installed (see "<a href="#">Preparing the Luna Network HSM 7 to Use FMs</a>" on page 256).</li> <li>&gt; <b>Disallowed</b> on FM-ready HSMs with <a href="#">Luna HSM Firmware 7.4.0</a> or newer, without the FM capability license.</li> </ul> <p>Does not appear on HSMs that are not FM-ready or are running firmware older than <a href="#">Luna HSM Firmware 7.4.0</a>.</p>              | <p><b>Allow SMFS Auto Activation</b></p> <p><b>Destructive</b></p> <ul style="list-style-type: none"> <li>&gt; <b>ON:</b> With this policy enabled, the Secure Memory File System (SMFS) is automatically activated on startup, providing a secure, tamper-enabled location in the HSM memory where Functionality Modules can load keys and parameters. Auto-activation for SMFS, like auto-activation for multifactor quorum-authenticated partitions in general, persists through a power outage of up to 2 hours duration.</li> <li>&gt; <b>OFF (default):</b> If disabled, the HSM SO must manually activate the SMFS each time the HSM reboots or loses power.</li> </ul> |
| 52 | <p><b>Allow Restricting FM Privilege Level</b></p> <p>This capability enables the HSM SO to restrict the sensitive key attributes of partition objects from FMs.</p> <ul style="list-style-type: none"> <li>&gt; <b>Allowed</b> on FM-ready HSMs with <a href="#">Luna HSM Firmware 7.4.0</a> or newer, with the FM capability license installed (see "<a href="#">Preparing the Luna Network HSM 7 to Use FMs</a>" on page 256).</li> <li>&gt; <b>Disallowed</b> on FM-ready HSMs with <a href="#">Luna HSM Firmware 7.4.0</a> or newer, without the FM capability license.</li> </ul> <p>Does not appear on HSMs that are not FM-ready or are running firmware older than <a href="#">Luna HSM Firmware 7.4.0</a>.</p> | <p><b>Restrict FM Privilege Level</b></p> <p><b>Destructive</b></p> <ul style="list-style-type: none"> <li>&gt; <b>ON:</b> FM privilege is restricted.</li> <li>&gt; <b>OFF (default):</b> FM privilege permits FMs to see the sensitive key attributes (including key values) of cryptographic objects on application partitions. This privilege is necessary for most FMs, so that the Crypto Officer (CO) and Crypto User (CU) roles can use partition objects with the FM. However, some FMs might not require this privilege and it can be restricted to satisfy some certification requirements (such as Common Criteria).</li> </ul>                                    |

| #  | HSM Capability  | HSM Policy   |
|----|---|--|
| 53 | <p><b>Allow Encrypting of Keys from FM to HSM</b></p> <p>This capability enables key encryption between the FM and the Functionality Module Crypto Engine interface (FMCE).</p> <ul style="list-style-type: none"> <li>&gt; <b>Allowed</b> on FM-ready HSMs with <a href="#">Luna HSM Firmware 7.4.0</a> or newer, with the FM capability license installed (see "<a href="#">Preparing the Luna Network HSM 7 to Use FMs</a>" on page 256).</li> <li>&gt; <b>Disallowed</b> on FM-ready HSMs with <a href="#">Luna HSM Firmware 7.4.0</a> or newer, without the FM capability license.</li> </ul> <p>Does not appear on HSMs that are not FM-ready or are running firmware older than <a href="#">Luna HSM Firmware 7.4.0</a>.</p> | <p><b>Encrypt Keys Passing from FM to HSM</b></p> <p><b>Destructive</b></p> <ul style="list-style-type: none"> <li>&gt; <b>ON:</b> With this policy enabled, keys created by an FM are encrypted before crossing from the FM to the Functionality Module Crypto Engine interface (FMCE). This internal encryption may be required to satisfy some certification requirements (such as Common Criteria).</li> <li>&gt; <b>OFF</b> (default): Keys are not encrypted before crossing to the FMCE.</li> </ul> |

| #  | HSM Capability   | HSM Policy  |
|----|--|---|
| 55 | <p><b>Enable Restricted Restore</b></p> <p>This capability allows the HSM SO to restrict a Luna Backup HSM 7 from being used with firmware older than <a href="#">Luna HSM Firmware 7.7.0</a>, for any purpose other than to migrate cryptographic objects to <a href="#">Luna HSM Firmware 7.7.0</a> or newer. See <a href="#">Behavior of Pre-Firmware 7.7, V0, and V1 Partitions</a> for more information.</p> <p>Appears on Luna Backup HSM 7 running <a href="#">Luna Backup HSM 7 Firmware 7.7.1</a> or newer.</p> <div data-bbox="316 785 582 1146" style="border: 1px solid #ccc; padding: 5px; margin-top: 10px;"> <p><b>NOTE</b> Not visible on Luna Network HSM 7 via lunash commands. Look for this Capability/Policy via <b>lunacm</b> when a Luna Backup HSM 7 is the current slot.</p> </div> | <p><b>Enable Restricted Restore</b></p> <p><b>ON-to-OFF Destructive</b></p> <ul style="list-style-type: none"> <li>&gt; <b>1</b>: Objects backed up from pre-7.7.0 firmware partitions <i>can only be</i> restored to V0 or V1 partitions (<a href="#">Luna HSM Firmware 7.7.0</a> or newer). Enable this policy to ensure FIPS compliance.</li> <li>&gt; <b>0</b> (default): Objects backed up from pre-7.7.0 firmware partitions <i>can be</i> restored to pre-7.7.0 firmware partitions. Do not use this setting if you require FIPS compliance.</li> </ul> <div data-bbox="783 600 1394 1003" style="border: 1px solid #ccc; padding: 10px; margin-top: 10px;"> <p><b>CAUTION!</b> FIPS compliance requires that objects are never cloned or restored to an HSM using less secure firmware, and this includes restoring from Luna Backup HSM 7 firmware.</p> <p>If you have backups already stored on the Luna Backup HSM 7 that were taken from pre-7.7.0 partitions, turning this policy ON will prevent you from restoring them to the same source partition. You must update the HSM containing the source partition to <a href="#">Luna HSM Firmware 7.7.0</a> or newer before restoring from backup.</p> </div> |



| #  | HSM Capability   | HSM Policy  |
|----|--|---|
| 56 | <p><b>Enable User Defined ECC Curves</b></p> <p>This capability allows the HSM SO to restrict or allow the use of user-defined ECC curves.</p> <p>The state of the associated policy is preserved through firmware update.</p> | <p><b>Allow User Defined ECC Curves</b></p> <p><b>Destructive</b></p> <ul style="list-style-type: none"> <li>&gt; <b>ON:</b> User-defined ECC curves can be used, without restriction.</li> <li>&gt; <b>OFF (default):</b> Named curves (that we have verified) can still be used, as can user-defined ECC curves where the named-curve parameters are provided. User-defined ECC curves that cannot map to built-in named curves during key-pair generation, public key creation, private key unwrapping, cloning or SKS, and key derivation, return the error ECC_CURVE_NOT_ALLOWED.</li> <li>&gt; Named-curve samples are provided when you include the SDK option while installing the Client. The files must be unmodified.</li> </ul> <p>/usr/safenet/lunaclient/samples/ecc_examples</p> <ul style="list-style-type: none"> <li>• bpP160r1.txt</li> <li>• bpP512t1.txt</li> <li>• x962_char2_163v1.txt</li> <li>• bpP192r1.txt</li> <li>• secp384r1.txt</li> <li>• x962_char2_359V1.txt</li> <li>• bpP224r1.txt</li> <li>• bpP384R1.txt</li> <li>• sm2p256v1.txt</li> </ul> <div style="border: 1px solid black; padding: 10px; margin-top: 10px;"> <p><b>NOTE</b> For FIPS compliance, NIST requires us to make security claims with respect to the curves that we support.</p> <p>It is impossible to test and report on all possible user-defined ECC curves. Therefore, commonly-used, named curves are explicitly tested, documented to comply with FIPS requirements, and allowed in FIPS mode.</p> </div> |

| #  | HSM Capability   | HSM Policy  |
|----|--|---|
| 57 | <p><b>Enable Sync with Host Time</b></p> <p>This capability enables the HSM SO to automatically synchronize the HSM's time to the host system time every 24 hours.</p> | <p><b>Allow Sync with Host Time</b></p> <p>&gt; <b>ON:</b> The HSM's time is synchronized to the host system time once every 24 hours.</p> <p>The maximum drift that is allowed to be synchronized by this policy is 3 seconds. If the HSM time and the host time have drifted by more than 3 seconds in the last 24 hours, a log entry is created instead:</p> <pre>[HSM] LOG(INFO): Hsm clock(1647624503) drifts from host clock(1647628144) &gt; threshold, stop sync clock!</pre> <pre>[HSM] ALM2029: HSM clock drift allowed threshold exceeded</pre> <p>This applies to the first synchronization as well -- set the time manually using <code>hsm time get</code> and <code>hsm time sync</code> before setting this policy to ON. See also the <code>System times</code> block in the output of <code>hsm show</code> command.</p> <p>&gt; <b>OFF</b> (default): HSM time is not automatically synchronized to host time. The HSM SO can still synchronize the clocks manually.</p> |

\* The Backup HSM performs only backup and restore operations and is not a general-purpose HSM. It has no information about the origin of keys or objects. In the case of FIPS-mode or non-FIPS the status of a source HSM (Policy 12) is not noticed, and a target HSM decides what to do with keys from a restore operation. However, the actions of a Backup HSM can be affected by the cloning protocol that is used - see Policy 55.

## Setting HSM Policies Manually

The HSM SO can change available policies to customize HSM functionality. Some policies apply to all partitions on the HSM; others enable the Partition SO to customize functionality at the partition level. Refer to "[HSM Capabilities and Policies](#)" on page 156 for a complete list of HSM policies and their effects.

In most cases, HSM policies are either enabled (**1**) or disabled (**0**), but some allow a range of values.

To change multiple policy settings during HSM initialization, see "[Setting HSM Policies Using a Template](#)" on the next page.

### Prerequisites

- > The HSM must be initialized (see "[Initializing the HSM](#)" on page 149).
- > If you are changing a destructive policy and you have partitions existing on the HSM, back up any important cryptographic objects (see [Partition Backup and Restore](#)).

### To manually set or change an HSM policy

1. Log in to LunaSH as **admin**, or an **admin**-level custom user.
2. [Optional] Display the existing HSM policy settings.

```
lunash:> hsm showPolicies
```

3. Log in as HSM SO (see "Logging In as HSM Security Officer" on page 154).

```
lunash:> hsm login
```

4. Change the policy setting by specifying the policy number and the desired value (**0**, **1**, or a number in the accepted range for that policy).

```
lunash:> hsm changePolicy -policy <policy_ID> -value <value>
```

## Setting HSM Policies Using a Template

An HSM policy template is a file containing a set of preferred HSM policy settings, used to initialize HSMs with those settings. You can use the same file to initialize multiple HSMs, rather than changing policies manually after initialization. This can save time and effort when initializing multiple HSMs that are to function together (such as in an HA group), or must comply with your company's overall security strategy. Templates enable scalable policy management and simplify future audit and compliance requirements.

See also [Setting Partition Policies Using a Policy Template](#).

**NOTE** This feature requires minimum [Luna HSM Firmware 7.1.0](#) and appliance software [Luna Network HSM 7 Appliance Software 7.1.0](#).

You can create a policy template file from an initialized or uninitialized HSM, and edit it using a standard text editor.

HSM policy templates cannot be used to alter settings for an initialized HSM. Once an HSM has been initialized, the SO must change individual policy values manually (see "[Setting HSM Policies Manually](#)" on the previous page).

To zeroize the HSM and revert policies to their default values, see "[Resetting the Luna Network HSM 7 to Factory Condition](#)" on page 268.

To zeroize the HSM and keep the existing policy settings, use `lunash:> hsm zeroize`

This section provides instructions for the following procedures, and some general guidelines and restrictions:

- > "[Creating an HSM Policy Template](#)" below
- > "[Editing an HSM Policy Template](#)" on the next page
- > "[Applying an HSM Policy Template](#)" on page 173

### Creating an HSM Policy Template

The following procedures describe how to generate an HSM policy template from the HSM. This can be done optionally at two points in the HSM setup process:

- > before the HSM is initialized: this produces a template file containing the default policy settings, which can then be edited
- > after initializing and setting the HSM policies manually: this produces a template file with the current HSM policy settings, which can then be used to initialize other HSMs with the same settings. The HSM SO must complete the procedure.

## To create an HSM policy template

1. Login to LunaSH as **admin**. If you are creating a template from an initialized HSM, you must log in as HSM SO.

```
lunash:> hsm login
```

2. Create the HSM policy template file with an original filename. No file extension is required. If a template file with the same name exists, it is overwritten.

```
lunash:> hsm showpolicies -exporttemplate <filename>
```

3. On a client workstation, use **pscp/scp** to transfer the template file from the source appliance.
4. Customize the template file with a standard text editor (see ["Editing an HSM Policy Template" below](#)).

## Editing an HSM Policy Template

Use a standard text editor to manually edit HSM policy templates for custom configurations. This section provides template examples and customization guidelines.

### HSM Policy Template Example

This example shows the contents of an HSM policy template created using the factory default policy settings. Use a standard text editor to change the policy values (0=OFF, 1=ON, or the desired value 0-255). You cannot edit the destructiveness of HSM policies. See ["HSM Capabilities and Policies" on page 156](#) for more information.

If you export a policy template from an uninitialized HSM, the **Sourced from HSM** header field remains blank. This field is informational and you can still apply the template.

The **Policy Description** field is included in the template for user readability only. Policies are verified by the number in the **Policy ID** field.

```
# Policy template FW Version 7.1.0
# Field format - Policy ID:Policy Description:Policy Value
# Sourced from HSM: myLunaHSM, SN: 66331
```

```
6:"Allow masking":0
7:"Allow cloning":1
12:"Allow non-FIPS algorithms":1
15:"SO can reset partition PIN":0
16:"Allow network replication":1
21:"Force user PIN change after set/reset":1
22:"Allow offboard storage":1
23:"Allow partition groups":0
25:"Allow remote PED usage":0
30:"Allow unmasking":1
33:"Current maximum number of partitions":100
35:"Force Single Domain":0
36:"Allow Unified PED Key":0
37:"Allow MofN":0
38:"Allow small form factor backup/restore":0
39:"Allow Secure Trusted Channel":0
40:"Decommission on tamper":0
42:"Allow partition re-initialize":0
43:"Allow low level math acceleration":0
46:"Disable Decommission":1
47:"Allow Tunnel Slot":0
```

```
48:"Do Controlled Tamper Recovery":1
49:"Allow Partition Utilization Metrics":0
56:"Allow User Defined ECC Curves":0
```

### Editing Guidelines and Restrictions

When creating or editing policy templates:

- > You can remove a policy from the template by adding **#** at the beginning of the line or deleting the line entirely. When you apply the template, the HSM will use the default value for that policy.
- > You may not use invalid policy values (outside the acceptable range), or values that conflict with your HSM's capabilities. For example, **HSM capability 6: Enable Masking** is always **Disallowed**, so you cannot set the corresponding HSM policy to **1**. If you attempt to initialize an HSM with a template containing invalid policy values, an error is returned and initialization fails.

### Applying an HSM Policy Template

The following procedure describes how to initialize the HSM using a policy template.

---

#### To apply a policy template to a new HSM

1. From a client workstation, use **pscp/pscp** to transfer the template file to the **admin** user on the destination appliance.
2. Login to LunaSH as **admin** on the destination appliance, and initialize the HSM using the policy template file.  
lunash:> **hsm init -label** <label> **-applytemplate** <filename>
3. Verify that the template has been applied correctly by checking the partition's policy settings.  
lunash:> **hsm showpolicies**

# CHAPTER 7: Application Partitions

The Luna Network HSM 7 has two types of partition:

- > one administrative partition, created when you initialize the HSM. The administrative partition is owned by the HSM Security Officer (SO). This partition is used by the HSM SO and the Auditor, and is not used to store cryptographic objects. Operations on the administrative partition are handled using LunaSH.
- > at least one application partition, created by the HSM SO. The application partition is owned by its Partition Security Officer (PO), and has its own access controls and security policies independent from the administrative partition and other application partitions. Its function is to store cryptographic objects used by your applications.

An application partition is like a safe deposit box that resides within a bank's vault. The HSM (vault) itself offers an extremely high level of security for its contents. An application partition (safe deposit box) on the HSM has its own security and access controls, so that even though the HSM SO has access to the vault, they still cannot access the contents of the individual partitions. Only the Partition Security Officer holds the partition's administrative credentials.

Depending on your Luna Network HSM 7 model and the number of additional partition licenses you have purchased, you can create anywhere from 5 to 100 application partitions on the HSM. Each partition can store cryptographic objects according to the amount of memory you assign. The HSM SO can customize the size of individual partitions until all the memory on the HSM is allotted. To purchase additional partition licenses, see ["Upgrading HSM Capabilities and Partition Licenses" on page 236](#).

This chapter contains the following procedures for managing application partitions:

- > ["Creating or Deleting an Application Partition" below](#)
- > ["Customizing Partition Sizes" on the next page](#)

## Creating or Deleting an Application Partition

---

The HSM Security Officer (SO) is responsible for creating the application partition and assigning it to a registered client. The HSM SO can delete the partition at any time, destroying all partition roles and stored cryptographic objects.

### Prerequisites

- > The HSM must be initialized (see ["Initializing the HSM" on page 149](#)).
- > You require the HSM SO credential (blue PED key).

---

### To create an application partition

1. Connect to the appliance via SSH or a serial connection, and log in to LunaSH as **admin** or **operator**, or a custom user with an **admin** or **operator** role (see [Logging In to LunaSH](#)).
2. Log in as HSM SO (see ["Logging In as HSM Security Officer" on page 154](#)).

```
lunash:> hsm login
```

3. Create the application partition, specifying a partition name. This name is distinct from the partition label assigned during initialization and can be changed later. You can also specify the desired partition size in bytes (see also "[Customizing Partition Sizes](#)" below).

Partition names created in LunaSH must be 1-32 characters in length. The following characters are allowed:

```
abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ 0123456789!@#$%^*()_-=+{}[]:'. /~
```

Spaces are allowed; enclose the partition name in double quotes if it includes spaces.

The following characters are not allowed: & \ | ; < > ` ` " ?

No two partitions can have the same name.

```
lunash:> partition create -partition <name> [-size <size> | -allfreestorage] [-version <1/0>]
```

4. [Optional] Confirm that the partition was created.

```
lunash:> partition list
```

---

### To delete an application partition

1. Connect to the appliance via SSH or a serial connection, and log in to LunaSH as **admin** or **operator**, or a custom user with an **admin** or **operator** role (see [Logging In to LunaSH](#)).
2. Log in as HSM SO (see "[Logging In as HSM Security Officer](#)" on page 154).

```
lunash:> hsm login
```

3. Delete the application partition by specifying its name.

```
lunash:> partition delete -partition <name>
```

---

## Customizing Partition Sizes

If you do not specify a size in bytes when creating a partition, LunaSH automatically assigns an equal share of the total HSM memory. For example, if you purchased a Luna Network HSM 7 with 16MB of memory and 10 partition licenses, each partition would have a default size of 1.6 MB. The basic allotment ensures that you can create all licensed partitions, each with enough space to hold at least one RSA key pair.

The maximum number of partitions depends on the model of Luna Network HSM 7 you purchased. Your HSM can be upgraded with additional partition licenses if your desired configuration calls for them.

LunaSH allows you to customize the size of a partition for its intended purpose. You can choose to do this when you create each partition, or you can re-size them later, even if the partition is initialized. You must log in as HSM SO to re-size existing partitions.

- > ["Creating a Custom-Sized Partition" on the next page](#)
- > ["Re-sizing an Existing Partition" on the next page](#)
- > ["Creating Multiple Equal Large Partitions" on page 177](#)

### Prerequisites

Use lunash:> **hsm show** to see:

- > Total HSM storage
- > Current memory usage

- > Current number of partitions
- > Maximum number of partitions allowed

Use `lunash:> partition list` to see:

- > All current application partitions
- > Total storage allotted to each
- > Total used and available storage on each partition

**NOTE** Each partition requires 9648 bytes of memory to store security and identity information. Take this into account when creating very small specialized partitions (for example, a partition containing a single key pair for signing and verification).

## Creating a Custom-Sized Partition

Use the following procedure to specify the size of a new application partition. You must be logged in as HSM SO to create new partitions.

### To create a custom-sized partition

1. Connect to the appliance via SSH or a serial connection, and log in to LunaSH as **admin** or **operator**, or a custom user with an **admin** or **operator** role (see [Logging In to LunaSH](#)).
2. Log in to the HSM as HSM SO (see ["Logging In as HSM Security Officer" on page 154](#)).
3. Create the application partition, specifying the desired size in bytes. To use all remaining space on the HSM, specify **-allfreestorage** instead of **-size**.

Partition names created in LunaSH must be 1-32 characters in length. The following characters are allowed:

abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ 0123456789!@#\$%^\*()\_+={}[]:'.~/~

Spaces are allowed; enclose the partition name in double quotes if it includes spaces.

The following characters are not allowed: & \ | ; < > ` ` ?

No two partitions can have the same name.

`lunash:> partition create -partition <name> [-size <size> | -allfreestorage]`

## Re-sizing an Existing Partition

Use the following procedure to change the size of an existing application partition. You can change the size of any partition on the HSM, even if it is already initialized, as long as the space is available on the HSM and target size is not less than the objects currently stored on the partition. You must be logged in as HSM SO to re-size partitions.

**CAUTION!** Before you re-size a partition, back up the partition contents. If a partition is at or near capacity, it might be necessary to remove some objects before re-sizing. You may need to restore the partition from backup after it has been re-sized.

### To re-size an existing partition

1. Connect to the appliance via SSH or a serial connection, and log in to LunaSH as **admin** or **operator**, or a custom user with an **admin** or **operator** role (see [Logging In to LunaSH](#)).



2. Log in to the HSM as HSM SO (see "[Logging In as HSM Security Officer](#)" on page 154).
3. Re-size the desired partition by specifying the partition name and the desired size in bytes. To use all remaining space on the HSM, specify **-allfreestorage** instead of **-size**.

```
lunash:> partition resize -partition <name> {-size <size> | -allfreestorage}
```

## Creating Multiple Equal Large Partitions

You can use the re-sizing function to customize the space usage on the HSM. If you prefer to have all your partitions sized equally, and to let the HSM do the calculations, the following example might be useful. In this example, the HSM has 20 partition licenses.

---

### To create four equal-size partitions, using all the available storage

1. Start by creating 20 partitions (the maximum allowed) – each will have X bytes available to it.
2. Delete 4 of them (leaving 16).
3. Re-size one partition to use **-allfreestorage**, which makes that partition as large as five small partitions – the four partitions you just deleted, freeing their allotment, plus the one you are currently resizing – and leaves the HSM with 15 partitions having X bytes each, plus the large one.

```
lunash:> partition resize -partition <name> -allfreestorage
```

4. Delete another four small partitions.
5. Re-size one small partition to use **-allfreestorage**, which makes that partition large (there are now two equally-sized large partitions) and leaves the HSM with 10 partitions having X bytes each, plus the two large ones.
6. Delete another four small partitions.
7. Re-size one small partition to use **-allfreestorage**, which makes that partition large (there are now three equally-sized large partitions) and leaves the HSM with 5 partitions having X bytes each, plus the three large ones.
8. Delete another four small partitions.
9. Re-size the single remaining small partition to use **-allfreestorage**, which makes that partition large and leaves 0 (zero) of the original partitions with X bytes each, and the four large partitions of equal size, with no unallocated space on the HSM.

This example uses conveniently round numbers. You might have a few bytes left over, or one partition slightly larger or smaller than the others, depending on the actual configuration of your HSM.

# CHAPTER 8: Security in Operation

This section addresses actions and settings with security-related implications.

- > ["Tamper Events" below](#)
- > ["Security Effects of Administrative Actions" on page 180](#)

Refer also to [Security of Your Partition Challenge](#).

## Tamper Events

---

Luna Network HSM 7 detects hardware anomalies (such as card over-temperature) and physical events (such as card removal or chassis intrusion), and registers them as tamper events. A tamper event is considered a security breach, and effectively locks the HSM.

If **Policy 48: Do Controlled Tamper Recovery** is enabled (the default), the HSM SO must clear the tamper condition before the HSM is reset, to return the HSM to normal operation (see ["HSM Capabilities and Policies" on page 156](#)). While the HSM is in the tamper condition, only the subset of LunaSH commands required to view the HSM status or clear the tamper condition are available. For multifactor quorum-authenticated HSMs, the cached PED key data that allows activation is zeroized, and activation is disabled. When an HSM is in the tamper state, only the HSM SO is able to log in to the HSM.

You can enable **Policy 40: Decommission on Tamper** to decommission the HSM when a tamper event occurs, so that partitions and roles are deleted from the HSM. By default, **Policy 40: Decommission on Tamper** is disabled, and the contents of the HSM are not affected by the tamper event.

If both policies are disabled, the HSM sends a warning when a tamper event occurs but does not make partition data inaccessible. We do not recommend disabling both policies.

If both policies are enabled, the HSM SO role is deleted when a tamper event occurs, so you do not need to log in this role to clear the tamper condition.

There are several conditions that can result in a tamper event. The tamper state is indicated by the **HSM Tamper State** field in the output of `lunash:> hsm show`. If tamper events have been detected and not cleared, the field will read **Tamper(s) detected**. Use `lunash:>hsm tamper show` to view detailed information for the tamper event, including whether it requires an HSM reset in addition to a tamper clear.

**NOTE** A tamper event resets the HSM hardware, including the PCIe logic. This prevents the HSM from reporting any statuses, including the cause of the tamper condition. The only thing which is detected in this case is `k7pf0: ALM0015: PCIe Link Failure`. The HSM must be rebooted before the cause of the tamper event can be reported.

| Tamper event              | Response   |
|---------------------------|--|
| Chassis intrusion         | Halt the HSM. Deactivate activated partitions.<br>Decommission the HSM if <b>policy 40: Decommission on Tamper</b> is enabled.   |
| Card removal              | Halt the HSM. Deactivate activated partitions.<br>Decommission the HSM if <b>policy 40: Decommission on Tamper</b> is enabled.   |
| Over/under temperature    | Halt the HSM. Deactivate activated partitions.<br>Decommission the HSM if <b>policy 40: Decommission on Tamper</b> is enabled.<br>Warnings are logged for mild over/under temperature events. Warnings are self-clearing if the condition is resolved. |
| Over/under voltage        | Halt the HSM. Deactivate activated partitions.<br>Decommission the HSM if <b>policy 40: Decommission on Tamper</b> is enabled.<br>Warnings are logged for mild over/under voltage events. Warnings are self-clearing if the condition is resolved.     |
| Battery removal/depletion | Halt the HSM. Deactivate activated partitions.<br>Decommission the HSM.<br>Warnings are logged for low battery conditions.   |

## Recovering from a Tamper Event

How you recover from a tamper event depends on how the following HSM policies are set. See "[HSM Capabilities and Policies](#)" on page 156 for more information:

|   |  |
|---|--|
| <b>Policy 40: Decommission on tamper</b>        | If enabled, the HSM is decommissioned when a tamper event occurs. You must clear the tamper condition before you can re-initialize the HSM SO, re-create your partitions, restore the partition contents from backup, and re-initialize the partition roles (Partition SO, Crypto Officer, and Crypto User, and Audit, as relevant). |
| <b>Policy 48: Do Controlled Tamper Recovery</b> | If enabled, the tamper condition that halted the HSM must be cleared by the HSM SO (by issuing the <b>tamper clear</b> command), before the HSM can be reset to resume normal operations.  |

### Activation and auto-activation is disabled on tamper

If you are using activation or auto-activation on your multifactor quorum-authenticated partitions, it is disabled when a tamper is detected, or if any uncleared tamper conditions are detected on reboot. See [Activation on Multifactor Quorum-Authenticated Partitions](#) and [Partition Capabilities and Policies](#) for more information.

### To recover from a tamper

1. Use the following command to display the last tamper event:

```
lunash:> hsm tamper show
```

**NOTE** `hsm tamper show` only shows the last tamper event, even if several tampers have occurred. To view a complete list of the tamper events that have occurred on the HSM, use `lunash:> hsm supportinfo`.

2. Resolve the issue(s) that caused the tamper event.
3. If **Policy 48: Do Controlled Tamper Recovery** is enabled, clear the tamper condition. Otherwise, go to the next step:  
`lunash:> hsm tamper clear`
4. If the tamper message indicates that a reset is required, reboot the HSM:  
`lunash:> hsm restart`
5. Verify that all tampers have been cleared:  
`lunash:> hsm tamper show`
6. If the HSM was decommissioned as a result of the tamper, you must re-create your partitions, re-initialize the partition roles (Partition SO, Crypto Officer, and Crypto User, and Audit as relevant), and restore the partition contents from backup. Refer to the following procedures:
  - a. To re-create your partitions, see "[Creating or Deleting an Application Partition](#)" on page 174.
  - b. Re-initialize the partition roles. See [Initializing an Application Partition](#).
  - c. To restore the partition contents from backup, see [Partition Backup and Restore](#).
7. If the **Policy 22: Allow Activation** and/or **Policy 23: Allow AutoActivation** are enabled on your multifactor quorum-authenticated partitions, the CO and CU (if enabled) must log in to reactivate those roles:  
`lunacm:> role login -name <role>`

## Security Effects of Administrative Actions

Actions that you take, in the course of administering your Luna HSM, can have effects, including destruction, on the roles, the spaces, and the contents of your HSM and its application partition(s). It is important to be aware of such consequences before taking action.

### Overt Security Actions

Some actions in the administration of the HSM, or of an application partition, are explicitly intended to adjust specific security aspects of the HSM or partition. Examples are:

- > Changing a password
- > Modifying a policy to make a password or other attribute more stringent than the original setting

Those are discussed in their own sections.

### Actions with Security- and Content-Affecting Outcomes

Other administrative events have security repercussions as included effects of the primary action, which could have other intent. Some examples are:

- > HSM factory reset

- > HSM zeroization
- > Change of a destructive policy
- > HSM initialization
- > HSM firmware rollback
- > Application partition initialization

This table lists some major administrative actions that can be performed on the HSM, and compares relevant security-related effects. Use the information in this table to help decide if your contemplated action is appropriate in current circumstances, or if additional preparation (such as backup of partition content, collection of audit data) would be prudent before continuing.

### Factory Reset HSM

|                                  |   |
|----------------------------------|---|
| <b>Domain</b>                    | Destroyed   |
| <b>HSM SO Role</b>               | Destroyed   |
| <b>Partition SO Role</b>         | Destroyed   |
| <b>Auditor Role</b>              | Destroyed   |
| <b>Partition Roles</b>           | Destroyed   |
| <b>HSM or Partition/Contents</b> | HSM/Destroyed   |
| <b>HSM Policies</b>              | Reset   |
| <b>RPV</b>                       | Destroyed   |
| <b>Messaging</b>                 | You are about to factory reset the HSM. All contents of the HSM will be destroyed. HSM policies will be reset and the remote PED vector will be erased. |

### Zeroize HSM

|                                  |               |
|----------------------------------|---------------|
| <b>Domain</b>                    | Destroyed     |
| <b>HSM SO Role</b>               | Destroyed     |
| <b>Partition SO Role</b>         | Destroyed     |
| <b>Auditor Role</b>              | Unchanged     |
| <b>Partition Roles</b>           | Destroyed     |
| <b>HSM or Partition/Contents</b> | HSM/Destroyed |

|                     |  |
|---------------------|--|
| <b>HSM Policies</b> | Unchanged  |
| <b>RPV</b>          | Unchanged  |
| <b>Messaging</b>    | You are about to zeroize the HSM. All contents of the HSM will be destroyed. HSM policies, remote PED vector and Auditor left unchanged. |

### Change Destructive HSM Policy

|                                  |  |
|----------------------------------|--|
| <b>Domain</b>                    | Unchanged  |
| <b>HSM SO Role</b>               | Unchanged  |
| <b>Partition SO Role</b>         | Destroyed  |
| <b>Auditor Role</b>              | Unchanged  |
| <b>Partition Roles</b>           | Destroyed  |
| <b>HSM or Partition/Contents</b> | HSM/Destroyed  |
| <b>HSM Policies</b>              | Unchanged except for new policy  |
| <b>RPV</b>                       | Unchanged  |
| <b>Messaging</b>                 | You are about to change a destructive HSM policy. All partitions of the HSM will be destroyed. |

### HSM Initialize When Zeroized (hard init)

|                                  |   |
|----------------------------------|---|
| <b>Domain</b>                    | Destroyed   |
| <b>HSM SO Role</b>               | Destroyed   |
| <b>Partition SO Role</b>         | Destroyed   |
| <b>Auditor Role</b>              | Unchanged   |
| <b>Partition Roles</b>           | Destroyed   |
| <b>HSM or Partition/Contents</b> | HSM/Destroyed   |
| <b>HSM Policies</b>              | Unchanged   |
| <b>RPV</b>                       | Unchanged   |
| <b>Messaging</b>                 | You are about to initialize the HSM. All contents of the HSM will be destroyed. |

**HSM Initialize From Non-Zeroized State (soft init)**

|                                  |  |
|----------------------------------|--|
| <b>Domain</b>                    | Unchanged  |
| <b>HSM SO Role</b>               | Unchanged  |
| <b>Partition SO Role</b>         | Destroyed  |
| <b>Auditor Role</b>              | Unchanged  |
| <b>Partition Roles</b>           | Destroyed  |
| <b>HSM or Partition/Contents</b> | HSM/Destroyed  |
| <b>HSM Policies</b>              | Unchanged  |
| <b>RPV</b>                       | Unchanged  |
| <b>Messaging</b>                 | You are about to initialize the HSM that is already initialized. All partitions of the HSM will be destroyed. You are required to provide the current SO password. |

**HSM Firmware Rollback**

|                                  |  |
|----------------------------------|--|
| <b>Domain</b>                    | Destroyed  |
| <b>HSM SO Role</b>               | Destroyed  |
| <b>Partition SO Role</b>         | Destroyed  |
| <b>Auditor Role</b>              | Destroyed  |
| <b>Partition Roles</b>           | Destroyed  |
| <b>HSM or Partition/Contents</b> | HSM/Destroyed  |
| <b>HSM Policies</b>              | Unchanged  |
| <b>RPV</b>                       | Unchanged  |
| <b>Messaging</b>                 | <p>WARNING: This operation will rollback your HSM to the previous firmware version !!!</p> <ol style="list-style-type: none"> <li>(1) This is a destructive operation.</li> <li>(2) You will lose all your partitions.</li> <li>(3) You may lose some capabilities.</li> <li>(4) You must re-initialize the HSM.</li> <li>(5) If the PED use is remote, you must re-connect it.</li> </ol> |

**Partition Initialize When Zeroized (hard init)**

|                                  |   |
|----------------------------------|---|
| <b>Domain</b>                    | Unchanged   |
| <b>HSM SO Role</b>               | Unchanged   |
| <b>Partition SO Role</b>         | Destroyed   |
| <b>Auditor Role</b>              | Unchanged   |
| <b>Partition Roles</b>           | Destroyed   |
| <b>HSM or Partition/Contents</b> | Partition/Destroyed   |
| <b>HSM Policies</b>              | Unchanged   |
| <b>RPV</b>                       | Unchanged   |
| <b>Messaging</b>                 | You are about to initialize the partition. All contents of the partition will be destroyed. |

**Partition Initialize From Non-Zeroized State (soft init)**

|                                  |  |
|----------------------------------|--|
| <b>Domain</b>                    | Unchanged  |
| <b>HSM SO Role</b>               | Unchanged  |
| <b>Partition SO Role</b>         | Destroyed  |
| <b>Auditor Role</b>              | Unchanged  |
| <b>Partition Roles</b>           | Destroyed  |
| <b>HSM or Partition/Contents</b> | Partition/Destroyed  |
| <b>HSM Policies</b>              | Unchanged  |
| <b>RPV</b>                       | Unchanged  |
| <b>Messaging</b>                 | You are about to initialize the partition that is already initialized. All contents of the partition will be destroyed. You are required to provide the current Partition SO password. |

**Elsewhere**

Certain other actions can sometimes cause collateral changes to the HSM, like firmware update. They usually do not affect contents, unless a partition is full and the action changes the size of partitions or changes the amount of space-per-partition that is taken by overhead/infrastructure. These are discussed elsewhere.



# CHAPTER 9: Monitoring the HSM

Thales provides different methods of monitoring activity on the HSM. This chapter contains the following sections:

- > ["HSM Status Values" below](#)
- > ["System Operational and Error Messages" on the next page](#)
- > ["Performance Monitoring" on page 189](#)
- > ["Partition Utilization Metrics" on page 190](#)
- > ["Cryptographic Module and Token Return Codes" on page 192](#)
- > ["Library Codes" on page 210](#)
- > ["Vendor-Defined Return Codes" on page 215](#)
- > ["HSM Alarm Codes" on page 220](#)

Refer also to [About the Syslog and SNMP Monitoring Guide](#).

## HSM Status Values

Each HSM administrative slot shown in a LunaCM slot listing includes an HSM status. Here are the possible values and what they mean, and what is required to recover from each one. In LunaSH, this information is displayed under *HSM Details* by running **hsm show**.

| Indicated Status of HSM | Meaning   | Recovery   |
|-------------------------|---|--|
| OK                      | The HSM is in a good state, working properly.                     | n/a  |
| Zeroized                | The HSM is in zeroized state. All objects and roles are unusable. | HSM initialization is required before the HSM can be used again. "Hard init" - HSM SO and domain are gone, no authentication required. (see Note1) |
| Decommissioned          | The HSM has been decommissioned.                                  | HSM initialization is required before the HSM can be used again. "Hard init" - HSM SO and domain are gone, no authentication required. (see Note1) |
| Transport Mode          | The HSM is in Secure Transport Mode.                              | STM must be disabled before the HSM can be used.   |

| Indicated Status of HSM        | Meaning  | Recovery   |
|--------------------------------|--|--|
| Transport Mode, zeroized       | The HSM is in Secure Transport Mode, and is also zeroized.   | STM must be disabled, and then HSM initialization is required before the HSM can be used.  |
| Transport Mode, Decommissioned | The HSM is in Secure Transport Mode, and has been decommissioned.  | STM must be disabled, and then HSM initialization is required before the HSM can be used.  |
| Hardware Tamper                | The HSM has been tampered. (MTK is destroyed and must be rebuilt from recovery vectors.)   | Reboot the host or restart the HSM. The event is logged  |
| Hardware Tamper, Zeroized      | The HSM has been tampered. (MTK is destroyed and must be rebuilt from recovery vectors.)<br>The HSM is also in zeroized state. All objects and roles are unusable. | Reboot the host or restart the HSM. The event is logged.<br>HSM initialization is required before the HSM can be used again. HSM SO and domain are gone, no authentication required. (see Note1) |
| HSM Tamper, Decommissioned     | The HSM has been tampered. (MTK is destroyed and must be rebuilt from recovery vectors.)<br>The HSM has also been decommissioned.                                  | Reboot the host or restart the HSM. The event is logged.<br>HSM initialization is required before the HSM can be used again. HSM SO and domain are gone, no authentication required. (see Note1) |

**NOTE1:** A condition, not reported above, preserves the HSM SO and the associated Domain, while SO objects and all application partitions and contents are destroyed. In this case, HSM SO login is required to perform a "soft init". See ["Initializing the HSM" on page 149](#) for more information.

For a comparison of various destruction or denial actions on the HSM, see ["Comparison of Destruction/Denial Actions" on page 270](#).

## System Operational and Error Messages

### Extra slots that say "token not present"

This happens for two reasons:

- > PKCS#11 originated in a world of software cryptography, which only later acknowledged the existence of Hardware Security Modules, so initially it did not have the concept of physically removable crypto slots. PKCS#11 requires a static list of slots when an application starts. The cryptographic "token" can be inserted into, or removed from a slot dynamically (by a user), for the duration of the application.

- > When the token is inserted, the running application must be able to detect that token. When the token is removed, the running application gets "token not present". Because we allow for the possibility of backup, we routinely declare 'place-holder' slots that might later be filled by a physical Luna USB HSM 7 or a Luna Backup HSM.

In the `Chrystoki.conf` file (or the Windows `crystoki.ini` file), for Luna USB HSM 7, you can remove the empty slots by modifying the `CardReader` entry, like this:

```
CardReader = {
  LunaG5Slots=0;
}
```

For Luna Network HSM 7, which has its configuration file internal to the appliance, and not directly accessible for modification, you cannot change the default cryptographic slot allotments.

## Error: 'hsm update firmware' failed. (10A0B : LUNA\_RET\_OPERATION\_RESTRICTED) when attempting to perform hsm update firmware

You must ensure that STM is disabled before you run the firmware update.

Also, as with any update, you should backup any important HSM contents before proceeding.

## LUNA\_RET\_OPERATION\_RESTRICTED when attempting to perform a restore operation

Did you perform the backup before Functionality Modules (FMs) were enabled on the HSM? Enabling FMs allows injection of software into the HSM, which makes it inherently less secure than an HSM that has never had FMs enabled. The cloning operation (used to perform backup and restore) recognizes the state of the source and target devices, and can refuse to transfer objects from a more secure device to a less-secure device.

In general, to ensure that you will be able to backup and restore (with partition archive commands) or clone directly with clone commands or include partitions in HA groups (which also uses cloning), ensure that partition policies are set the same on the involved partitions.

## KR\_ECC\_POINT\_INVALID Error when decrypting a file encrypted from BSAFE through ECIES using ECC key with any of the curves from the x9\_t2 section

As indicated on the BSAFE web site, they support only the NIST-approved curves (prime, Binary, and Koblitz). That includes most/all the curves from test items 0 through 37 in CK Demo: the "secp", "X9\_62\_prime", and "sect" curves.

The X9.62 curves that are failing in this task are X9.62 binary/char2 curves which do not appear to be supported by BSAFE. So, you appear to be encountering a BSAFE limitation and not a Luna HSM problem.

## Error during SSL Connect (RC\_OPERATION\_TIMED\_OUT) logged to /var/log/messages by the Luna HSM Client

It means that the client did not receive the SSL handshake response from the appliance within 20 seconds (hard coded).

The following is a list of some potential causes:

- > Network issue.

- > Appliance is under heavy load with connection requests - this can happen at startup/restart, if client applications attempt to (re-)assert hundreds of connections all at once, without staging or staggering them, and the initial setup handshakes take too long for some transactions (start-up bottleneck). After a large number of simultaneous connections has been successfully established, they can be maintained without further problem.
- > Appliance is under heavy load servicing crypto requests from connected clients.
- > Appliance was powered down (perhaps the power plug was pulled) in the middle of the handshake.
- > The client computer might be experiencing high CPU load, causing it to occasionally delay responses to the appliance.

## Error during shutdown like "PolicyKit daemon disconnected from the bus. We are no longer a registered authenticated agent. Unrecoverable Error: Cannot get child exit status"

This messaging is normal and expected: communication and authentication services have already closed; the admin user is no longer authenticated and connected to the appliance at this stage of shutdown.

## Slow/interrupted response from the HSM, and the "hsm show" command shows LUNA\_RET\_SM\_SESSION\_REALLOC\_ERROR

```
Appliance Details:
=====
Software Version:          7.0.0
Error: 'hsm show' failed. (310102 : LUNA_RET_SM_SESSION_REALLOC_ERROR)
```

Command Result : 65535 (Luna Shell execution)

The error LUNA\_RET\_SM\_SESSION\_REALLOC\_ERROR means the HSM cannot expand the session table.

The HSM maintains a table for all of the open sessions. For performance reasons, the table is quite small initially. As sessions are opened (and not closed) the table fills up. When the table gets full, the HSM tries to expand the table. If there is not enough available RAM to grow the table, this error is returned.

RAM can be used up by an application that creates and does not delete a large number of session objects, as well as by an application that opens and fails to close a large number of sessions.

The obvious solution is proper housekeeping. Your applications must clean up after themselves, by closing sessions that are no longer in use - this deletes session objects associated with those sessions. If your application practice is to have long-lived sessions, and to open many objects in a given session, then your application should explicitly delete those session objects as soon as each one is no longer necessary.

By far, we see more of the former problem - abandoned sessions - and very often in conjunction with Java-based applications. Proper garbage collection includes deleting session objects when they are no longer useful, or simply closing sessions as soon as they are not required. Formally closing a session (or stopping/restarting the HSM) deletes all session objects within each affected session. These actions keep the session table small, so it uses the least possible HSM volatile memory.

## Low Battery Message

The HSM card used in the Luna Network HSM 7 and Luna PCIe HSM 7 products, is equipped with a non-replaceable battery that is expected to last the life of the product. If you notice a log message or other warning about 'battery low', or similar, contact Technical Support.

## Performance Monitoring

An HSM administrator might find it helpful to know how busy the HSM is and at what percentage of its capacity it has been running.

The HSM Information Monitor is a use counter that provides an indication of momentary and cumulative resource usage on the HSM, in the form of a percentage. The HSM firmware tracks the overall time elapsed since the last reset (Up-Time), and the overall time during which the processor was not performing useful work (Idle-Time).

On request, the HSM calculates "Busy-time" over an interval, by subtracting Idle-time for that interval from Up-time for the interval. Then, the load on the processor is calculated as the Busy-time divided by the Up-time, and expressed as a percentage.

You can use the available commands for a single, one-off query, which actually takes an initial reading and then another, five seconds later (the default setting), in order to calculate and show the one-time difference.

You can specify a sampling interval (five seconds is the shortest) and a number of repetitions for an extended view of processor activity/resource usage. The resulting records, showing the time of each measurement, the percentage value at that time, and the difference from the previous measurement, can be output to a file that you import into other tools to analyze and graph the trends.

By watching trends and correlating with what your application is doing, you can:

- > Determine the kinds of loads you are placing on the HSM.
- > Seek efficiencies in how your applications are coded and configured.
- > Plan for expansion or upgrades of your existing HSM infrastructure.
- > Plan for upgrades of electrical capacity and HVAC capacity.

## Notes about Monitor/Counter Behavior

When performing certain operations the HSM reaches its maximum performance capability before the counter reaches 100%. This occurs because the counter measures the load on the HSM's CPU and the CPU is able to saturate the asymmetric engines and still have capacity to perform other actions.

Also, symmetric cryptographic operations cause the counter to quickly rise to 90% even though there is significant remaining capacity. This behavior occurs because, as the HSM receives more concurrent symmetric commands, its CPU is able to handle them more efficiently (by performing them in bulk) – thus achieving more throughput from the same number of CPU cycles.

See `lunash:> hsm information`.

## Partition Utilization Metrics

In order to ensure the quality of service (QoS) that you provide to applications that make use of HSM partitions, it is first necessary to know how the users and applications are making use of the HSM resources - that is, the distribution of demand.

For an HSM with a single application partition, it can be helpful to know what type of load is being imposed on the HSM and the enumeration and categorization of operations that are being performed. Application developers might have a good idea of the expected ratio of operations, but the operations team managing the application servers would like to know the real-world utilization, for their planning and management purposes.

For a Luna Network HSM 7 with multiple partitions that are sharing the space and the processing resources of the HSM, it is useful to know which partitions are presenting the greatest load, and the kinds of operations that are most common or frequent. That knowledge aids in resource planning and possible relocation or reallocation of partitions to ensure reliable service for all users.

**NOTE** Utilization metrics are based on *utilization counters* that track operations by category. This is not to be confused with *usage counters*, that track and limit the number of times a key or certificate is allowed to be used.

This feature requires minimum [Luna HSM Firmware 7.3.0](#), [Luna Network HSM 7 Appliance Software 7.3.0](#), and [Luna HSM Client 7.3.0](#).

### Rules of acquisition

Utilization Metrics count these operations within category "bins" per partition:

- > Sign
- > Verify
- > Encrypt
- > Decrypt
- > Key generate
- > Key derive

Operations not in that list do not increment any counter. That is, an operation request to the HSM increments counters in 0 or more bins. The list might expand in future releases. Each bin has a single counter that counts how many requests have been received from the host, since the last counter-reset order or power cycle. Counters for a partition can be read and reset as a single operation, or as two separate operations.

The utilization counters count *requests* to the HSM, because, while successful requests are expected and are counted, unsuccessful requests also consume resources and therefore need to be counted as well. Any request that fails on the host - meaning it does not reach the HSM - is not counted, because it did not use any HSM resources.

Utilization counters are volatile, and therefore are lost in the event of a power failure. If they are valued, they should be polled regularly and the results kept in non-volatile storage on the host.

## Availability of Partition Utilization Metrics

Utilization metrics are supported by [Luna HSM Firmware 7.3.0](#) and newer, using HSM-level policy **49: Allow Partition Utilization Metrics**. That policy is off (value 0) by default, as it is not required in all use-cases, and is most useful where multiple applications use the HSM.

**NOTE** The Utilization Metrics feature allows the HSM SO to know which operations are being performed on the HSM. This information is normally available only to the Auditor when audit logging is turned on. However, while the SO can see a record of cryptographic operations, there is no visibility as to which keys are being used.

Setting the policy on (value 1) enables utilization metrics for all partitions including the Admin partition. Changing the policy is not destructive in either direction (off-to-on or on-to-off).

The **hsm qos metrics show** command allows you to view the current utilization counter values for all partitions, and overall counts for the entire HSM, or to export the current counts to a file, without resetting the counters.

The **hsm qos metrics reset** command allows you to reset to zero the current utilization counter values for all partitions; additionally, you have the option to view the current counts or to export the current counts to a file, without losing any counts between the view/export action and the reset action.

### To access the Partition Utilization Metrics feature

1. Ensure that your HSM is at [Luna HSM Firmware 7.3.0](#) or newer (if needed, upgrade to a suitable version; see ["Updating the Luna HSM Firmware" on page 233](#)).
2. Log in as HSM SO (see ["Logging In as HSM Security Officer" on page 154](#)).  
lunash:> **hsm login**
3. Enable HSM policy **49: Allow Partition Utilization Metrics**.  
lunash:> **hsm changePolicy -policy 49 -value 1**

### To view or save Partition Utilization Metrics without resetting

lunash:> **hsm qos metrics show**

### To reset the Partition Utilization Metrics counters to zero

Metrics are reset whenever power is lost to the HSM or the HSM is reset, or the HSM is initialized. These events do not save the metrics.

To reset the metrics without exporting:

lunash:> **hsm qos metrics reset**

### To reset the Partition Utilization Metrics counters to zero while also viewing or exporting the information

lunash:> **hsm qos metrics reset -export <filename>**

The current counter values are saved to a named file before they are zeroed.

lunash:> **hsm qos metrics reset -display**

The counter data is displayed but not saved.

## Cryptographic Module and Token Return Codes

The following table summarizes HSM error codes:

| HSM Error                               | Hex Code   | PKCS#11 or SFNT Defined CKR Error    |
|---|------------|--------------------------------------|
| LUNA_RET_OK                             | 0x00000000 | CKR_OK                               |
| LUNA_RET_CANCEL                         | 0x00010000 | CKR_CANCEL                           |
| LUNA_RET_FLAGS_INVALID                  | 0x00040000 | CKR_FLAGS_INVALID, removed from v2.0 |
| LUNA_RET_TOKEN_NOT_PRESENT              | 0x00E00000 | CKR_TOKEN_NOT_PRESENT                |
| LUNA_RET_FORMER_INVALID_ENTRY_TYPE      | 0x00300130 | CKR_DEVICE_ERROR                     |
| LUNA_RET_SP_TX_ERROR                    | 0x00300131 | CKR_DEVICE_ERROR                     |
| LUNA_RET_SP_RX_ERROR                    | 0x00300132 | CKR_DEVICE_ERROR                     |
| LUNA_RET_PED_ID_INVALID                 | 0x00300140 | CKR_DEVICE_ERROR                     |
| LUNA_RET_PED_UNSUPPORTED_PROTOCOL       | 0x00300141 | CKR_DEVICE_ERROR                     |
| LUNA_RET_PED_UNPLUGGED                  | 0x00300142 | CKR_PED_UNPLUGGED                    |
| LUNA_RET_PED_ERROR                      | 0x00300144 | CKR_DEVICE_ERROR                     |
| LUNA_RET_PED_UNSUPPORTED_CRYPTOPROTOCOL | 0x00300145 | CKR_DEVICE_ERROR                     |
| LUNA_RET_PED_DEK_INVALID                | 0x00300146 | CKR_DEVICE_ERROR                     |
| LUNA_RET_PED_CLIENT_NOT_RUNNING         | 0x00300147 | CKR_PED_CLIENT_NOT_RUNNING           |
| LUNA_RET_CL_ALIGNMENT_ERROR             | 0x00300200 | CKR_DEVICE_ERROR                     |
| LUNA_RET_CL_QUEUE_LOCATION_ERROR        | 0x00300201 | CKR_DEVICE_ERROR                     |
| LUNA_RET_CL_QUEUE_OVERLAP_ERROR         | 0x00300202 | CKR_DEVICE_ERROR                     |
| LUNA_RET_CL_TRANSMISSION_ERROR          | 0x00300203 | CKR_DEVICE_ERROR                     |
| LUNA_RET_CL_NO_TRANSMISSION             | 0x00300204 | CKR_DEVICE_ERROR                     |



| HSM Error                                   | Hex Code   | PKCS#11 or SFNT Defined CKR Error |
|---|------------|-----------------------------------|
| LUNA_RET_CL_COMMAND_MALFORMED               | 0x00300205 | CKR_DEVICE_ERROR                  |
| LUNA_RET_CL_MAILBOXES_NOT_AVAILABLE         | 0x00300206 | CKR_DEVICE_ERROR                  |
| LUNA_RET_MM_NOT_ENOUGH_MEMORY               | 0x00310000 | CKR_DEVICE_MEMORY †               |
| LUNA_RET_MM_INVALID_HANDLE                  | 0x00310001 | CKR_DEVICE_MEMORY †               |
| LUNA_RET_MM_USAGE_ALREADY_SET               | 0x00310002 | CKR_DEVICE_MEMORY †               |
| LUNA_RET_MM_ACCESS_OUTSIDE_ALLOCATION_RANGE | 0x00310003 | CKR_DEVICE_MEMORY †               |
| LUNA_RET_MM_INVALID_USAGE                   | 0x00310004 | CKR_DEVICE_MEMORY †               |
| LUNA_RET_MM_ITERATOR_PAST_END               | 0x00310005 | CKR_DEVICE_MEMORY †               |
| LUNA_RET_MM_FATAL_ERROR                     | 0x00310006 | CKR_DEVICE_MEMORY †               |
| LUNA_RET_MEMORY_ALLOCATION_FAILED           | 0x00310007 | CKR_DEVICE_MEMORY †               |
| LUNA_RET_TEMPLATE_INCOMPLETE                | 0x00D00000 | CKR_TEMPLATE_INCOMPLETE           |
| LUNA_RET_TEMPLATE_INCONSISTENT              | 0x00D10000 | CKR_TEMPLATE_INCONSISTENT*        |
| LUNA_RET_ATTRIBUTE_TYPE_INVALID             | 0x00120000 | CKR_ATTRIBUTE_TYPE_INVALID        |
| LUNA_RET_ATTRIBUTE_VALUE_INVALID            | 0x00130000 | CKR_ATTRIBUTE_VALUE_INVALID       |
| LUNA_RET_ATTRIBUTE_READ_ONLY                | 0x00100000 | CKR_ATTRIBUTE_READ_ONLY           |
| LUNA_RET_ATTRIBUTE_SENSITIVE                | 0x00110000 | CKR_ATTRIBUTE_SENSITIVE           |
| LUNA_RET_OBJECT_HANDLE_INVALID              | 0x00820000 | CKR_OBJECT_HANDLE_INVALID         |
| LUNA_RET_MAX_OBJECT_COUNT                   | 0x00820001 | CKR_MAX_OBJECT_COUNT_EXCEEDED     |
| LUNA_RET_ATTRIBUTE_NOT_FOUND                | 0x00120010 | CKR_ATTRIBUTE_TYPE_INVALID        |
| LUNA_RET_CAN_NOT_CREATE_SECRET_KEY          | 0x00D10011 | CKR_TEMPLATE_INCONSISTENT         |
| LUNA_RET_CAN_NOT_CREATE_PRIVATE_KEY         | 0x00D10012 | CKR_TEMPLATE_INCONSISTENT         |

| HSM Error  | Hex Code   | PKCS#11 or SFNT Defined CKR Error |
|--|------------|-----------------------------------|
| LUNA_RET_SECRET_KEY_MUST_BE_SENSITIVE              | 0x00130013 | CKR_ATTRIBUTE_VALUE_INVALID       |
| LUNA_RET_SECRET_KEY_MUST_HAVE_SENSITIVE_ATTRIBUTE  | 0x00D00014 | CKR_TEMPLATE_INCOMPLETE           |
| LUNA_RET_PRIVATE_KEY_MUST_BE_SENSITIVE             | 0x00130015 | CKR_ATTRIBUTE_VALUE_INVALID       |
| LUNA_RET_PRIVATE_KEY_MUST_HAVE_SENSITIVE_ATTRIBUTE | 0x00D00016 | CKR_TEMPLATE_INCOMPLETE           |
| LUNA_RET_SIGNING_KEY_MUST_BE_LOCAL                 | 0x00680001 | CKR_KEY_FUNCTION_NOT_PERMITTED    |
| LUNA_RET_MULTI_FUNCTION_KEYS_NOT_ALLOWED           | 0x00D10018 | CKR_TEMPLATE_INCONSISTENT         |
| LUNA_RET_CAN_NOT_CHANGE_KEY_FUNCTION               | 0x00100019 | CKR_ATTRIBUTE_READ_ONLY           |
| LUNA_RET_KEY_SIZE_RANGE                            | 0x00620000 | CKR_KEY_SIZE_RANGE                |
| LUNA_RET_KEY_TYPE_INCONSISTENT                     | 0x00630000 | CKR_KEY_TYPE_INCONSISTENT         |
| LUNA_RET_KEY_INVALID_FOR_OPERATION                 | 0x00630001 | CKR_KEY_TYPE_INCONSISTENT         |
| LUNA_RET_KEY_PARITY                                | 0x00630002 | CKR_KEY_TYPE_INCONSISTENT         |
| LUNA_RET_KEY_UNEXTRACTABLE                         | 0x006a0000 | CKR_KEY_UNEXTRACTABLE             |
| LUNA_RET_KEY_EXTRACTABLE                           | 0x006a0001 | KR_KEY_UNEXTRACTABLE              |
| LUNA_RET_KEY_INDIGESTIBLE                          | 0x00670000 | CKR_KEY_INDIGESTIBLE              |
| LUNA_RET_KEY_NOT_WRAPPABLE                         | 0x00690000 | CKR_KEY_NOT_WRAPPABLE             |
| LUNA_RET_KEY_NOT_UNWRAPPABLE                       | 0x00690001 | CKR_KEY_NOT_WRAPPABLE             |
| LUNA_RET_ARGUMENTS_BAD                             | 0x00070000 | CKR_ARGUMENTS_BAD                 |
| LUNA_RET_INVALID_ENTRY_TYPE                        | 0x00070001 | CKR_INVALID_ENTRY_TYPE            |
| LUNA_RET_DATA_INVALID                              | 0x00200000 | CKR_DATA_INVALID                  |

| HSM Error                        | Hex Code   | PKCS#11 or SFNT Defined CKR Error |
|----------------------------------|------------|-----------------------------------|
| LUNA_RET_SM_DATA_INVALID         | 0x00200002 | CKR_DATA_INVALID                  |
| LUNA_RET_NO_RNG_SEED             | 0x00200015 | CKR_DATA_INVALID                  |
| LUNA_RET_FUNCTION_NOT_SUPPORTED  | 0x00540000 | CKR_FUNCTION_NOT_SUPPORTED        |
| LUNA_RET_NO_OFFBOARD_STORAGE     | 0x00540001 | CKR_FUNCTION_NOT_SUPPORTED        |
| LUNA_RET_CL_COMMAND_NON_BACKUP   | 0x00540002 | CKR_FUNCTION_NOT_SUPPORTED        |
| LUNA_RET_BUFFER_TOO_SMALL        | 0x01500000 | CKR_BUFFER_TOO_SMALL              |
| LUNA_RET_DATA_LEN_RANGE          | 0x00210000 | CKR_DATA_LEN_RANGE                |
| LUNA_RET_GENERAL_ERROR           | 0x00050000 | CKR_GENERAL_ERROR                 |
| LUNA_RET_DEVICE_ERROR            | 0x00300000 | CKR_DEVICE_ERROR                  |
| LUNA_RET_UNKNOWN_COMMAND         | 0x00300001 | CKR_FUNCTION_NOT_SUPPORTED        |
| LUNA_RET_TOKEN_LOCKED_OUT        | 0x00300002 | CKR_PIN_LOCKED                    |
| LUNA_RET_RNG_ERROR               | 0x00300003 | CKR_DEVICE_ERROR                  |
| LUNA_RET_DES_SELF_TEST_FAILURE   | 0x00300004 | CKR_DEVICE_ERROR                  |
| LUNA_RET_CAST_SELF_TEST_FAILURE  | 0x00300005 | CKR_DEVICE_ERROR                  |
| LUNA_RET_CAST3_SELF_TEST_FAILURE | 0x00300006 | CKR_DEVICE_ERROR                  |
| LUNA_RET_CAST5_SELF_TEST_FAILURE | 0x00300007 | CKR_DEVICE_ERROR                  |
| LUNA_RET_MD2_SELF_TEST_FAILURE   | 0x00300008 | CKR_DEVICE_ERROR                  |
| LUNA_RET_MD5_SELF_TEST_FAILURE   | 0x00300009 | CKR_DEVICE_ERROR                  |
| LUNA_RET_SHA_SELF_TEST_FAILURE   | 0x0030000a | CKR_DEVICE_ERROR                  |
| LUNA_RET_RSA_SELF_TEST_FAILURE   | 0x0030000b | CKR_DEVICE_ERROR                  |

| HSM Error                                   | Hex Code   | PKCS#11 or SFNT Defined CKR Error |
|---|------------|-----------------------------------|
| LUNA_RET_RC2_SELF_TEST_FAILURE              | 0x0030000c | CKR_DEVICE_ERROR                  |
| LUNA_RET_RC4_SELF_TEST_FAILURE              | 0x0030000d | CKR_DEVICE_ERROR                  |
| LUNA_RET_RC5_SELF_TEST_FAILURE              | 0x0030000e | CKR_DEVICE_ERROR                  |
| LUNA_RET_SO_LOGIN_FAILURE_THRESHOLD         | 0x0030000f | CKR_SO_LOGIN_FAILURE_THRESHOLD    |
| LUNA_RET_RNG_SELF_TEST_FAILURE              | 0x00300010 | CKR_DEVICE_ERROR                  |
| LUNA_RET_SM_UNKNOWN_COMMAND                 | 0x00300011 | CKR_DEVICE_ERROR                  |
| LUNA_RET_UM_TSN_MISSING                     | 0x00300012 | CKR_DEVICE_ERROR                  |
| LUNA_RET_SM_TSV_MISSING                     | 0x00300013 | CKR_DEVICE_ERROR                  |
| LUNA_RET_SM_UNKNOWN_TOSM_STATE              | 0x00300014 | CKR_DEVICE_ERROR                  |
| LUNA_RET_DSA_PARAM_GEN_FAILURE              | 0x00300015 | CKR_DEVICE_ERROR                  |
| LUNA_RET_DSA_SELF_TEST_FAILURE              | 0x00300016 | CKR_DEVICE_ERROR                  |
| LUNA_RET_SEED_SELF_TEST_FAILURE             | 0x00300017 | CKR_DEVICE_ERROR                  |
| LUNA_RET_AES_SELF_TEST_FAILURE              | 0x00300018 | CKR_DEVICE_ERROR                  |
| LUNA_RET_FUNCTION_NOT_SUPPORTED_BY_HARDWARE | 0x00300019 | CKR_DEVICE_ERROR                  |
| LUNA_RET_HAS160_SELF_TEST_FAILURE           | 0x0030001a | CKR_DEVICE_ERROR                  |
| LUNA_RET_KCDSA_PARAM_GEN_FAILURE            | 0x0030001b | CKR_DEVICE_ERROR                  |
| LUNA_RET_KCDSA_SELF_TEST_FAILURE            | 0x0030001c | CKR_DEVICE_ERROR                  |
| LUNA_RET_HSM_INTERNAL_BUFFER_TOO_SMALL      | 0x0030001d | CKR_DEVICE_ERROR                  |
| LUNA_RET_COUNTER_WRAPAROUND                 | 0x0030001e | CKR_DEVICE_ERROR                  |
| LUNA_RET_TIMEOUT                            | 0x0030001f | CKR_TIMEOUT                       |
| LUNA_RET_NOT_READY                          | 0x00300020 | CKR_DEVICE_ERROR                  |

| HSM Error                            | Hex Code   | PKCS#11 or SFNT Defined CKR Error |
|--------------------------------------|------------|-----------------------------------|
| LUNA_RET_RETRY                       | 0x00300021 | CKR_DEVICE_ERROR                  |
| LUNA_RET_SHA1_RSA_SELF_TEST_FAILURE  | 0x00300022 | CKR_DEVICE_ERROR                  |
| LUNA_RET_SELF_TEST_FAILURE           | 0x00300023 | CKR_DEVICE_ERROR                  |
| LUNA_RET_INCOMPATIBLE                | 0x00300024 | CKR_DEVICE_ERROR                  |
| LUNA_RET_RIPEMD160_SELF_TEST_FAILURE | 0x00300034 | CKR_DEVICE_ERROR                  |
| LUNA_RET_TOKEN_LOCKED_OUT_CL         | 0x00300100 | CKR_DEVICE_ERROR                  |
| LUNA_RET_TOKEN_LOCKED_OUT_MM         | 0x00300101 | CKR_DEVICE_ERROR                  |
| LUNA_RET_TOKEN_LOCKED_OUT_UM         | 0x00300102 | CKR_DEVICE_ERROR                  |
| LUNA_RET_TOKEN_LOCKED_OUT_SM         | 0x00300103 | CKR_DEVICE_ERROR                  |
| LUNA_RET_TOKEN_LOCKED_OUT_RN         | 0x00300104 | CKR_DEVICE_ERROR                  |
| LUNA_RET_TOKEN_LOCKED_OUT_CA         | 0x00300105 | CKR_DEVICE_ERROR                  |
| LUNA_RET_TOKEN_LOCKED_OUT_PM         | 0x00300106 | CKR_DEVICE_ERROR                  |
| LUNA_RET_TOKEN_LOCKED_OUT_OH         | 0x00300107 | CKR_DEVICE_ERROR                  |
| LUNA_RET_TOKEN_LOCKED_OUT_CCM        | 0x00300108 | CKR_DEVICE_ERROR                  |
| LUNA_RET_TOKEN_LOCKED_OUT_SHA_DIGEST | 0x00300109 | CKR_DEVICE_ERROR                  |
| LUNA_RET_SM_ACCESS_REALLOC_ERROR     | 0x00310101 | CKR_DEVICE_ERROR                  |
| LUNA_RET_SM_SESSION_REALLOC_ERROR    | 0x00310102 | CKR_DEVICE_ERROR                  |
| LUNA_RET_SM_MEMORY_ALLOCATION_ERROR  | 0x00310103 | CKR_DEVICE_ERROR                  |
| LUNA_RET_ENCRYPTED_DATA_INVALID      | 0x00400000 | CKR_ENCRYPTED_DATA_INVALID        |
| LUNA_RET_ENCRYPTED_DATA_LEN_RANGE    | 0x00410000 | CKR_ENCRYPTED_DATA_LEN_RANGE      |
| LUNA_RET_FUNCTION_CANCELED           | 0x00500000 | CKR_FUNCTION_CANCELED             |
| LUNA_RET_KEY_HANDLE_INVALID          | 0x00600000 | CKR_KEY_HANDLE_INVALID            |

| HSM Error                                    | Hex Code   | PKCS#11 or SFNT Defined CKR Error    |
|--|------------|--------------------------------------|
| LUNA_RET_MECHANISM_INVALID                   | 0x00700000 | CKR_MECHANISM_INVALID                |
| LUNA_RET_MECHANISM_PARAM_INVALID             | 0x00710000 | CKR_MECHANISM_PARAM_INVALID          |
| LUNA_RET_OPERATION_ACTIVE                    | 0x00900000 | CKR_OPERATION_ACTIVE                 |
| LUNA_RET_OPERATION_NOT_INITIALIZED           | 0x00910000 | CKR_OPERATION_NOT_INITIALIZED        |
| LUNA_RET_UM_PIN_INCORRECT                    | 0x00a00000 | CKR_PIN_INCORRECT                    |
| LUNA_RET_UM_PIN_INCORRECT_CONTAINER_ZEROIZED | 0x00a00001 | CKR_PIN_INCORRECT                    |
| LUNA_RET_UM_PIN_INCORRECT_CONTAINER_LOCKED   | 0x00a00002 | CKR_PIN_INCORRECT                    |
| LUNA_RET_UM_PIN_LEN_RANGE                    | 0x00a20000 | CKR_PIN_LEN_RANGE                    |
| LUNA_RET_SM_PIN_EXPIRED                      | 0x00a30000 | CKR_PIN_EXPIRED                      |
| LUNA_RET_SM_EXCLUSIVE_SESSION_EXISTS         | 0x00b20000 | CKR_SESSION_EXCLUSIVE_EXISTS         |
| LUNA_RET_SM_SESSION_HANDLE_INVALID           | 0x00b30000 | CKR_SESSION_HANDLE_INVALID           |
| LUNA_RET_SIGNATURE_INVALID                   | 0x00c00000 | CKR_SIGNATURE_INVALID                |
| LUNA_RET_SIGNATURE_LEN_RANGE                 | 0x00c10000 | CKR_SIGNATURE_LEN_RANGE              |
| LUNA_RET_UNWRAPPING_KEY_HANDLE_INVALID       | 0x00f00000 | CKR_UNWRAPPING_KEY_HANDLE_INVALID    |
| LUNA_RET_UNWRAPPING_KEY_SIZE_RANGE           | 0x00f10000 | CKR_UNWRAPPING_KEY_SIZE_RANGE        |
| LUNA_RET_UNWRAPPING_KEY_TYPE_INCONSISTENT    | 0x00f20000 | CKR_UNWRAPPING_KEY_TYPE_INCONSISTENT |
| LUNA_RET_USER_ALREADY_LOGGED_IN              | 0x01000000 | CKR_USER_ALREADY_LOGGED_IN           |

| HSM Error                                 | Hex Code   | PKCS#11 or SFNT Defined CKR Error  |
|---|------------|------------------------------------|
| LUNA_RET_SM_OTHER_USER_LOGGED_IN          | 0x01000001 | CKR_USER_ALREADY_LOGGED_IN         |
| LUNA_RET_USER_NOT_LOGGED_IN               | 0x01010000 | CKR_USER_NOT_LOGGED_IN             |
| LUNA_RET_SM_NOT_LOGGED_IN                 | 0x01010001 | CKR_USER_NOT_LOGGED_IN             |
| LUNA_RET_USER_PIN_NOT_INITIALIZED         | 0x01020000 | CKR_USER_PIN_NOT_INITIALIZED       |
| LUNA_RET_USER_TYPE_INVALID                | 0x01030000 | CKR_USER_TYPE_INVALID              |
| LUNA_RET_WRAPPED_KEY_INVALID              | 0x01100000 | CKR_WRAPPED_KEY_INVALID            |
| LUNA_RET_WRAPPED_KEY_LEN_RANGE            | 0x01120000 | CKR_WRAPPED_KEY_LEN_RANGE          |
| LUNA_RET_WRAPPING_KEY_HANDLE_INVALID      | 0x01130000 | CKR_WRAPPING_KEY_HANDLE_INVALID    |
| LUNA_RET_WRAPPING_KEY_SIZE_RANGE          | 0x01140000 | CKR_WRAPPING_KEY_SIZE_RANGE        |
| LUNA_RET_WRAPPING_KEY_TYPE_INCONSISTENT   | 0x01150000 | CKR_WRAPPING_KEY_TYPE_INCONSISTENT |
| LUNA_RET_CERT_VERSION_NOT_SUPPORTED       | 0x00300300 | CKR_DEVICE_ERROR                   |
| LUNA_RET_SIM_AUTHFORM_INVALID             | 0x0020011e | CKR_SIM_AUTHFORM_INVALID           |
| LUNA_RET_CCM_TOO_LARGE                    | 0x00210001 | CKR_DATA_LEN_RANGE                 |
| LUNA_RET_TEST_VS_BSAFE_FAILED             | 0x00300820 | CKR_DEVICE_ERROR                   |
| LUNA_RET_SFNT3120_ERROR                   | 0x00300821 | CKR_DEVICE_ERROR                   |
| LUNA_RET_SFNT3120_SELFTEST_FAILED         | 0x00300822 | CKR_DEVICE_ERROR                   |
| LUNA_RET_SFNT3120_CRC                     | 0x00300823 | CKR_DEVICE_ERROR                   |
| LUNA_RET_SFNT3120_ALG_NO_SOFTWARE_SUPPORT | 0x00300824 | CKR_DEVICE_ERROR                   |
| LUNA_RET_ISES_ERROR                       | 0x00300880 | CKR_DEVICE_ERROR                   |

| HSM Error                                    | Hex Code   | PKCS#11 or SFNT Defined CKR Error |
|--|------------|-----------------------------------|
| LUNA_RET_ISES_INIT_FAILED                    | 0x00300881 | CKR_DEVICE_ERROR                  |
| LUNA_RET_ISES_LNAU_TEST_FAILED               | 0x00300882 | CKR_DEVICE_ERROR                  |
| LUNA_RET_ISES_RNG_TEST_FAILED                | 0x00300883 | CKR_DEVICE_ERROR                  |
| LUNA_RET_ISES_CMD_FAILED                     | 0x00300884 | CKR_DEVICE_ERROR                  |
| LUNA_RET_ISES_CMD_PARAMETER_INVALID          | 0x00300885 | CKR_DEVICE_ERROR                  |
| LUNA_RET_ISES_TEST_VS_BSAFE_FAILED           | 0x00300886 | CKR_DEVICE_ERROR                  |
| LUNA_RET_RM_ELEMENT_VALUE_INVALID            | 0x00200a00 | CKR_DATA_INVALID                  |
| LUNA_RET_RM_ELEMENT_ID_INVALID               | 0x00200a01 | CKR_DATA_INVALID                  |
| LUNA_RET_RM_NO_MEMORY                        | 0x00310a02 | CKR_DEVICE_MEMORY                 |
| LUNA_RET_RM_BAD_HSM_PARAMS                   | 0x00300a03 | CKR_DEVICE_ERROR                  |
| LUNA_RET_RM_POLICY_ELEMENT_DESTRUCTIVE       | 0x00200a04 | CKR_DATA_INVALID                  |
| LUNA_RET_RM_POLICY_ELEMENT_NOT_DESTRUCTIVE   | 0x00200a05 | CKR_DATA_INVALID                  |
| LUNA_RET_RM_CONFIG_CHANGE_ILLEGAL            | 0x00010a06 | CKR_CANCEL                        |
| LUNA_RET_RM_CONFIG_CHANGE_FAILS_DEPENDENCIES | 0x00010a07 | CKR_CANCEL                        |
| LUNA_RET_LICENSE_ID_UNKNOWN                  | 0x00200a08 | CKR_DATA_INVALID                  |
| LUNA_RET_LICENSE_CAPACITY_EXCEEDED           | 0x00010a09 | CKR_LICENSE_CAPACITY_EXCEEDED     |
| LUNA_RET_RM_POLICY_WRITE_RESTRICTED          | 0x00010a0a | CKR_CANCEL                        |
| LUNA_RET_OPERATION_RESTRICTED                | 0x00010a0b | CKR_OPERATION_NOT_ALLOWED         |
| LUNA_RET_CANNOT_PERFORM_OPERATION_TWICE      | 0x00010a0c | CKR_CANCEL                        |



| HSM Error                                | Hex Code   | PKCS#11 or SFNT Defined CKR Error |
|--|------------|-----------------------------------|
| LUNA_RET_BAD_PPID                        | 0x00200a0d | CKR_DATA_INVALID                  |
| LUNA_RET_BAD_FW_VERSION                  | 0x00200a0e | CKR_DATA_INVALID                  |
| LUNA_RET_OPERATION_SHOULD_BE_DESTRUCTIVE | 0x00200a0f | CKR_DATA_INVALID                  |
| LUNA_RET_RM_CONFIG_ILLEGAL               | 0x00200a10 | CKR_DATA_INVALID                  |
| LUNA_RET_BAD_SN                          | 0x00200a11 | CKR_DATA_INVALID                  |
| LUNA_RET_CHALLENGE_TYPE_INVALID          | 0x00200b00 | CKR_DATA_INVALID                  |
| LUNA_RET_CHALLENGE_REQUIRES_PED          | 0x00010b01 | CKR_CANCEL                        |
| LUNA_RET_CHALLENGE_NOT_REQUIRED          | 0x00010b02 | CKR_CANCEL                        |
| LUNA_RET_CHALLENGE_RESPONSE_INCORRECT    | 0x00a00b03 | CKR_PIN_INCORRECT                 |
| LUNA_RET_OH_OBJECT_VERSION_INVALID       | 0x00300c00 | CKR_DEVICE_ERROR                  |
| LUNA_RET_OH_OBJECT_TYPE_INVALID          | 0x00300c01 | CKR_DEVICE_ERROR                  |
| LUNA_RET_OH_OBJECT_ALREADY_EXISTS        | 0x00010c02 | CKR_CANCEL                        |
| LUNA_RET_OH_OBJECT_OWNER_DOES_NOT_EXIST  | 0x00200c03 | CKR_DATA_INVALID                  |
| LUNA_RET_STORAGE_TYPE_INCONSISTENT       | 0x00200c04 | CKR_DATA_INVALID                  |
| LUNA_RET_CONTAINER_CAN_NOT_HAVE_MEMBERS  | 0x00200c05 | CKR_DATA_INVALID                  |
| LUNA_RET_SAVED_STATE_INVALID             | 0x01600000 | CKR_SAVED_STATE_INVALID           |
| LUNA_RET_STATE_UNSAVEABLE                | 0x01800000 | CKR_STATE_UNSAVEABLE              |
| LUNA_RET_ERROR                           | 0x80000000 | CKR_GENERAL_ERROR                 |
| LUNA_RET_CONTAINER_HANDLE_INVALID        | 0x80000001 | CKR_CONTAINER_HANDLE_INVALID      |
| LUNA_RET_INVALID_PADDING_TYPE            | 0x80000002 | CKR_DATA_INVALID                  |

| HSM Error                                 | Hex Code   | PKCS#11 or SFNT Defined CKR Error    |
|---|------------|--------------------------------------|
| LUNA_RET_NOT_FOUND                        | 0x80000007 | CKR_FUNCTION_FAILED                  |
| LUNA_RET_TOO_MANY_CONTAINERS              | 0x80000008 | CKR_TOO_MANY_CONTAINERS              |
| LUNA_RET_CONTAINER_LOCKED                 | 0x80000009 | CKR_PIN_LOCKED                       |
| LUNA_RET_CONTAINER_IS_DISABLED            | 0x8000000a | CKR_PARTITION_DISABLED               |
| LUNA_RET_SECURITY_PARAMETER_MISSING       | 0x8000000b | CKR_SECURITY_PARAMETER_MISSING       |
| LUNA_RET_DEVICE_TIMEOUT                   | 0x8000000c | CKR_DEVICE_TIMEOUT                   |
| LUNA_RET_OBJECT_DELETED                   | 0x8000000d | HSM Internal ONLY                    |
| LUNA_RET_INVALID_FUF_TARGET               | 0x8000000e | CKR_INVALID_FUF_TARGET               |
| LUNA_RET_INVALID_FUF_HEADER               | 0x8000000f | CKR_INVALID_FUF_HEADER               |
| LUNA_RET_INVALID_FUF_VERSION              | 0x80000010 | CKR_INVALID_FUF_VERSION              |
| LUNA_RET_KCV_PARAMETER_ALREADY_EXISTS     | 0x80000100 | CKR_CLONING_PARAMETER_ALREADY_EXISTS |
| LUNA_RET_KCV_PARAMETER_COULD_NOT_BE_ADDED | 0x80000101 | CKR_DEVICE_MEMORY                    |
| LUNA_RET_INVALID_CERTIFICATE_DATA         | 0x80000102 | CKR_CERTIFICATE_DATA_INVALID         |
| LUNA_RET_INVALID_CERTIFICATE_TYPE         | 0x80000103 | CKR_CERTIFICATE_DATA_INVALID         |
| LUNA_RET_INVALID_CERTIFICATE_VERSION      | 0x80000104 | CKR_CERTIFICATE_DATA_INVALID         |
| LUNA_RET_INVALID_MODULUS_SIZE             | 0x80000105 | CKR_ATTRIBUTE_VALUE_INVALID          |
| LUNA_RET_WRAPPING_ERROR                   | 0x80000107 | CKR_WRAPPING_ERROR                   |
| LUNA_RET_UNWRAPPING_ERROR                 | 0x80000108 | CKR_UNWRAPPING_ERROR                 |
| LUNA_RET_INVALID_PRIVATE_KEY_TYPE         | 0x80000109 | CKR_DATA_INVALID                     |

| HSM Error                         | Hex Code   | PKCS#11 or SFNT Defined CKR Error |
|-----------------------------------|------------|-----------------------------------|
| LUNA_RET_TSN_MISMATCH             | 0x8000010a | CKR_DATA_INVALID                  |
| LUNA_RET_KCV_PARAMETER_MISSING    | 0x8000010b | CKR_CLONING_PARAMETER_MISSING     |
| LUNA_RET_TWC_PARAMETER_MISSING    | 0x8000010c | CKR_CERTIFICATE_DATA_MISSING      |
| LUNA_RET_TUK_PARAMETER_MISSING    | 0x8000010d | CKR_CERTIFICATE_DATA_MISSING      |
| LUNA_RET_CPK_PARAMETER_MISSING    | 0x8000010e | CKR_KEY_NEEDED                    |
| LUNA_RET_MASKING_NOT_SUPPORTED    | 0x8000010f | CKR_FUNCTION_NOT_SUPPORTED        |
| LUNA_RET_INVALID_ACCESS_LEVEL     | 0x80000110 | CKR_ARGUMENTS_BAD                 |
| LUNA_RET_MAC_MISSING              | 0x80000111 | CKR_MAC_MISSING                   |
| LUNA_RET_DAC_POLICY_PID_MISMATCH  | 0x80000112 | CKR_DAC_POLICY_PID_MISMATCH       |
| LUNA_RET_DAC_MISSING              | 0x80000113 | CKR_DAC_MISSING                   |
| LUNA_RET_BAD_DAC                  | 0x80000114 | CKR_BAD_DAC                       |
| LUNA_RET_SSK_MISSING              | 0x80000115 | CKR_SSK_MISSING                   |
| LUNA_RET_BAD_MAC                  | 0x80000116 | CKR_BAD_MAC                       |
| LUNA_RET_DAK_MISSING              | 0x80000117 | CKR_DAK_MISSING                   |
| LUNA_RET_BAD_DAK                  | 0x80000118 | CKR_BAD_DAK                       |
| LUNA_RET_HOK_MISSING              | 0x80000119 | CKR_CERTIFICATE_DATA_MISSING      |
| LUNA_RET_CITS_DAK_MISSING         | 0x8000011a | CKR_CITS_DAK_MISSING              |
| LUNA_RET_SIM_AUTHORIZATION_FAILED | 0x8000011b | CKR_SIM_AUTHORIZATION_FAILED      |

| HSM Error                             | Hex Code   | PKCS#11 or SFNT Defined CKR Error |
|---------------------------------------|------------|-----------------------------------|
| LUNA_RET_SIM_VERSION_UNSUPPORTED      | 0x8000011c | CKR_SIM_VERSION_UNSUPPORTED       |
| LUNA_RET_SIM_CORRUPT_DATA             | 0x8000011d | CKR_SIM_CORRUPT_DATA              |
| LUNA_RET_ECC_MIC_MISSING              | 0x8000011e | CKR_CERTIFICATE_DATA_MISSING      |
| LUNA_RET_ECC_HOK_MISSING              | 0x8000011f | CKR_CERTIFICATE_DATA_MISSING      |
| LUNA_RET_ECC_HOC_MISSING              | 0x80000120 | CKR_CERTIFICATE_DATA_MISSING      |
| LUNA_RET_ECC_DAK_MISSING              | 0x80000121 | CKR_CERTIFICATE_DATA_MISSING      |
| LUNA_RET_ECC_DAC_MISSING              | 0x80000122 | CKR_CERTIFICATE_DATA_MISSING      |
| LUNA_RET_ROOT_CERT_MISSING            | 0x80000123 | CKR_CERTIFICATE_DATA_MISSING      |
| LUNA_RET_HOC_MISSING                  | 0x80000124 | CKR_CERTIFICATE_DATA_MISSING      |
| LUNA_RET_INVALID_CERTIFICATE_FUNCTION | 0x80000125 | CKR_CERTIFICATE_DATA_INVALID      |
| LUNA_RET_N_TOO_LARGE                  | 0x80000200 | CKR_ARGUMENTS_BAD                 |
| LUNA_RET_N_TOO_SMALL                  | 0x80000201 | CKR_ARGUMENTS_BAD                 |
| LUNA_RET_M_TOO_LARGE                  | 0x80000202 | CKR_ARGUMENTS_BAD                 |
| LUNA_RET_M_TOO_SMALL                  | 0x80000203 | CKR_ARGUMENTS_BAD                 |
| LUNA_RET_WEIGHT_TOO_LARGE             | 0x80000204 | CKR_ARGUMENTS_BAD                 |
| LUNA_RET_WEIGHT_TOO_SMALL             | 0x80000205 | CKR_ARGUMENTS_BAD                 |
| LUNA_RET_TOTAL_WEIGHT_INVALID         | 0x80000206 | CKR_ARGUMENTS_BAD                 |
| LUNA_RET_MISSING_SPLITS               | 0x80000207 | CKR_ARGUMENTS_BAD                 |

| HSM Error                               | Hex Code   | PKCS#11 or SFNT Defined CKR Error |
|---|------------|-----------------------------------|
| LUNA_RET_SPLIT_DATA_INVALID             | 0x80000208 | CKR_ARGUMENTS_BAD                 |
| LUNA_RET_SPLIT_ID_INVALID               | 0x80000209 | CKR_ARGUMENTS_BAD                 |
| LUNA_RET_M_OF_N_PARAMETER_NOT_AVAILABLE | 0x8000020a | CKR_OPERATION_NOT_INITIALIZED     |
| LUNA_RET_M_OF_N_ACTIVATION_REQUIRED     | 0x8000020b | CKR_OPERATION_NOT_INITIALIZED     |
| LUNA_RET_TOO_MANY_WEIGHTS               | 0x8000020e | CKR_ARGUMENTS_BAD                 |
| LUNA_RET_MISSING_WEIGHT_VALUE           | 0x8000020f | CKR_ARGUMENTS_BAD                 |
| LUNA_RET_MISSING_VALUE_FOR_M            | 0x80000210 | CKR_ARGUMENTS_BAD                 |
| LUNA_RET_MISSING_VALUE_FOR_N            | 0x80000211 | CKR_ARGUMENTS_BAD                 |
| LUNA_RET_MISSING_NUMBER_OF_VECTORS      | 0x80000212 | CKR_ARGUMENTS_BAD                 |
| LUNA_RET_MISSING_VECTOR                 | 0x80000213 | CKR_ARGUMENTS_BAD                 |
| LUNA_RET_VECTOR_TOO_LARGE               | 0x80000214 | CKR_ARGUMENTS_BAD                 |
| LUNA_RET_VECTOR_TOO_SMALL               | 0x80000215 | CKR_ARGUMENTS_BAD                 |
| LUNA_RET_TOO_MANY_VECTORS_PROVIDED      | 0x80000216 | CKR_ARGUMENTS_BAD                 |
| LUNA_RET_INVALID_VECTOR_SIZE            | 0x80000217 | CKR_ARGUMENTS_BAD                 |
| LUNA_RET_M_OF_N_PARAMETER_EXIST         | 0x80000218 | CKR_FUNCTION_FAILED               |
| LUNA_RET_VECTOR_VERSION_INVALID         | 0x80000219 | CKR_DATA_INVALID                  |
| LUNA_RET_VECTOR_OF_DIFFERENT_SET        | 0x8000021a | CKR_ARGUMENTS_BAD                 |
| LUNA_RET_VECTOR_DUPLICATE               | 0x8000021b | CKR_ARGUMENTS_BAD                 |
| LUNA_RET_VECTOR_TYPE_INVALID            | 0x8000021c | CKR_ARGUMENTS_BAD                 |
| LUNA_RET_MISSING_COMMAND_PARAMETER      | 0x8000021d | CKR_ARGUMENTS_BAD                 |
| LUNA_RET_M_OF_N_CLONING_IS_NOT_ALLOWED  | 0x8000021e | CKR_FUNCTION_NOT_SUPPORTED        |

| HSM Error                             | Hex Code   | PKCS#11 or SFNT Defined CKR Error |
|---------------------------------------|------------|-----------------------------------|
| LUNA_RET_M_OF_N_IS_NOT_REQUIRED       | 0x8000021f | CKR_OPERATION_NOT_INITIALIZED     |
| LUNA_RET_M_OF_N_IS_NOT_INITIALIZED    | 0x80000220 | CKR_OPERATION_NOT_INITIALIZED     |
| LUNA_RET_M_OF_N_SECRET_INVALID        | 0x80000221 | CKR_GENERAL_ERROR                 |
| LUNA_RET_CCM_NOT_PRESENT              | 0x80000300 | CKR_FUNCTION_NOT_SUPPORTED        |
| LUNA_RET_CCM_NOT_SUPPORTED            | 0x80000301 | CKR_FUNCTION_NOT_SUPPORTED        |
| LUNA_RET_CCM_UNREMOVABLE              | 0x80000302 | CKR_DATA_INVALID                  |
| LUNA_RET_CCM_CERT_INVALID             | 0x80000303 | CKR_DATA_INVALID                  |
| LUNA_RET_CCM_SIGN_INVALID             | 0x80000304 | CKR_DATA_INVALID                  |
| LUNA_RET_CCM_UPDATE_DENIED            | 0x80000305 | CKR_DATA_INVALID                  |
| LUNA_RET_CCM_FWUPDATE_DENIED          | 0x80000306 | CKR_DATA_INVALID                  |
| LUNA_RET_SM_ACCESS_ID_INVALID         | 0x80000400 | CKR_DATA_INVALID                  |
| LUNA_RET_SM_ACCESS_ALREADY_EXISTS     | 0x80000401 | CKR_DATA_INVALID                  |
| LUNA_RET_SM_MULTIPLE_ACCESS_DISABLED  | 0x80000402 | CKR_FUNCTION_NOT_SUPPORTED        |
| LUNA_RET_SM_UNKNOWN_ACCESS_TYPE       | 0x80000403 | CKR_ARGUMENTS_BAD                 |
| LUNA_RET_SM_BAD_ACCESS_HANDLE         | 0x80000404 | CKR_DATA_INVALID                  |
| LUNA_RET_SM_BAD_CONTEXT_NUMBER        | 0x80000405 | CKR_DATA_INVALID                  |
| LUNA_RET_SM_UNKNOWN_SESSION_TYPE      | 0x80000406 | CKR_DATA_INVALID                  |
| LUNA_RET_SM_CONTEXT_ALREADY_ALLOCATED | 0x80000407 | CKR_DATA_INVALID                  |
| LUNA_RET_SM_CONTEXT_NOT_ALLOCATED     | 0x80000408 | CKR_DEVICE_MEMORY                 |

| HSM Error                              | Hex Code   | PKCS#11 or SFNT Defined CKR Error |
|--|------------|-----------------------------------|
| LUNA_RET_SM_CONTEXT_BUFFER_OVERFLOW    | 0x80000409 | CKR_DEVICE_MEMORY                 |
| LUNA_RET_SM_TOSM_DOES_NOT_VALIDATE     | 0x8000040A | CKR_USER_NOT_LOGGED_IN            |
| LUNA_RET_SM_ACCESS_DOES_NOT_VALIDATE   | 0x8000040B | CKR_USER_NOT_AUTHORIZED           |
| LUNA_RET_MTK_ZEROIZED                  | 0x80000531 | CKR_MTK_ZEROIZED                  |
| LUNA_RET_MTK_STATE_INVALID             | 0x80000532 | CKR_MTK_STATE_INVALID             |
| LUNA_RET_MTK_SPLIT_INVALID             | 0x80000533 | CKR_MTK_SPLIT_INVALID             |
| LUNA_RET_INVALID_IP_PACKET             | 0x80000600 | CKR_DEVICE_ERROR                  |
| LUNA_RET_INVALID_BOARD_TYPE            | 0x80000700 | CKR_DEVICE_ERROR                  |
| LUNA_RET_ECC_NOT_SUPPORTED             | 0x80000601 | CKR_FUNCTION_NOT_SUPPORTED        |
| LUNA_RET_ECC_BUFFER_OVERFLOW           | 0x80000602 | CKR_DEVICE_ERROR                  |
| LUNA_RET_ECC_POINT_INVALID             | 0x80000603 | CKR_ECC_POINT_INVALID**           |
| LUNA_RET_ECC_SELF_TEST_FAILURE         | 0x80000604 | CKR_DEVICE_ERROR                  |
| LUNA_RET_ECC_UNKNOWN_CURVE             | 0x80000605 | CKR_ECC_UNKNOWN_CURVE             |
| LUNA_RET_HA_NOT_SUPPORTED              | 0x80000900 | CKR_FUNCTION_NOT_SUPPORTED        |
| LUNA_RET_HA_USER_NOT_INITIALIZED       | 0x80000901 | CKR_OPERATION_NOT_INITIALIZED     |
| LUNA_RET_HSM_STORAGE_FULL              | 0x80000902 | CKR_HSM_STORAGE_FULL              |
| LUNA_RET_CONTAINER_OBJECT_STORAGE_FULL | 0x80000903 | CKR_CONTAINER_OBJECT_STORAGE_FULL |
| LUNA_RET_KEY_NOT_ACTIVE                | 0x80000904 | CKR_KEY_NOT_ACTIVE                |
| LUNA_RET_CB_NOT_SUPPORTED              | 0x80000a01 | CKR_FUNCTION_NOT_SUPPORTED        |
| LUNA_RET_CB_PARAM_INVALID              | 0x80000a02 | CKR_CALLBACK_ERROR                |

| HSM Error                                | Hex Code   | PKCS#11 or SFNT Defined CKR Error |
|--|------------|-----------------------------------|
| LUNA_RET_CB_NO_MEMORY                    | 0x80000a03 | CKR_DEVICE_MEMORY                 |
| LUNA_RET_CB_TIMEOUT                      | 0x80000a04 | CKR_CALLBACK_ERROR                |
| LUNA_RET_CB_RETRY                        | 0x80000a05 | CKR_CALLBACK_ERROR                |
| LUNA_RET_CB_ABORTED                      | 0x80000a06 | CKR_CALLBACK_ERROR                |
| LUNA_RET_CB_SYS_ERROR                    | 0x80000a07 | CKR_CALLBACK_ERROR                |
| LUNA_RET_CB_HIOS_HANDLE_INVALID          | 0x80000a10 | CKR_CALLBACK_ERROR                |
| LUNA_RET_CB_HIOS_ID_INVALID              | 0x80000a11 | CKR_CALLBACK_ERROR                |
| LUNA_RET_CB_HIOS_CLOSED                  | 0x80000a12 | CKR_CALLBACK_ERROR                |
| LUNA_RET_CB_HIOS_CANCELED                | 0x80000a13 | CKR_CALLBACK_ERROR                |
| LUNA_RET_CB_HIOS_IO_ERROR                | 0x80000a14 | CKR_CALLBACK_ERROR                |
| LUNA_RET_CB_HIOS_SEND_TIMEOUT            | 0x80000a15 | CKR_CALLBACK_ERROR                |
| LUNA_RET_CB_HIOS_RECV_TIMEOUT            | 0x80000a16 | CKR_CALLBACK_ERROR                |
| LUNA_RET_CB_HIOS_STATE_INVALID           | 0x80000a17 | CKR_CALLBACK_ERROR                |
| LUNA_RET_CB_HIOS_OUTPUT_BUFFER_TOO_SMALL | 0x80000a18 | CKR_CALLBACK_ERROR                |
| LUNA_RET_CB_HIOS_INPUT_BUFFER_TOO_SMALL  | 0x80000a19 | CKR_CALLBACK_ERROR                |
| LUNA_RET_CB_HANDLE_INVALID               | 0x80000a20 | CKR_CALLBACK_ERROR                |
| LUNA_RET_CB_ID_INVALID                   | 0x80000a21 | CKR_CALLBACK_ERROR                |
| LUNA_RET_CB_REMOTE_ABORT                 | 0x80000a22 | CKR_CALLBACK_ERROR                |
| LUNA_RET_CB_REMOTE_CLOSED                | 0x80000a23 | CKR_CALLBACK_ERROR                |
| LUNA_RET_CB_REMOTE_ABANDONED             | 0x80000a24 | CKR_CALLBACK_ERROR                |
| LUNA_RET_CB_MUST_READ                    | 0x80000a25 | CKR_CALLBACK_ERROR                |



| HSM Error                                | Hex Code   | PKCS#11 or SFNT Defined CKR Error   |
|--|------------|-------------------------------------|
| LUNA_RET_CB_MUST_WRITE                   | 0x80000a26 | CKR_CALLBACK_ERROR                  |
| LUNA_RET_CB_INVALID_CALL_FOR_THE_STATE   | 0x80000a27 | CKR_CALLBACK_ERROR                  |
| LUNA_RET_CB_SYNC_ERROR                   | 0x80000a28 | CKR_CALLBACK_ERROR                  |
| LUNA_RET_CB_PROT_DATA_INVALID            | 0x80000a29 | CKR_CALLBACK_ERROR                  |
| LUNA_RET_LOG_FILE_NOT_OPEN               | 0x80000d00 | CKR_LOG_FILE_NOT_OPEN               |
| LUNA_RET_LOG_FILE_WRITE_ERROR            | 0x80000d01 | CKR_LOG_FILE_WRITE_ERROR            |
| LUNA_RET_LOG_BAD_FILE_NAME               | 0x80000d02 | CKR_LOG_BAD_FILE_NAME               |
| LUNA_RET_LOG_FULL                        | 0x80000d03 | CKR_LOG_FULL                        |
| LUNA_RET_LOG_NO_KCV                      | 0x80000d04 | CKR_LOG_NO_KCV                      |
| LUNA_RET_LOG_BAD_RECORD_HMAC             | 0x80000d05 | CKR_LOG_BAD_RECORD_HMAC             |
| LUNA_RET_LOG_BAD_TIME                    | 0x80000d06 | CKR_LOG_BAD_TIME                    |
| LUNA_RET_LOG_AUDIT_NOT_INITIALIZED       | 0x80000d07 | CKR_LOG_AUDIT_NOT_INITIALIZED       |
| LUNA_RET_LOG_RESYNC_NEEDED               | 0x80000d08 | CKR_LOG_RESYNC_NEEDED               |
| LUNA_RET_AUDIT_LOGIN_TIMEOUT_IN_PROGRESS | 0x80000d09 | CKR_AUDIT_LOGIN_TIMEOUT_IN_PROGRESS |
| LUNA_RET_AUDIT_LOGIN_FAILURE_THRESHOLD   | 0x80000d0a | CKR_AUDIT_LOGIN_FAILURE_THRESHOLD   |
| LUNA_RET_XTC_ERROR                       | 0x80001600 | CKR_XTC_ERROR                       |
| LUNA_RET_CONTEXT_INVALID                 | 0x80001601 | CKR_CONTEXT_INVALID                 |
| LUNA_RET_SESSION_COUNT                   | 0x80001603 | CKR_MAX_SESSION_COUNT               |
| LUNA_RET_BUSY                            | 0x80001604 | CKR_BUSY                            |

\* This error (CKR\_TEMPLATE\_INCONSISTENT) might be encountered when using CKDemo in a new client with firmware older than version 6.22.0. Try CKDemo option 98, sub-option 16. If it is set to "enhanced roles", try selecting it to set it to "legacy Luna roles". The setting is a toggle, and flips every time you select it.

\*\* This error, or "unable to read public key", might be encountered when using BSAFE to encrypt data with ECC public key using curves from the Brainpool suite. As indicated on the BSAFE website (May 2012) they do not appear to support Brainpool curves. Therefore, your own applications should not attempt that combination, and you should avoid attempting to specify Brainpool curves with BSAFE ECC when using the Luna CKDemo utility.

† These errors (0x00310000 through 0x00310007) are all considered as the same generic CKR\_DEVICE\_MEMORY error *by a host application*. They are visible using [Luna HSM Firmware 7.8.1](#) or newer. Your application is responsible for closing crypto sessions and releasing resources when they are no longer being used. Failure to do so allows accumulating orphan sessions to eventually consume all available HSM memory. The HSM has no way to know that any given session is no longer needed, unless your application explicitly closes the session. If a solution/application mixes Java and C/C++ operations, those might not agree on when sessions are to close.

**Workaround:** If you are seeing device memory errors in the logs, consider:

1. Stopping your application (so that it does not continue attempting cryptographic operations against the HSM)
2. Restarting the HSM to clear any orphan sessions or processes (use [hsm restart](#) to restart the HSM or [sysconf appliance reboot](#) to restart the whole appliance including the HSM)
3. Restarting your application.

**NOTE** This is a temporary measure to clear the effects of application behavior that should be corrected, or the problem can recur. Contact your application vendor to report the memory issue.

## Library Codes

| Hex value  | Decimal value | Return code/error description      |
|------------|---------------|------------------------------------|
| 0          | 0             | OKAY, NO ERROR                     |
| 0xC0000000 | 3221225472    | PROGRAMMING ERROR: RETURN CODE     |
| 0xC0000001 | 3221225473    | OUT OF MEMORY                      |
| 0xC0000002 | 3221225474    | NON-SPECIFIC ERROR                 |
| 0xC0000003 | 3221225475    | UNEXPECTED NULL POINTER            |
| 0xC0000004 | 3221225476    | PROGRAMMING ERROR: LOGIC           |
| 0xC0000005 | 3221225477    | OPERATION WOULD BLOCK IF ATTEMPTED |
| 0xC0000006 | 3221225478    | BUFFER IS TOO SMALL                |
| 0xC0000100 | 3221225728    | OPERATION CANCEL                   |

| Hex value  | Decimal value | Return code/error description              |
|------------|---------------|--|
| 0xC0000101 | 3221225729    | INVALID SLOT IDENTIFIER                    |
| 0xC0000102 | 3221225730    | INVALID DATA                               |
| 0xC0000103 | 3221225731    | INVALID PIN                                |
| 0xC0000104 | 3221225732    | NO TOKEN PRESENT                           |
| 0xC0000105 | 3221225733    | FUNCTION IS NOT SUPPORTED                  |
| 0xC0000106 | 3221225734    | NON-CRYPTOKI ELEMENT CLONE                 |
| 0xC0000107 | 3221225735    | INVALID BUFFER SIZE FOR CHALLENGE          |
| 0xC0000108 | 3221225736    | PIN IS LOCKED                              |
| 0xC0000109 | 3221225737    | INVALID VERSION                            |
| 0xC000010a | 3221225738    | NEEDED KEY NOT PROVIDED                    |
| 0xC000010b | 3221225739    | USER NAME IS IN USE                        |
| 0xC0000200 | 3221225984    | INVALID DISTINGUISHED ENCODING RULES CLASS |
| 0xC0000303 | 3221226243    | OPERATION TIMED OUT                        |
| 0xC0000304 | 3221226244    | RESET FAILED                               |
| 0xC0000400 | 3221226496    | INVALID TOKEN STATE                        |
| 0xC0000401 | 3221226497    | DATA APPEARS CORRUPTED                     |
| 0xC0000402 | 3221226498    | INVALID FILENAME                           |
| 0xC0000403 | 3221226499    | FILE IS READ-ONLY                          |
| 0xC0000404 | 3221226500    | FILE ERROR                                 |
| 0xC0000405 | 3221226501    | INVALID OBJECT IDENTIFIER                  |
| 0xC0000406 | 3221226502    | INVALID SOCKET ADDRESS                     |
| 0xC0000407 | 3221226503    | INVALID LISTEN SOCKET                      |

| Hex value  | Decimal value | Return code/error description |
|------------|---------------|-------------------------------|
| 0xC0000408 | 3221226504    | CACHE IS NOT CURRENT          |
| 0xC0000409 | 3221226505    | CACHE IS NOT MAPPED           |
| 0xC000040a | 3221226506    | OBJECT IS NOT IN LIST         |
| 0xC000040b | 3221226507    | INVALID INDEX                 |
| 0xC000040c | 3221226508    | OBJECT ALREADY EXISTS         |
| 0xC000040d | 3221226509    | SEMAPHORE ERROR               |
| 0xC000040e | 3221226510    | END OF LIST ENCOUNTERED       |
| 0xC000040f | 3221226511    | WOULD ASSIGN SAME VALUE       |
| 0xC0000410 | 3221226512    | INVALID GROUP NAME            |
| 0xC0000411 | 3221226513    | NOT HSM BACKUP TOKEN          |
| 0xC0000412 | 3221226514    | NOT PARTITION BACKUP TOKEN    |
| 0xC0000413 | 3221226515    | SIM NOT SUPPORTED             |
| 0xC0000500 | 3221226752    | SOCKET ERROR                  |
| 0xC0000501 | 3221226753    | SOCKET WRITE ERROR            |
| 0xC0000502 | 3221226754    | SOCKET READ ERROR             |
| 0xC0000503 | 3221226755    | CLIENT MESSAGE ERROR          |
| 0xC0000504 | 3221226756    | SERVER DISCONNECTED           |
| 0xC0000505 | 3221226757    | CLIENT DISCONNECTED           |
| 0xC0000506 | 3221226758    | SOCKET WOULD BLOCK            |
| 0xC0000507 | 3221226759    | SOCKET ADDRESS IS IN USE      |
| 0xC0000508 | 3221226760    | SOCKET BAD FILE DESCRIPTOR    |
| 0xC0000509 | 3221226761    | HOST RESOLUTION ERROR         |
| 0xC000050a | 3221226762    | INVALID HOST CERTIFICATE      |

| Hex value  | Decimal value | Return code/error description         |
|------------|---------------|---------------------------------------|
| 0xC0000600 | 3221227008    | NO BUFFER AVAILABLE                   |
| 0xC0000601 | 3221227009    | INVALID ENUMERATION OPTION            |
| 0xC0000700 | 3221227264    | SSL ERROR                             |
| 0xC0000701 | 3221227265    | SSL CTX ERROR                         |
| 0xC0000702 | 3221227266    | SSL CIPHER LIST ERROR                 |
| 0xC0000703 | 3221227267    | SSL CERT VERIFICATION LOCATION ERROR  |
| 0xC0000704 | 3221227268    | SSL LOAD SERVER CERT ERROR            |
| 0xC0000705 | 3221227269    | SSL LOAD SERVER PRIVATE KEY ERROR     |
| 0xC0000706 | 3221227270    | SSL VALIDATE SERVER PRIVATE KEY ERROR |
| 0xC0000707 | 3221227271    | SSL CREATE SSL ERROR                  |
| 0xC0000708 | 3221227272    | SSL LOAD CLIENT CERT ERROR            |
| 0xC0000709 | 3221227273    | SSL GET CERTIFICATE ERROR             |
| 0xC000070a | 3221227274    | SSL INVALID CERT STRUCTURE            |
| 0xC000070b | 3221227275    | SSL LOAD CLIENT PRIVATE KEY ERROR     |
| 0xC000070c | 3221227276    | SSL GET PEER CERT ERROR               |
| 0xC000070d | 3221227277    | SSL WANT READ ERROR                   |
| 0xC000070e | 3221227278    | SSL WANT WRITE ERROR                  |
| 0xC000070f | 3221227279    | SSL WANT X509 LOOKUP ERROR            |
| 0xC0000710 | 3221227280    | SSL SYSCALL ERROR                     |
| 0xC0000711 | 3221227281    | SSL FAILED HANDSHAKE                  |
| 0xC0000800 | 3221227520    | INVALID CERTIFICATE TYPE              |
| 0xC0000900 | 3221227776    | INVALID PORT                          |

| Hex value  | Decimal value | Return code/error description |
|------------|---------------|-------------------------------|
| 0xC0000901 | 3221227777    | SESSION SCRIPT EXISTS         |
| 0xC0001000 | 3221229568    | PARTITION LOCKED              |
| 0xC0001001 | 3221229569    | PARTITION NOT ACTIVATED       |
| 0xc0002000 | 3221233664    | FAILED TO CREATE THREAD       |
| 0xc0002001 | 3221233665    | CALLBACK ERROR                |
| 0xc0002002 | 3221233666    | UNKNOWN CALLBACK COMMAND      |
| 0xc0002003 | 3221233667    | SHUTTING DOWN                 |
| 0xc0002004 | 3221233668    | REMOTE SIDE DISCONNECTED      |
| 0xc0002005 | 3221233669    | SOCKET CLOSED                 |
| 0xC0002006 | 3221233670    | INVALID COMMAND               |
| 0xC0002007 | 3221233671    | UNKNOWN COMMAND               |
| 0xC0002008 | 3221233672    | UNKNOWN COMMAND VERSION       |
| 0xC0002009 | 3221233673    | FILE LOCK FAILED              |
| 0xC0002010 | 3221233680    | FILE LOCK ERROR               |
| 0xc0002011 | 3221233681    | FAILED TO CREATE PROCESS      |
| 0xc0002012 | 3221233682    | USB PED NOT FOUND             |
| 0xc0002013 | 3221233683    | USB PED NOT RESPONDING        |
| 0xc0002014 | 3221233684    | USB PED OPERATION CANCELLED   |
| 0xc0002015 | 3221233685    | USB PED TOO MANY CONNECTED    |
| 0xc0002016 | 3221233686    | USB PED OUT OF SYNC           |
| 0xC0001100 | 3221229824    | UNABLE TO CONNECT             |

## Vendor-Defined Return Codes

| Code       | Name                                 |
|------------|--------------------------------------|
| 0x80000004 | CKR_RC_ERROR                         |
| 0x80000005 | CKR_CONTAINER_HANDLE_INVALID         |
| 0x80000006 | CKR_TOO_MANY_CONTAINERS              |
| 0x80000007 | CKR_USER_LOCKED_OUT                  |
| 0x80000008 | CKR_CLONING_PARAMETER_ALREADY_EXISTS |
| 0x80000009 | CKR_CLONING_PARAMETER_MISSING        |
| 0x8000000a | CKR_CERTIFICATE_DATA_MISSING         |
| 0x8000000b | CKR_CERTIFICATE_DATA_INVALID         |
| 0x8000000c | CKR_ACCEL_DEVICE_ERROR               |
| 0x8000000d | CKR_WRAPPING_ERROR                   |
| 0x8000000e | CKR_UNWRAPPING_ERROR                 |
| 0x8000000f | CKR_MAC_MISSING                      |
| 0x80000010 | CKR_DAC_POLICY_PID_MISMATCH          |
| 0x80000011 | CKR_DAC_MISSING                      |
| 0x80000012 | CKR_BAD_DAC                          |
| 0x80000013 | CKR_SSK_MISSING                      |
| 0x80000014 | CKR_BAD_MAC                          |
| 0x80000015 | CKR_DAK_MISSING                      |
| 0x80000016 | CKR_BAD_DAK                          |
| 0x80000017 | CKR_SIM_AUTHORIZATION_FAILED         |
| 0x80000018 | CKR_SIM_VERSION_UNSUPPORTED          |

| Code       | Name                              |
|------------|-----------------------------------|
| 0x80000019 | CKR_SIM_CORRUPT_DATA              |
| 0x8000001a | CKR_USER_NOT_AUTHORIZED           |
| 0x8000001b | CKR_MAX_OBJECT_COUNT_EXCEEDED     |
| 0x8000001c | CKR_SO_LOGIN_FAILURE_THRESHOLD    |
| 0x8000001d | CKR_SIM_AUTHFORM_INVALID          |
| 0x8000001e | CKR_CITS_DAK_MISSING              |
| 0x8000001f | CKR_UNABLE_TO_CONNECT             |
| 0x80000020 | CKR_PARTITION_DISABLED            |
| 0x80000021 | CKR_CALLBACK_ERROR                |
| 0x80000022 | CKR_SECURITY_PARAMETER_MISSING    |
| 0x80000023 | CKR_SP_TIMEOUT                    |
| 0x80000024 | CKR_TIMEOUT                       |
| 0x80000025 | CKR_ECC_UNKNOWN_CURVE             |
| 0x80000026 | CKR_MTK_ZEROIZED                  |
| 0x80000027 | CKR_MTK_STATE_INVALID             |
| 0x80000028 | CKR_INVALID_ENTRY_TYPE            |
| 0x80000029 | CKR_MTK_SPLIT_INVALID             |
| 0x8000002a | CKR_HSM_STORAGE_FULL              |
| 0x8000002b | CKR_DEVICE_TIMEOUT                |
| 0x8000002c | CKR_CONTAINER_OBJECT_STORAGE_FULL |
| 0x8000002d | CKR_PED_CLIENT_NOT_RUNNING        |
| 0x8000002e | CKR_PED_UNPLUGGED                 |
| 0x8000002f | CKR_ECC_POINT_INVALID             |



| Code       | Name                                   |
|------------|--|
| 0x80000030 | CKR_OPERATION_NOT_ALLOWED              |
| 0x80000031 | CKR_LICENSE_CAPACITY_EXCEEDED          |
| 0x80000032 | CKR_LOG_FILE_NOT_OPEN                  |
| 0x80000033 | CKR_LOG_FILE_WRITE_ERROR               |
| 0x80000034 | CKR_LOG_BAD_FILE_NAME                  |
| 0x80000035 | CKR_LOG_FULL                           |
| 0x80000036 | CKR_LOG_NO_KCV                         |
| 0x80000037 | CKR_LOG_BAD_RECORD_HMAC                |
| 0x80000038 | CKR_LOG_BAD_TIME                       |
| 0x80000039 | CKR_LOG_AUDIT_NOT_INITIALIZED          |
| 0x8000003A | CKR_LOG_RESYNC_NEEDED                  |
| 0x8000003B | CKR_AUDIT_LOGIN_TIMEOUT_IN_PROGRESS    |
| 0x8000003C | CKR_AUDIT_LOGIN_FAILURE_THRESHOLD      |
| 0x8000003D | CKR_INVALID_FUF_TARGET                 |
| 0x8000003E | CKR_INVALID_FUF_HEADER                 |
| 0x8000003F | CKR_INVALID_FUF_VERSION                |
| 0x80000040 | CKR_ECC_ECC_RESULT_AT_INF              |
| 0x80000041 | CKR_AGAIN                              |
| 0x80000042 | CKR_TOKEN_COPIED                       |
| 0x80000043 | CKR_SLOT_NOT_EMPTY                     |
| 0x80000044 | CKR_USER_ALREADY_ACTIVATED             |
| 0x80000045 | CKR_STC_NO_CONTEXT                     |
| 0x80000046 | CKR_STC_CLIENT_IDENTITY_NOT_CONFIGURED |

| Code       | Name                                      |
|------------|---|
| 0x80000047 | CKR_STC_PARTITION_IDENTITY_NOT_CONFIGURED |
| 0x80000048 | CKR_STC_DH_KEYGEN_ERROR                   |
| 0x80000049 | CKR_STC_CIPHER_SUITE_REJECTED             |
| 0x8000004a | CKR_STC_DH_KEY_NOT_FROM_SAME_GROUP        |
| 0x8000004b | CKR_STC_COMPUTE_DH_KEY_ERROR              |
| 0x8000004c | CKR_STC_FIRST_PHASE_KDF_ERROR             |
| 0x8000004d | CKR_STC_SECOND_PHASE_KDF_ERROR            |
| 0x8000004e | CKR_STC_KEY_CONFIRMATION_FAILED           |
| 0x8000004f | CKR_STC_NO_SESSION_KEY                    |
| 0x80000050 | CKR_STC_RESPONSE_BAD_MAC                  |
| 0x80000051 | CKR_STC_NOT_ENABLED                       |
| 0x80000052 | CKR_STC_CLIENT_HANDLE_INVALID             |
| 0x80000053 | CKR_STC_SESSION_INVALID                   |
| 0x80000054 | CKR_STC_CONTAINER_INVALID                 |
| 0x80000055 | CKR_STC_SEQUENCE_NUM_INVALID              |
| 0x80000056 | CKR_STC_NO_CHANNEL                        |
| 0x80000057 | CKR_STC_RESPONSE_DECRYPT_ERROR            |
| 0x80000058 | CKR_STC_RESPONSE_REPLAYED                 |
| 0x80000059 | CKR_STC_REKEY_CHANNEL_MISMATCH            |
| 0x8000005a | CKR_STC_RSA_ENCRYPT_ERROR                 |
| 0x8000005b | CKR_STC_RSA_SIGN_ERROR                    |
| 0x8000005c | CKR_STC_RSA_DECRYPT_ERROR                 |
| 0x8000005d | CKR_STC_RESPONSE_UNEXPECTED_KEY           |

| Code       | Name  |
|------------|---|
| 0x8000005e | CKR_STC_UNEXPECTED_NONCE_PAYLOAD_SIZE         |
| 0x8000005f | CKR_STC_UNEXPECTED_DH_DATA_SIZE               |
| 0x80000060 | CKR_STC_OPEN_CIPHER_MISMATCH                  |
| 0x80000061 | CKR_STC_OPEN_DHNIST_PUBKEY_ERROR              |
| 0x80000062 | CKR_STC_OPEN_KEY_MATERIAL_GEN_FAIL            |
| 0x80000063 | CKR_STC_OPEN_RESP_GEN_FAIL                    |
| 0x80000064 | CKR_STC_ACTIVATE_MACTAG_U_VERIFY_FAIL         |
| 0x80000065 | CKR_STC_ACTIVATE_MACTAG_V_GEN_FAIL            |
| 0x80000066 | CKR_STC_ACTIVATE_RESP_GEN_FAIL                |
| 0x80000067 | CKR_CHALLENGE_INCORRECT                       |
| 0x80000068 | CKR_ACCESS_ID_INVALID                         |
| 0x80000069 | CKR_ACCESS_ID_ALREADY_EXISTS                  |
| 0x8000006a | CKR_KEY_NOT_KEKABLE                           |
| 0x8000006b | CKR_MECHANISM_INVALID_FOR_FP                  |
| 0x8000006c | CKR_OPERATION_INVALID_FOR_FP                  |
| 0x8000006d | CKR_SESSION_HANDLE_INVALID_FOR_FP             |
| 0x8000006e | CKR_CMD_NOT_ALLOWED_HSM_IN_TRANSPORT          |
| 0x8000006f | CKR_OBJECT_ALREADY_EXISTS                     |
| 0x80000070 | CKR_PARTITION_ROLE_DESC_VERSION_INVALID       |
| 0x80000071 | CKR_PARTITION_ROLE_POLICY_VERSION_INVALID     |
| 0x80000072 | CKR_PARTITION_ROLE_POLICY_SET_VERSION_INVALID |
| 0x80000073 | CKR_REKEK_KEY                                 |
| 0x80000074 | CKR_KEK_RETRY_FAILURE                         |

| Code       | Name                                  |
|------------|---------------------------------------|
| 0x80000075 | CKR_RNG_RESEED_TOO_EARLY              |
| 0x80000076 | CKR_HSM_TAMPERED                      |
| 0x80000077 | CKR_CONFIG_CHANGE_ILLEGAL             |
| 0x80000078 | CKR_SESSION_CONTEXT_NOT_ALLOCATED     |
| 0x80000079 | CKR_SESSION_CONTEXT_ALREADY_ALLOCATED |
| 0x8000007a | CKR_INVALID_BL_ITB_AUTH_HEADER        |
| 0x80000114 | CKR_OBJECT_READ_ONLY                  |
| 0x80000136 | CKR_KEY_NOT_ACTIVE                    |
| 0x80000400 | CKR_ACCESS_ID_INVALID                 |
| 0x80001600 | CKR_XTC_ERROR                         |
| 0x80001601 | CKR_CONTEXT_INVALID                   |
| 0x80001603 | CKR_MAX_SESSION_COUNT                 |
| 0x80001604 | CKR_BUSY                              |
| 0x80001606 | CKR_SERVICE_UNAVAILABLE               |

## HSM Alarm Codes

The Luna PCIe HSM 7 alarm messages indicate error conditions on the HSM card that might require user intervention. The alarms apply to a Luna HSM, compliant with security level FIPS 140-2 Level 3. The alarm messages provide appropriate detail to alert HSM users of important events. Each alarm message has a unique character string for the message ID that allows higher level tools on the host system to parse for the alarm message IDs and generate notifications.

Messages are saved to the system log file in Linux host systems, allowing host application software like SNMP to parse the log file, and to the Windows Event Viewer in Windows host systems

Messages can be retrieved with the "dmesg" utility, to read messages from the driver log, which collects messages from the bootloader (BL), the firmware (FW), or from the Host Driver itself.

This section contains the following information:

- > ["Alarm Generation and Handling" on the next page](#)
- > ["List of HSM Alarm Codes" on page 222](#)
- > ["HSM Alarm Code Samples" on page 227](#)

- > ["Stored Data Integrity" on page 231](#)

## Alarm Generation and Handling

Alarm messages can be generated due to the HSM BL, FW, and Host Driver SW detecting unexpected conditions. Other alarm messages are generated after unexpected interrupts or tamper events. For each of these problems detailed error information and an alarm message is output to notify the user that something special has happened.

At least one alarm message is output as a result of each tamper event by BL, FW, or Host Driver. Depending on the type of tamper all of them may report an alarm message related to the same tamper event. The message timestamps assist you to identify which alarm messages are for the same tamper event. Tamper alarm messages from BL, FW, and Host Driver have the same text description for the same tamper event. A specific type of tamper event is not reported again until FW clears the tamper information in the tamper circuit. If the tamper event happens after that, then either a new tamper condition has been detected or the same tamper event is still active and cannot be cleared.

### Alarm Handling for Special Situations

Alarm messages are still generated during rare occurrences where BL, FW, or Host Driver might be in an abnormal state.

As long as the Host Driver is running, the BL and FW are able to output their alarm messages to the DLOG (driver log), which can be parsed to notify the user. If either BL or FW stops execution due to error detection, they output an alarm message to the Host Driver, which stores it in DLOG. All BL and FW checking for alarm conditions is stopped but all HW tamper event monitoring (soft and hard tampers) is still enabled including Host Driver monitoring. The card reset caused by these tampers restarts BL and possibly FW and the alarm messages are output. The following situations are also handled:

- > **BL starts before Host Driver is loaded (System power-up):** Without Host Driver available, BL outputs all alarms only to an internal HSM log. When the Host Driver loads it resets the HSM card, causing BL to start again. BL can then send any new alarms to the host driver and either stop or proceed to FW, as the situation allows.
  - For an L3 card if FW is started it will output alarm messages for any existing tamper conditions. Any tamper event alarm messages including those not sent out while the Host Driver was not loaded can be fetched from the FRAM Log.

**NOTE** If needed, use `lunash:> hsm supportinfo` to output the FRAM Log in order to determine the tamper information, or to pass on to Thales Technical Support.

- > **FW halted due to internal error:** In order to get to FW the Host Driver must be running so the FW halted alarm message will be stored in DLOG. No further BL or FW alarm messages are generated in this state until the next card reset.
- > **FW in locked state (tamper clear required):** An alarm message is generated to signal locked state is active. FW is still doing periodic checks and FW alarm messages are still possible. Only a small subset of FW commands is available.
- > **FW in Secure Transport Mode (STM):** An alarm message is generated to signal STM is active. FW is still doing periodic checks and FW alarm messages are still possible. Only a small subset of FW commands are available.

- > **Host Driver loses communications with the HSM card:** If the Host Driver has any errors communicating with the K7 (BL or FW) it will generate alarm messages. The Host Driver also periodically checks that the Luna PCIe HSM 7 card is still present on the PCIe bus (i.e. chassis open causes a cold reset of the HSM) and if there is no response for a pre-determined period of time an alarm message is generated.

## FRAM LOG

The Boot Loader and firmware also store all alarm event information in the FRAM Log in the non-volatile FRAM device on the K7. There is no specific FRAM Log partition for DLOG or alarm messages. Use LUNADIAG to retrieve the FRAM Log contents and return it to Thales Customer Support for further analysis. In the event the Host Driver is unavailable to receive this information, it is still present in the FRAM Log and can be retrieved long after the alarm event has finished.

## List of HSM Alarm Codes

| ALM ID             | Alarm Message                     | Description  | Info               |
|--------------------|-----------------------------------|--|--------------------|
| <b>Host Driver</b> |                                   |  | <b>Tamper Flag</b> |
| 0001               | Soft tamper - over voltage        | HSM voltage is above the operating range. HSM will stay in reset until voltage goes back in range.                                   | HCCSR: VST         |
| 0002               | Soft tamper - temperature (nnC)   | HSM temperature (nn degrees Celsius) is outside the range (-2C to 80C). HSM will stay in reset until temperature goes back in range. | HRCSR: TST         |
| 0003               | Soft tamper - indeterminate cause | A soft tamper occurred but cannot determine the cause.   |                    |
| 0004               | Hard tamper - high temperature    | HSM temperature is higher than 88C.  | HT_T               |
| 0005               | Hard tamper - low temperature     | HSM temperature is lower than -40C   | LT_T               |
| 0006               | Hard tamper - over voltage        | HSM voltage is higher than the maximum allowed.  | OV_T, TC3_T        |
| 0009               | Hard tamper - oscillator failure  | HSM tamper clock oscillator has failed   | OSC_T              |
| 0010               | Decommission signal triggered     | Decommission button (connector P9) has been pressed.   | TC2_T              |

| ALM ID | Alarm Message                     | Description  | Info |
|--------|-----------------------------------|--|------|
| 0011   | Hard tamper - indeterminate cause | A hard tamper occurred but cannot determine the cause.                       |      |
| 0012   | Hardware Error                    | Error detected in device hardware  |      |
| 0013   | High Temperature - nnC            | HSM has reached nn degrees Celsius and needs to be cooled to avoid tampering |      |
| 0014   | Low Battery                       | HSM battery voltage is below 2.75V and needs to be replaced soon.            |      |
| 0015   | PCIe Link Failure                 | HSM no longer appears on PCIe bus. Chassis may have been opened.             |      |
| 0016   | Device Error                      | Internal error detected during communications with HSM                       |      |
| 0017   | Request Timed Out                 | Request to HSM took too long   |      |

| Boot Loader |   |  | Tamper Flag |
|-------------|---|--|-------------|
| 1000        | Unknown alarm ID xx in boot loader      | Illegal alarm ID used in Boot Loader.  |             |
| 1001        | HSM restart required                    | Soft or hard tamper occurred. HSM needs to be restarted (reset) before firmware is allowed to run.   |             |
| 1003        | HSM halted - internal boot loader error | Boot Loader detected an error during diagnostics and did not jump to FW.   |             |
| 1004        | Warning - boot loader diagnostic error  | Boot Loader detected an error during diagnostics that does not stop execution but needs to be investigated (i.e. fan, VPD, or RTC problems). |             |

| ALM ID | Alarm Message                              | Description   | Info              |
|--------|--|---|-------------------|
| 1005   | HSM FW signature check failed              | The FW image on the HSM failed authentication and will not be executed.                                 |                   |
| 1006   | Soft tamper temperature/voltage            | HSM voltage or temperature is outside the acceptable range. HSM will stay in reset until back in range. | PORSM status reg. |
| 1007   | Hard tamper - high temperature             | HSM voltage or temperature is outside the acceptable range. HSM will stay in reset until back in range. | HT_T              |
| 1008   | Hard tamper - low temperature              | HSM temperature is lower than -40C.   | LT_T              |
| 1009   | Hard tamper - over voltage                 | HSM voltage is higher than the maximum allowed.   | OV_T, TC3_T       |
| 1012   | Hard tamper - oscillator failure           | HSM tamper clock oscillator has failed  | OSC_T             |
| 1013   | Hard tamper - tamper configuration invalid | HSM tamper configuration lost (set to defaults) due to power loss.                                      | FS_T              |
| 1014   | Chassis opened                             | Chassis open switch (connector P7) has been triggered.  | TC1_T             |
| 1015   | HSM removed from chassis                   | HSM was removed from host chassis then re-inserted  | CS                |
| 1016   | Decommission signal triggered              | Decommission button (connector P9) has been pressed.  | TC2_T             |

| Firmware |                                    |  |  |
|----------|------------------------------------|--|--|
| 2000     | Unknown alarm ID xx in firmware    | Illegal alarm ID used in firmware.   |  |
| 2001     | High temperature warning activated | HSM temperature is above 75C (FW checks every 2 minutes). This warning will not re-appear unless temperature drops below 75C and goes back up again. |  |



| ALM ID | Alarm Message                        | Description   | Info |
|--------|--------------------------------------|---|------|
| 2002   | High temperature warning deactivated | HSM temperature has dropped below 75C.  |      |
| 2003   | Battery low voltage warning          | Battery voltage is below 2.75V (FW checks every hour). This warning will not re-appear unless voltage goes above 2.75V then back down. Battery should to be replaced soon.  |      |
| 2004   | Battery depleted                     | Battery voltage is below 2.5V (FW checks every hour). HSM FW will be halted. Battery must to be replaced.   |      |
| 2005   | HSM deactivated                      | Auto-activation data has been cleared   |      |
| 2006   | HSM decommissioned by FW             | All user crypto material has been invalidated due to KEK CRC failure, decommission signal, or tamper (if decommission on tamper enabled).   |      |
| 2007   | HSM zeroized                         | All user crypto material has been erased. HSM product credentials still exist. This can occur for a variety of reasons including manual zeroization.  |      |
| 2008   | Internal data corruption             | Settings to control tamper monitoring are incorrect or Critical Security Parameter data (MTK) is invalid ( the tamper monitoring settings if incorrect are corrected. ). Otherwise there was an unexpected tamper security write protection change. |      |
| 2009   | HSM halted - internal firmware error | FW detected an error which caused it to halt itself. Can also be errors generated by the kernel such as: bad exception, out of memory, unrecoverable errors.  |      |

| ALM ID | Alarm Message                                  | Description   | Info        |
|--------|--|---|-------------|
| 2010   | HSM locked - tamper clear required             | Limited set of FW commands available due to an HSM tamper condition. Tamper needs to be cleared before proceeding. Controlled tamper recovery must be enabled for this message to appear. |             |
| 2011   | HSM unlocked - tamper clear done               | Tamper was cleared when in controlled tamper recovery mode.   |             |
| 2012   | HSM in secure transport mode                   | Checked on every FW start-up to remind the user to do a recovery operation. Limited set of FW commands available.   |             |
| 2013   | HSM recovered from secure transport mode       | HSM in secure transport mode was recovered back to normal mode.   |             |
| 2014   | Auto-activation data invalid – HSM deactivated | FW checked auto-activation data validity and failed. Re-activation required.  |             |
| 2015   | Hard tamper - high temperature                 | (L3 only) HSM temperature was higher than 88C.  | HT_T        |
| 2016   | Hard tamper - low temperature                  | (L3 only) HSM temperature was lower than -40C.  | LT_T        |
| 2017   | Hard tamper - over voltage                     | (L3 only) HSM voltage was higher than the maximum allowed.  | OV_T, TC3_T |
| 2018   | Hard tamper - oscillator failure               | (L3 only) HSM tamper clock oscillator has failed  | OSC_T       |
| 2019   | Hard tamper - tamper configuration invalid     | (L3 only) HSM tamper configuration lost (set to defaults) due to power loss.  | FS_T        |
| 2020   | Chassis opened                                 | Chassis open switch (connector P7) has been triggered.  | TC1_T       |
| 2021   | HSM was removed from chassis                   | HSM was removed from host chassis just before this FW execution. HSM will be deactivated.   | CS          |

| ALM ID | Alarm Message                      | Description   | Info  |
|--------|------------------------------------|---|-------|
| 2022   | Decommission signal triggered      | Decommission button (connector P9) has been pressed.  | TC2_T |
| 2023   | HSM fan x failure                  | Fault detected in HSM on-board fan (fan 1 or fan 2).  |       |
| 2024   | Stored data integrity verify error | Integrity of an object or CSP did not verify correctly. See <a href="#">"Stored Data Integrity" on page 231</a> .   |       |
| 2025   | Firmware update in progress        | A firmware update procedure is in progress. Recorded in the logs, but not shown onscreen. [ Added with firmware 7.7.0 ]   |       |
| 2026   | Firmware update canceled           | A firmware update procedure was halted due to insufficient memory to continue - the HSM rolls back to the previous f/w. [ Added with firmware 7.7.0 ]   |       |
| 2027   | HSM storage exceeded               | Attempt to use storage beyond the size of a partition (which was doubled with firmware 7.7.0) - the update proceeds to completion, but some restrictions apply to the affected partition -- see <a href="#">"Memory and partition and object interactions during and after firmware update " on page 1</a> . This is recorded only in the logs, not onscreen, but a message "HSM storage is currently over capacity" is shown onscreen. [ Added with firmware 7.7.0 ] |       |
| 2028   | HSM capacity exceeded              | Attempt to exceed the total memory size of the HSM cancels the operation. Refer to your backups. [ Added with firmware 7.7.0 ]  |       |

## HSM Alarm Code Samples

This section shows the details of some of the alarm event scenarios.

ALM = alarm message.

## Temperature - High Warning

If HSM temperature reaches 75 degrees Celsius and then drops back below 75C the following actions occur:

- > Temperature  $\geq 75C$ 
  - After 5 minutes at this temperature or higher, the Host Driver receives a 'High Temperature Warning' interrupt and issues an ALM
  - Firmware checks temperature at start-up and once per hour
  - Firmware issues ALM for high temperature warning activated
- > Temperature  $< 75C$ 
  - Firmware issues ALM for high temperature warning deactivated

## Temperature – High Soft Tamper

When the temperature starts below 75C and reaches the high soft tamper limit of 80C and then drops back below 75C the following actions occur:

- > Temperature  $\geq 75C$ 
  - After 5 minutes at this temperature or higher, the Host Driver receives a High Temperature Warning interrupt and issues an ALM
  - Firmware issues ALM for activation of high temperature warning
- > Temperature  $\geq 80C$ 
  - Soft Tamper reset – card put into reset. Stays in reset until temperature lowers.
  - Host Driver receives soft tamper interrupt and issues ALM (only one when soft tamper condition starts).
- > Temperature  $< 80C$ 
  - Bootloader issues soft tamper ALM, then an ALM that HSM restart is required and waits for host reset.
  - User receives ALM and goes to LunaCM/Lunash to do an “hsm restart” command.
  - Bootloader starts – jumps to firmware.
  - Firmware starts – no actions taken for the soft tamper. If temperature  $\geq 75C$ , firmware re-issues ALM for activation of high temperature warning.
- > Temperature  $< 75C$ 
  - Firmware issues ALM for deactivation of high temperature warning.

## Temperature – High Hard Tamper

When the temperature starts below 75C and reaches high hard tamper limit of 88C and then drops back below 75C the following actions occur:

- > Same as soft tamper described above up to when card is held in soft tamper reset
- > Temperature  $> 88C$ 
  - Hard Tamper reset – Card in hard tamper reset for 5 seconds then returns to soft tamper reset. K7 HW does erase/reset of all internal temporary memory. Tamper chip latches time and type of tamper. Host driver receives hard tamper interrupt and issues ALM.

- HSM also erases auto-activation and STM data in tamper chip
  - If decommission on tamper is enabled then key encryption data is erased in tamper chip as well
- > Temperature < 80C
- Bootloader starts – issues hard tamper ALM and logs it in FRAM Log
  - Bootloader issues ALM that HSM restart is required and waits for host reset.
  - User receives ALM and goes to LunaCM/Lunash to perform an **hsm restart** command.
  - Bootloader starts – jumps to firmware.
  - Firmware starts – saves hard tamper latches. If controlled tamper recovery is enabled, firmware locks HSM commands to a minimal subset only, and issues ALM for HSM locked. User must go to LunaCM/Lunash and perform a “tamper clear” command to get a full HSM command set. When tamper clear is issued, firmware outputs an ALM for HSM unlocked.
  - Firmware – issues deactivation and decommission (if enabled for tamper) ALMs
  - Firmware - temperature  $\geq 75C$ , firmware re-issues ALM for activation of high temperature warning
- > Temperature < 75C
- Firmware issues ALM for deactivation of high temperature warning
- > Temperature < 80C
- Bootloader starts – issues hard tamper ALM
  - Bootloader erases all of flash except for Boot Loader area and issues ALM for 'HSM permanently tampered'
  - Bootloader issues ALM that 'HSM restart is required' and waits for host reset.
  - User receives ALM and goes to LunaCM/Lunash to do an “hsm restart” command.
  - Bootloader starts – Only bootloader commands are available. Bootloader again issues 'ALM for HSM permanently tampered'. User can dump the FRAM Log using LUNADIAG.

## Hard Tampers During Storage

When the HSM is powered off its tamper detection is powered by the on-card battery. Some hard tampers can occur when main power is not applied. The condition that caused the tamper might not be present (for example high or low temperature) when the HSM is powered back on, while others might never turn off (for example enclosure penetration, oscillator failure). If they occur while in storage, then after the HSM is powered up, the bootloader runs and logs the tamper events in FRAM Log and the serial port. Since the host K7 driver has not started yet, none of the messages from the bootloader are sent to the host, but other alarm messages are output later to notify the user.

- Bootloader waits for the host driver to be loaded
- When the host driver starts up it immediately resets the HSM causing the bootloader to run again
- Bootloader does not re-log the same tamper events
- Bootloader jumps to firmware which outputs the ALM for the tamper event. If controlled tamper recovery is enabled firmware also outputs an ALM for the 'HSM is locked and a tamper clear is required'. The user can then use LunaCM or Lunash to clear the tamper

**NOTE** If needed, use lunash:> [hsm supportinfo](#) to output the FRAM Log in order to determine the tamper information, or to pass on to Thales Technical Support.

## Decommission with power on

If the HSM is powered on and a decommission is triggered either by the decommission switch or by a tamper (if decommission on tamper is enabled) then the HSM goes into reset for 5 seconds. The following alarm messages are output to FRAM Log, serial port, and host driver:

- > The host driver immediately receives an interrupt and outputs an 'ALM for decommission triggered'
- > After 5 seconds lapses, the bootloader starts running and also outputs an 'ALM for decommission triggered'
- > Bootloader outputs an ALM for 'HSM restart required' and then waits
- > User gets alarm notification and performs an HSM restart
- > Bootloader restarts and jumps to firmware which finishes the decommission operations and firmware outputs an ALM for 'HSM decommissioned by firmware' and an ALM for 'HSM locked' (if enabled)

## Decommission with power off

If the HSM is powered off and a decommission is triggered either by the decommission switch or by a tamper (if decommission on tamper is enabled) then the decommission is latched in the tamper chip. When the HSM is powered on the following alarm messages are output:

- > Bootloader starts running and outputs an ALM for 'Decommission triggered' only to FRAM Log and serial port since the host driver is not loaded yet
- > Bootloader waits for the driver to be loaded which then forces a host reset
- > Bootloader restarts and jumps to firmware which finishes the decommission operations and firmware outputs an ALM for 'HSM decommissioned by firmware' and an ALM for 'HSM locked' (if enabled)

**NOTE** If needed, use lunash:> [hsm supportinfo](#) to output the FRAM Log in order to determine the tamper information, or to pass on to Thales Technical Support.

## Chassis open with power on

If the HSM is powered on and the chassis open switch triggered then a cold reset is performed on the HSM which effectively removes the HSM from the PCIe bus. After about 10 seconds the HSM is released from reset and the following alarm messages are output:

- > Host Driver notices the device is no longer present on the PCIe bus and outputs an ALM for 'HSM missing from PCIe bus'
- > Bootloader starts running and outputs an ALM for 'HSM chassis opened' only to FRAM Log and serial port
- > Bootloader waits for the driver to be loaded
- > User gets notification of missing HSM and powers off then on the host system
- > Bootloader starts running and does not re-log the same tamper events
- > Bootloader waits for the host driver to be loaded
- > When the host driver starts up it immediately resets the HSM causing Bootloader to run again

- > Bootloader jumps to firmware which finishes the chassis opened operations and firmware outputs an ALM for 'HSM chassis opened' and an ALM for 'HSM locked' (if enabled).

**NOTE** If the chassis is still open then the HSM performs a cold reset after the tampers are cleared by firmware.

If needed, use `lunash:> hsm supportinfo` to output the FRAM Log in order to determine the tamper information, or to pass on to Thales Technical Support.

## Chassis open with power off

If the HSM is powered off and the chassis open switch triggered then the chassis open is latched in the tamper chip. When the HSM is powered on the following alarm messages are output:

- > Bootloader starts running and outputs an ALM for 'HSM chassis opened' only to FRAM Log and serial port
- > Bootloader waits for the driver to be loaded which then forces a host reset
- > Bootloader starts running and does not re-log the same tamper events
- > Bootloader jumps to firmware which finishes the chassis opened operations and firmware outputs an ALM for 'HSM chassis opened' and an ALM for 'HSM locked' (if enabled)

**NOTE** If the chassis is still open then the HSM performs a cold reset after the tampers are cleared by firmware.

## Card removal

When an HSM is powered off and removed from the chassis a card removal latch is saved in the tamper chip. When the HSM is powered on the following alarm messages are output:

- > Bootloader starts running and outputs an ALM for 'card removal' only to FRAM Log and serial port
- > Bootloader waits for the driver to be loaded which then forces a host reset
- > Bootloader starts running and does not re-log the same tamper events
- > Bootloader restarts and jumps to firmware which outputs an ALM for 'HSM was removed from the chassis' and an ALM for 'HSM locked' (if enabled)

**NOTE** If needed, use `lunash:> hsm supportinfo` to output the FRAM Log in order to determine the tamper information, or to pass on to Thales Technical Support.

## Stored Data Integrity

The HSM performs data integrity checks at startup and during runtime.

### Startup

If a check fails during startup, meaning that an object stored in flash memory was corrupted, then ALM 2024 is generated, along with additional log messages, and the HSM firmware halts:

```
k7pf0: [HSM] ALM2024: Stored data integrity verify error
... additional messages that might include "LOG (SEVERE)" and "LOG (CRITICAL)", "Fatal
error", and possibly also
```

```
k7pf0: [HSM] ALM2009: HSM halted - internal firmware error
```

### What to do

1. Restart the HSM.
2. If the ALM persists, cycle the power to the HSM.
3. If the ALM persists, zeroize the HSM.
4. If the ALM persists, contact Support.

### Runtime

If a check fails during runtime, meaning that an object stored in volatile memory was corrupted, then ALM 2024 is generated, along with log messages, and the HSM is unable to perform any actions that involve the corrupted object:

```
k7pf0: [HSM] ALM2024: Stored data integrity verify error  
... additional messages that might include "LOG (SEVERE)"
```

### What to do

1. Try restarting the HSM.
2. If an SDI alarm occurs during startup, see the section about "Startup", above.
3. If no SDI alarm occurs during startup, but an SDI alarm occurs later, contact Support.

## Appliance reports out-of-service (OOS) code 30

Anything that halts the firmware (such as ALM\_2004, ALM\_2009, ALM\_2026) results in an out-of-service code 30. Other critical events that halt the firmware include:

- > failed self-test
- > failure in the random number generator
- > failure in integrity of the bootloader
- > failure in integrity of the firmware
- > failure in integrity of the HSM memory



# CHAPTER 10: HSM Updates and Upgrades

Thales releases periodic updates to the Luna Network HSM 7 appliance software and the HSM firmware, as well as updated versions of the Luna HSM Client software. If you have recently purchased a new Luna Network HSM 7 and your organization requires FIPS certification, you can download and install a FIPS-validated version of the HSM firmware. You can download these updates as they become available from the Thales Customer Support Portal: <https://supportportal.thalesgroup.com>.

Depending on the model of Luna Network HSM 7 you selected at time of purchase, you may also be able to purchase upgrades to the HSM's capabilities, or increase the number of partitions you can create. These upgrades are provided through the Thales Licensing Portal (GLP).

The [Customer Release Notes](#) (CRN) contain important information on updates.

The following chapter provides tested update paths and procedures for installing update packages, as well as a list of the version dependencies for certain features. It contains the following sections:

- > [Updating the Luna Network HSM 7 Appliance Software](#)
- > ["Updating the Luna HSM Firmware" below](#)
- > [Updating the Luna HSM Client](#)
- > [Updating the Luna Backup HSM 7 Firmware](#)
- > [Updating the Luna Backup HSM G5 Firmware](#)
- > ["Rolling Back the Luna HSM Firmware" on page 235](#)
- > ["Upgrading HSM Capabilities and Partition Licenses" on page 236](#)

## Updating the Luna HSM Firmware

A new Luna Network HSM 7 is delivered with the current FIPS- validated firmware installed on the HSM card, and the most recently released firmware version saved on the Luna Network HSM 7 hard drive as an optional update. When you install an appliance software update, this optional update is replaced with the latest firmware version. If you wish to use a different HSM firmware version, you can download it from the Thales Support Portal.

**CAUTION!** Use an uninterruptible power supply (UPS) to power your HSM. There is a small chance that a power failure during an update could leave your HSM in an unrecoverable condition.

**NOTE** If you are updating to [Luna HSM Firmware 7.7.0](#) or newer, refer to [Special Considerations for Updating to Luna Network HSM 7 Firmware 7.7.0 or Higher](#) before proceeding with the firmware update.

## Updating the HSM Firmware After an Appliance Software Update

After an appliance software update, the latest firmware version is saved on the appliance and ready to install.

### To update the HSM firmware after a software appliance update

1. Log in to LunaSH on the appliance as **admin**.
2. At the LunaSH prompt, login as HSM SO.  
lunash:> **hsm login**
3. [Optional Step] Check that the desired firmware version is ready to install.  
lunash:> **hsm firmware show**

**CAUTION!** If you are using STC on the HSM Admin channel, disable it by running lunash:> **hsm stc disable** before you update the HSM firmware.

4. Update the firmware to the version currently stored on the appliance.  
lunash:> **hsm firmware upgrade**

## Updating the HSM Firmware to a Different Version

If you are not installing the firmware update provided in the appliance software update, download your desired HSM firmware from the Thales Support Portal. You require:

- > Luna Network HSM 7 firmware update package file (<filename>.**spkg**)
- > the secure package authentication code, provided in a text file accompanying the update package

### To update the HSM firmware to a version downloaded from the Support Portal

1. Transfer the secure package update file to the Luna Network HSM 7 using **pscp** or **scp**.  
**pscp** <filepath>/<packagename>.**spkg** **admin**@<appliance\_host\_or\_IP>:
2. Stop all client applications to the Luna Network HSM 7 appliance.
3. Using a serial or SSH connection, log in to the appliance as **admin**.
4. At the LunaSH prompt, login as HSM SO.  
lunash:> **hsm login**
5. [Optional Step] Verify that the secure package file is present on the Luna Network HSM 7.  
lunash:> **package listfile**
6. [Optional Step] Verify the package file, specifying the authorization code you received from Thales.  
lunash:> **package verify** <filename>.**spkg** **-authcode** <code\_string>
7. Install the firmware update package, specifying the authorization code you received from Thales.  
lunash:> **package update** <filename>.**spkg** **-authcode** <code\_string>

**NOTE** If you are using a service provider model, you can use the `-useevp` option to specify the OpenSSL EVP (Digital EnVeloPe library) API to validate the update package, rather than invoking the HSM. This allows you to install the update package without logging in as HSM SO ([package update](#)).

The package update process takes a few seconds. The firmware package is now stored on the appliance, waiting to be applied to the HSM.

8. [Optional Step] Check that the desired firmware version is ready to apply.

```
lunash:> hsm firmware show
```

**CAUTION!** If you are using STC on the HSM Admin channel, disable it by running `lunash:> hsm stc disable` before you update the HSM firmware.

9. Update the firmware to the version currently stored on the appliance.

```
lunash:> hsm firmware upgrade
```

## Rolling Back the Luna HSM Firmware

When updating the HSM firmware, the Luna Network HSM 7 saves the previously-installed firmware version on the HSM. If required, you can roll back to this previously-installed version. Rollback allows you to try firmware without permanently committing to the new version.

Rollback does not create a new rollback target; a single rollback target is preserved when a firmware update is performed. After a rollback operation, no further rollback is possible until the next firmware update saves the pre-update version as the new rollback target.

**CAUTION!** *Update any factory-fresh Luna Network HSM 7 to newer firmware before rolling back.* The firmware rollback feature is intended to return the firmware to the previously installed version. Attempting a firmware rollback on a new appliance received directly from the Thales factory can result in RMA (return of product), as the pre-shipment firmware is a factory-test version that does not accept your credentials.

Firmware rollback is destructive; earlier firmware versions might have older mechanisms and security vulnerabilities that a new version does not. Back up any important materials before rolling back the firmware. This procedure zeroes the HSM and all cryptographic objects are erased.

**NOTE** Firmware rollback is not supported on HSMs that use Functionality Modules. If you have ever enabled **HSM policy 50: Allow Functionality Modules**, even if the policy is currently disabled, you cannot roll back the HSM firmware. See "[FM Deployment Constraints](#)" on page 252 for details.

### To roll back the Luna HSM firmware to the previous version

1. Check the previous firmware version that is available on the HSM.

```
lunash:> hsm firmware show
```

2. Back up any important cryptographic objects currently stored on the HSM (see [Partition Backup and Restore](#)).
3. At the LunaSH prompt, login as HSM SO.  
lunash:> **hsm login**
4. Roll back the HSM firmware.  
lunash:> **hsm firmware rollback**
5. Re-initialize the HSM and restore your partition(s) from backup.

## Upgrading HSM Capabilities and Partition Licenses

---

The Luna Network HSM 7 offers most customers all the capabilities they need. If your needs change, however, Thales offers upgrades on some Luna Network HSM 7 models. You can select these upgrades when you purchase your HSM, or you can order an upgrade license anytime after purchase and apply it yourself, using the Thales Licensing Portal.

This section provides guidelines and instructions for managing your licenses:

- > ["Purchasing an Upgrade License" on page 238](#)
- > ["Activating a License on the Thales Licensing Portal" on page 240](#)
- > ["Managing Your Thales Licensing Portal Account" on page 244](#)
- > ["Applying an Upgrade License on the HSM" on page 250](#)
- > ["Upgrade Troubleshooting" on page 251](#)

### Upgrade Options

Thales offers multiple options for upgrading your Luna Network HSM 7.

#### Factory Upgrades

You can select your desired upgrades at the time you purchase your HSM. Thales installs the upgrades at the factory, so that the license is activated when you receive your order. You receive an email from Thales's order entry system with the details of your upgrade license. You do not need to take any action; the upgraded HSM is ready for service.

If you plan to use the upgraded HSM as received, you do not need to create a portal account. If you do create an account, you can use it to transfer upgrade licenses from one Luna Network HSM 7 to another as desired.

#### Field Upgrades

If you have one of the approved Luna Network HSM 7 models, you can order upgrades at any time. After placing an upgrade order, you receive an email from Thales's order entry system with instructions on how to obtain your license through the portal. Attached to the email is an entitlement certificate with an entitlement identifier. You need this number when you create your portal account.

### **Upgradable HSM Models**

Luna Network HSM 7 comes in three models for your convenience. If you have a Luna Network HSM 7 model 750 or 790, you can purchase upgrade licenses and apply them yourself. At this time, the 700 model does not accept upgrades.

### **Upgrade Types**

Thales currently offers three types of HSM upgrade:

- > partition upgrade packs (of 5) to increase the maximum number of application partitions
- > Korea-specific cryptographic algorithms
- > Functionality Modules (allowed on FM-ready HSMs only)

### **License Revocation**

You may purchase and apply upgrades to any upgradable Luna Network HSM 7 appliance you own. If you have already applied an upgrade to an HSM and wish to remove it and apply it to a different HSM, you can revoke the license from one HSM so that it may be activated on the other. Contact Thales to revoke an upgrade license from an HSM.

### **Return Material Authorization**

In the unlikely event that you must return an HSM to Thales, the unit that you receive in exchange or receive back will have your purchased upgrades installed, and appearing on the portal as activated. Thales's customer care team will revoke upgrades in portal on your behalf so that the appliance sent to you has the correct upgrades. If you receive a replacement appliance, you will need to refer to the new serial number when managing your licenses.

## Purchasing an Upgrade License

To place an order for an upgrade, contact your Thales sales representative. If you are purchasing a new Luna Network HSM 7, you can opt for factory-installed upgrades or field upgrades that you can install yourself. Thales offers the following types of upgrade licenses:

- > partition upgrade packs (of 5) to increase the maximum number of application partitions
- > Korea-specific cryptographic algorithms
- > Functionality Modules (allowed on FM-ready HSMs only)

For example, a Luna Network HSM 7 S790 appliance comes with the base maximum number of 10 partitions. To upgrade the maximum to allow 30 partitions, you must order four (4) partition upgrades. After you apply this full entitlement to your HSM, you have the desired maximum 30 partitions. The following table summarizes the upgrade options for different models.

| HSM Model | Factory-Installed Partitions | Maximum Number of Partitions | Maximum Number of 5-Pack Upgrades |
|-----------|------------------------------|------------------------------|-----------------------------------|
| *700      | 5                            | 5                            | N/A                               |
| *750      | 5                            | 20                           | 3                                 |
| *790      | 10                           | 100                          | 18                                |

After you place your order for an upgrade and a Thales Customer Care representative has entered the order, you receive an email with detailed instructions on how to obtain and apply your upgrade.

### Entitlement Certificate

Attached to the upgrade email is an entitlement certificate. On this certificate is an entitlement identifier that you need to activate your upgrade. Here is an example of an entitlement certificate and where to find the EID.

#### Thales Luna HSM License Purchase

Thank you for your recent Thales Luna HSM order. Your Entitlement ID and description of licenses purchased is below. Please keep this for your records.

We thank you for your business.

|   |   |                            |          |
|---|---|----------------------------|----------|
| <b>Entitlement ID:</b> A9E44520-19C5-4DA7-8385-7FCB9FE0876C |   |                            |          |
|   |   |                            |          |
| <b>Sold To Customer:</b>                                    | Customer Name, Inc.                                   |                            |          |
| <b>End Customer:</b>  | Customer Name   |                            |          |
| <b>Customer Purchase Order:</b>                             | Demo  | <b>Thales Sales Order:</b> | 12345678 |
| <b>Item Number:</b>   | 908-000396-001  | <b>Quantity:</b>           | 20       |
| <b>Description:</b>   | PARTITION 5-PACK,LUNA NETWORK HSM 7 (FACTORY INSTALL) |                            |          |
| <b>Order Book Date:</b>                                     | 04/01/2021  |                            |          |

Next, see ["Activating a License on the Thales Licensing Portal"](#) on the next page.

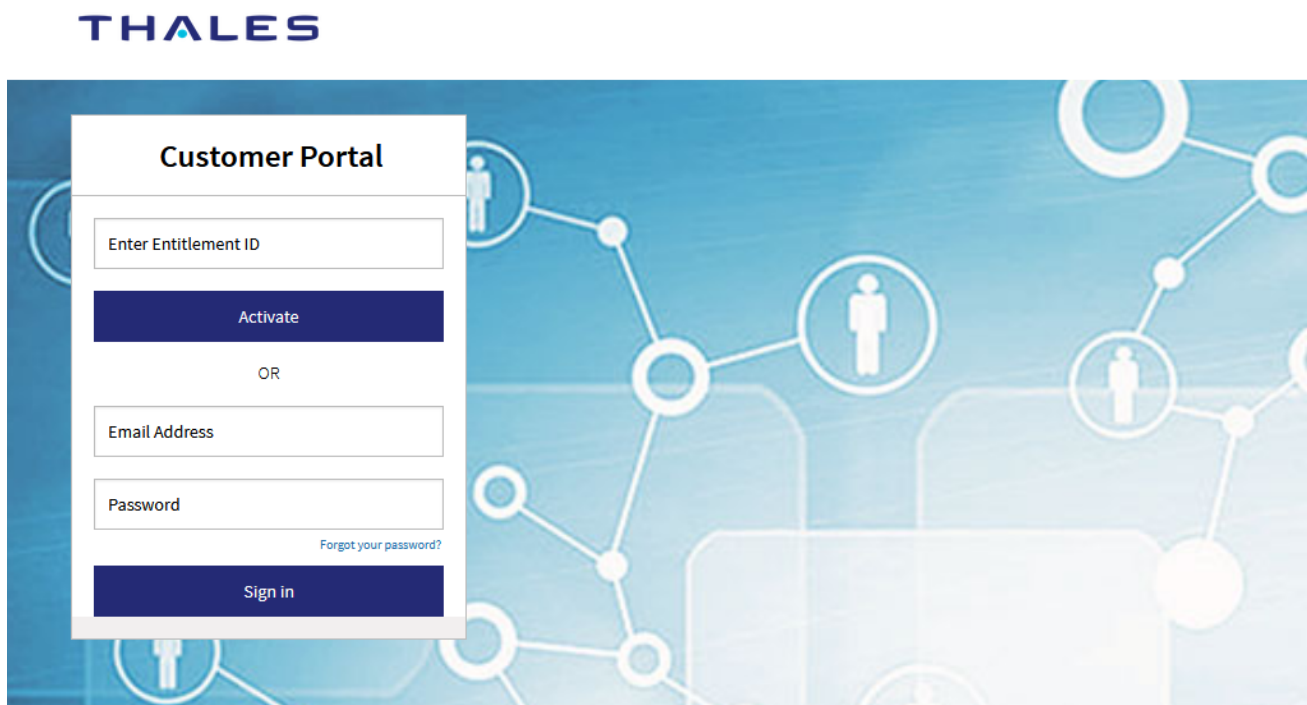
## Activating a License on the Thales Licensing Portal

After receiving the entitlement confirmation email, visit the Thales Licensing Portal and create an account to activate your upgrade license. You need the Entitlement ID from the confirmation email to complete this procedure.

### To activate a license

1. Navigate to the portal welcome page in your browser, enter the Entitlement ID from the email you received, and click **Activate**.

<https://safenetbelcamp.prod.sentinelcloud.com/ecp/>



2. If you do not already have an account, complete the mandatory user registration process by entering your email address and selecting a password and security questions, and click **Next**.

If you already have an account and are activating a new entitlement, click **Login** and enter your email address and password.



**THALES** English ▾

Licensing Portal Asterisk (\*) Indicates a required field

Please take some time to register with us. Already registered? Login

Enter Your Account Information

|   |  |
|---|--|
| <input type="text" value="Email Address*"/>         | <input type="text" value="Password*"/>         |
| <input type="text" value="Confirm Email Address*"/> | <input type="text" value="Confirm Password*"/> |

Set Your Security Preferences

|  |  |
|--|--|
| <input type="text" value="Security Question 1*"/>        | <input type="text" value="Security Question 2*"/>        |
| <input type="text" value="Security Question 1 Answer*"/> | <input type="text" value="Security Question 2 Answer*"/> |

Enter Your Personal Information

|                                    |   |  |
|------------------------------------|---|--|
| <input type="text" value="Name*"/> | <input type="text" value="Company Name"/> | <input type="text" value="United States"/> |
|------------------------------------|---|--|

**NOTE** The portal is arranged as a company account. Accounts with email addresses associated with a company are able to see all of that company's purchases. The association between a license and your company is created by registration and login using the Entitlement ID.

Multiple email addresses can be associated with your company. There is no limit.

If a registered portal user leaves the company, contact Thales Customer Support to make the adjustment.

- On the **License Activation** screen, enter the number of licenses from the entitlement that you wish to activate, and click **Next**.

**THALES** Zulu ▾ Home / Welcome ██████████

License Activation

|                         |                     |                 |
|-------------------------|---------------------|-----------------|
| Step 1 - Select License | Step 2 - Select HSM | Step 3 - Finish |
|-------------------------|---------------------|-----------------|

Company: ██████████ Order #: ██████ Order Date: ██████ Entitlement Expiration: No Expiration

Entitlement ID: 06129ec1-75ce-██████████

| Number | Product Name   | Activated | Available | Quantity To Activate                                |                                     |
|--------|--|-----------|-----------|---|-------------------------------------|
| 1      | PARTITION 5-PACK, LUNA HSM7+ (FIELD UPGRADE) 1.0<br><small>Part# 908-000395-001 Expiration: None</small> | 18        | 16        | <input style="width: 50px;" type="text" value="1"/> | <input checked="" type="checkbox"/> |

Cancel
Next

**NOTE** Partition licenses are distributed in packs of 5 -- for example, to apply licenses for 10 partitions, enter **2** (packs of 5 partitions), not **10**.

- Specify the HSM that will use this license by clicking **Enter New HSM SN** and entering the serial number. If you previously entered the HSM's serial number, click **Use Existing HSM SN** and select it from the drop-down menu. Click **Next**.

**THALES**

Zulu

Home / Welcome

### License Activation

| Step 1 - Select License  | Step 2 - Select HSM  | Step 3 - Finish |   |  |   |  |  |  |        |          |      |
|--|--|-----------------|---|--|---|--|--|--|--------|----------|------|
| Company: ██████████ Order #: ██████████ Order Date: 10/29/2020 Entitlement Expiration: No Expiration<br>Entitlement ID: 06129ec1-75ce-██████████   |  |                 |   |  |   |  |  |  |        |          |      |
| <table border="1"> <thead> <tr> <th>Product</th> <th>Apply to ⓘ</th> </tr> </thead> <tbody> <tr> <td>           PARTITION 5-PACK, LUNA HSM7+ (FIELD UPGRADE) 1.0<br/>           Part# 908-000395-001 Quantity To Activate : 1         </td> <td> <input checked="" type="radio"/> Enter New HSM SN    <input type="radio"/> Use Existing HSM SN<br/>           HSM SN: <input type="text" value="612886"/> </td> </tr> <tr> <td colspan="2"> <input type="text" value="Enter comments"/> </td> </tr> </tbody> </table> | Product  | Apply to ⓘ      | PARTITION 5-PACK, LUNA HSM7+ (FIELD UPGRADE) 1.0<br>Part# 908-000395-001 Quantity To Activate : 1 | <input checked="" type="radio"/> Enter New HSM SN <input type="radio"/> Use Existing HSM SN<br>HSM SN: <input type="text" value="612886"/> | <input type="text" value="Enter comments"/> |  | <table border="1"> <tr> <td>Cancel</td> <td>Previous</td> <td>Next</td> </tr> </table> |  | Cancel | Previous | Next |
| Product  | Apply to ⓘ   |                 |   |  |   |  |  |  |        |          |      |
| PARTITION 5-PACK, LUNA HSM7+ (FIELD UPGRADE) 1.0<br>Part# 908-000395-001 Quantity To Activate : 1  | <input checked="" type="radio"/> Enter New HSM SN <input type="radio"/> Use Existing HSM SN<br>HSM SN: <input type="text" value="612886"/> |                 |   |  |   |  |  |  |        |          |      |
| <input type="text" value="Enter comments"/>  |  |                 |   |  |   |  |  |  |        |          |      |
| Cancel   | Previous   | Next            |   |  |   |  |  |  |        |          |      |

- Your activation is now complete. The portal generates a license string that the Luna Network HSM 7 will use to validate an upgrade and apply it. Click **Download License File** to download a ZIP file containing this string. If you do not wish to install the upgrade at this time, click **Done**.

## License Activation

Step 1 - Select License

Step 2 - Select HSM

Step 3 - Finish

Company: ██████████ Order #: ██████████ Order Date: 10/29/2020 Entitlement Expiration: No Expiration  
 Entitlement ID: 06129ec1-75ce-██████████

## Activation Complete

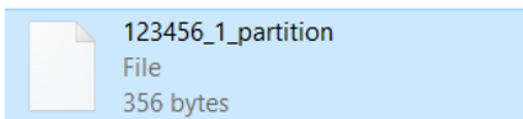
| Product Name  | Activated |
|---|-----------|
| PARTITION 5-PACK, LUNA HSM7+ (FIELD UPGRADE) 1.0<br>Part# 908-000395-001 Expiration: None | 1         |



Download License File

Done

6. Extract the license string file (default filename: **lserverc**) from the ZIP file. Thales recommends that you rename this file to something more distinctive, especially if you have multiple upgrades to manage. If you are managing upgrades for multiple HSMs, it is a good idea to include the HSM serial number, as in the example below.



```

123456_1_partition - Notepad
File Edit Format View Help
16 LUNA_PARTITIONS_5PACK 1.0 LONG NORMAL STANDALONE ADD 1_KEYS INFINITE_KEYS 27 APR 2021 19
48 NEVER NiL SLM_CODE CL_ND_LCK NiL *1DPEB4BL87NFNNX0400 NiL NiL NiL INFINITE_MINS NiL 0
59Kdd5R,Wd:uefzRzcTJV1ntw5:boCIzNstRvSkp4cVD4jvU8V9MvVhIhZ7nDmu83H19:HSNVV0ZTUfXbf56By30pXpcp
zdVMpi7:D92E4BBVOpqJRSqa41ProwVTABoJE3f##AID=bf1ac487-dc06-4709-a66e-3de4821d4fd4
Ln 1, Col 1 100% Unix (LF) UTF-8
  
```

Next, see ["Applying an Upgrade License on the HSM"](#) on page 250.

For more information about navigating the portal, see ["Managing Your Thales Licensing Portal Account"](#) on the next page.

## Managing Your Thales Licensing Portal Account

Once you have created your account, you can return to it at any time to manage and get information about your purchased licenses. The **My Assets** page is the home for this information. From this page, you can find the following information:

- > ["View Licenses by Product" below](#)
- > ["Activate New Entitlements" on the next page](#)
- > ["Products" on page 246](#)
- > ["Orders" on page 247](#)
- > ["Activations" on page 247](#)
- > ["Devices" on page 249](#)

### View Licenses by Product

To sort license information by product, choose the Thales product from the drop-down menu at the top left:

The screenshot shows the Thales Licensing Portal interface. At the top, there is a navigation bar with the Thales logo, a user profile dropdown (Zulu), and a home/welcome message. Below the navigation bar, there is a dropdown menu for product selection, currently set to 'All Products'. The main content area displays a table of products with the following columns: Product Name, Activated, Available, and View. The table contains five rows of product information, each with a 'View' button. An 'Export CSV' button is located in the top right corner of the table area.

| Product Name  | Activated | Available | View                 |
|---|-----------|-----------|----------------------|
| payShield HSM 10K 1<br>Part# HSM-PS10K  | 5         | 4         | <a href="#">View</a> |
| PARTITION 5-PACK, LUNA HSM7+ (FIELD UPGRADE) 1.0<br>Part# 908-000395-001                        | 35        | 15        | <a href="#">View</a> |
| PARTITION 5-PACK, LUNA HSM7+ (FACTORY INSTALL) 1.0<br>Part# 908-000396-001                      | 83        | 0         | <a href="#">View</a> |
| FUNCTIONALITY MODULES, LUNA NETWORK HSM 7+(FIELD UPGRADE) 1.0<br>Part# 908-000394-001           | 4         | 0         | <a href="#">View</a> |
| CRYPTO CMD CTR, MONITORING AND MANAGEMENT, PER PARTITION, PERPETUAL 3.0<br>Part# 908-000414-001 | 6         | 5         | <a href="#">View</a> |

## Activate New Entitlements

After you select the product type from the drop-down menu, you can activate any new licenses by entering the Entitlement ID in the upper right corner.

### Licensing Portal

My Assets ?

☰ Products (3)

**Instruction :** The following list displays all products that are available to your company. To view the list of orders for a given product, click the **View** button for that product. To activate a given order, click the associated **Activate** button from the list of orders.

| Products  |           | Export CSV |                      |  |
|---|-----------|------------|----------------------|--|
| Product Name ▼  | Activated | Available  | View                 |  |
| PARTITION 5-PACK, LUNA HSM7+ (FIELD UPGRADE) 1.0<br>Part# 908-000395-001              | 35        | 15         | <a href="#">View</a> |  |
| PARTITION 5-PACK, LUNA HSM7+ (FACTORY INSTALL) 1.0<br>Part# 908-000396-001            | 83        | 0          | <a href="#">View</a> |  |
| FUNCTIONALITY MODULES, LUNA NETWORK HSM 7+(FIELD UPGRADE) 1.0<br>Part# 908-000394-001 | 4         | 0          | <a href="#">View</a> |  |

## Products

To see the licenses you have purchased, expand the **Products** view. This page is a summary of upgrades, and shows the quantity available and how many are activated. Click **View** next to a product to see details.

### Licensing Portal

| Products  | Export CSV               |
|---|--------------------------|
| Product Name ▼  | Activated Available View |
| PARTITION 5-PACK, LUNA HSM7+ (FIELD UPGRADE) 1.0<br>Part# 908-000395-001              | 35 15 View               |
| PARTITION 5-PACK, LUNA HSM7+ (FACTORY INSTALL) 1.0<br>Part# 908-000396-001            | 83 0 View                |
| FUNCTIONALITY MODULES, LUNA NETWORK HSM 7+(FIELD UPGRADE) 1.0<br>Part# 908-000394-001 | 4 0 View                 |

## Orders

The **Orders** view provides details of each order you purchased. Click **Activate** next to an order to activate available licenses.



Zulu

Home / Welcome [Redacted]

Licensing Portal

| My Assets <span style="float: right;">Export CSV</span>   |              |                      |   |  |               |           |           |            |
|---|--------------|----------------------|---|--|---------------|-----------|-----------|------------|
| <span style="border: 1px solid #ccc; padding: 2px;">+ Products (3)</span>   |              |                      |   |  |               |           |           |            |
| <span style="border: 1px solid #ccc; padding: 2px;">- Orders (10)</span>  |              |                      |   |  |               |           |           |            |
| <b>Instruction :</b> The following list displays all orders for your company. Click <b>Activate</b> for an order to initiate an activation. |              |                      |   |  |               |           |           |            |
| Orders  |              |                      |   |  |               |           |           | Export CSV |
| Order Date  | Order Number | PO Number            | Product Name  | Entitlement ID                         | Order Details | Activated | Available | Activate   |
| 4/25/2022   | 10275248     | MW 12APR2022<br>CAF1 | PARTITION 5-PACK, LUNA HSM7+<br>(FACTORY INSTALL) 1.0<br>Part# 908-000396-001 Expiration:None | 1f72b815-970c-490d-<br>bcb0-[Redacted] |               | 18        | 0         | Activate   |
| 3/16/2022   | 10267593     | MW 07MAR2022<br>CAF1 | PARTITION 5-PACK, LUNA HSM7+<br>(FACTORY INSTALL) 1.0<br>Part# 908-000396-001 Expiration:None | 1a8855ab-c77f-4ca5-<br>b772-[Redacted] |               | 25        | 0         | Activate   |
| 3/2/2021  | 10193632     | MW 26FEB2021<br>CAF1 | PARTITION 5-PACK, LUNA HSM7+<br>(FACTORY INSTALL) 1.0<br>Part# 908-000396-001 Expiration:None | 6524fd98-fd6f-4817-[Redacted]          |               | 15        | 0         | Activate   |
| 3/2/2021  | 10193632     | MW 26FEB2021<br>CAF1 | PARTITION 5-PACK, LUNA HSM7+<br>(FACTORY INSTALL) 1.0<br>Part# 908-000396-001 Expiration:None | cd6a038c-0993-4180-<br>[Redacted]      |               | 15        | 0         | Activate   |
| 11/18/2020  | 10173018     | MW 16NOV2020<br>CAF1 | FUNCTIONALITY MODULES, LUNA<br>NETWORK HSM 7+(FIELD UPGRADE) 1.0                              | 54492815-90db-[Redacted]               |               | 1         | 0         | Activate   |

## Activations

The **Activations** view lists the entitlements you have previously activated. Click **Download** next to an activation to download the corresponding license string in a ZIP file.

Licensing Portal

My Assets **i**

Products (3)

Orders (10)

Activations (16)

**Instruction :** The following list displays all activations for your company.

Activations Export CSV

| Activation Date | Activation ID                    | Entitlement ID                   | HSM Serial Number | Locking Code     | Product Activated  | Download | Activated |
|-----------------|----------------------------------|----------------------------------|-------------------|------------------|--|----------|-----------|
| 8/18/2022       | 4dff31e5-3cf1-48b1-a400-████████ | 06129ec1-75ce-4002-9dc9-████████ | 612886            | *1748E8-████████ | PARTITION 5-PACK, LUNA HSM7+ (FIELD UPGRADE) 1.0<br>Part#908-000395-001 Expiration: None   | License  | 1         |
| 4/25/2022       | e838c0a5-884b-4958-b8f0-████████ | 1f72b815-970c-490d-bcb0-████████ | 646358            | *1U7MZ3-████████ | PARTITION 5-PACK, LUNA HSM7+ (FACTORY INSTALL) 1.0<br>Part#908-000396-001 Expiration: None | License  | 18        |
| 3/16/2022       | 34066dc7-0820-498e-baf2-████████ | 1a8855ab-c77f-4ca5-b772-████████ | 611869            | *132ZEE-████████ | PARTITION 5-PACK, LUNA HSM7+ (FACTORY INSTALL) 1.0<br>Part#908-000396-001 Expiration: None | License  | 12        |



## Devices

The **Devices** view shows all the HSMs you have registered on the portal. Click **View** next to a specific device to see more details (what features were activated and when, and the corresponding license string in a ZIP file).

Zulu

[Home](#) / Welcome 

Devices (12)

**Instruction :** The following list displays all devices that have an associated activation for your company.

| Devices           |                    | Export CSV  |           |                      |
|-------------------|--------------------|---|-----------|----------------------|
| HSM Serial Number | Locking Code       | Product Activated   | Activated | View                 |
| [REDACTED]        | *1LML4E [REDACTED] | PARTITION 5-PACK, LUNA HSM7+ (FACTORY INSTALL)<br>Part#908-000396-001 Expiration:None | 5         | <a href="#">View</a> |
|                   |                    | PARTITION 5-PACK, LUNA HSM7+ (FIELD UPGRADE)<br>Part#908-000395-001 Expiration:None   | 8         |                      |
| [REDACTED]        | *1PRKTJ [REDACTED] | PARTITION 5-PACK, LUNA HSM7+ (FIELD UPGRADE)<br>Part#908-000395-001 Expiration:None   | 8         | <a href="#">View</a> |
|                   |                    | PARTITION 5-PACK, LUNA HSM7+ (FACTORY INSTALL)<br>Part#908-000396-001 Expiration:None | 5         |                      |
| [REDACTED]        | *132ZEE [REDACTED] | PARTITION 5-PACK, LUNA HSM7+ (FACTORY INSTALL)<br>Part#908-000396-001 Expiration:None | 12        | <a href="#">View</a> |
| [REDACTED]        | *1748E8 [REDACTED] | PARTITION 5-PACK, LUNA HSM7+ (FIELD UPGRADE)<br>Part#908-000395-001 Expiration:None   | 1         | <a href="#">View</a> |
|                   |                    | PARTITION 5-PACK, LUNA HSM7+ (FACTORY INSTALL)<br>Part#908-000396-001 Expiration:None | 13        |                      |
| 623812            | *18U8Y6 [REDACTED] | PARTITION 5-PACK, LUNA HSM7+ (FACTORY INSTALL)<br>Part#908-000396-001 Expiration:None | 15        | <a href="#">View</a> |

## Applying an Upgrade License on the HSM

The license string file you downloaded from the portal (see ["Activating a License on the Thales Licensing Portal" on page 240](#)) is used to apply your HSM upgrade. The HSM Security Officer must complete this procedure.

### Prerequisites

- > Ensure that you have the license string file that is registered to the correct HSM serial number.
- > If you are installing partition upgrades, ensure that you have space available on the HSM. By default, partitions are created at a size that will utilize the entire HSM space based on the number of partition licenses at the time. If your existing partitions use all available space on the HSM, the new license application may fail with an error (LUNA\_RET\_RM\_CONFIG\_CHANGE\_FAILS\_DEPENDENCIES). To prevent this, reclaim space on the HSM by resizing the existing partitions (see ["Customizing Partition Sizes" on page 175](#)) before you apply the upgrade license.

### To apply an upgrade license on the HSM

1. Open a command prompt, navigate to the directory containing the license string file, and use **pscp/scp** to transfer it to an **admin**-level account on the Luna Network HSM 7 appliance.
 

```
pscp [options] <license_file> admin@<host/IP>:
```
2. Connect to the appliance via SSH or a serial connection, and log in to LunaSH using the **admin**-level account that received the file (see [Logging In to LunaSH](#)).
3. Log in as HSM SO (see ["Logging In as HSM Security Officer" on page 154](#)).

```
lunash:> hsm login
```

4. [Optional] Confirm that the HSM fingerprint matches the one in the license string. If this string does not match, the upgrade will not be applied.

```
lunash:> sysconf fingerprint license
```

```
Fingerprint for Use With Entitlement Management System
```

```
-----
HSM serial #123456 : *1DPEB4BL87NFNNX0400
```

```
License string:
```

```
16 LUNA_PARTITIONS_5PACK 1.0 LONG NORMAL STANDALONE ADD 1_KEYS INFINITE_KEYS 27 APR 2021
19 48 NEVER NiL SLM_CODE CL_ND_LCK NiL *1DPEB4BL87NFNNX0400 NiL NiL NiL INFINITE_MINS NiL 0
59Kdd5R,Wd:uefzRzcTJV1ntW5:boCIzNstRvSkP4cVD4jvU8V9MvVhIhZ7nDmu83H19:HSNVV0ZTUfXbf56By30
pXpcpzdVMpi7:D92E4BBVOpqJRSqa41ProwvTABoJE3f##AID=bf1ac487-dc06-4709-a66e-3de4821d4fd4
```

5. Apply the upgrade to the HSM.

```
lunash:> sysconf license apply -filename <license_file>
```

6. [Optional] Verify that the license has been applied.

```
lunash:> sysconf license list
```

**NOTE** The **QUANTITY** column represents the total number of additional partitions associated with a specific license. This column does not apply to other types of license upgrades.

## Upgrade Troubleshooting

If you are unable to apply an upgrade license from the Thales Licensing Portal, the table below provides descriptions of possible failure messages (lunash:> [sysconf license apply](#)).

| Message   | Description  |
|---|--|
| Cannot find <filename>  | The file that you specified containing the license string cannot be found on the HSM appliance. Use lunash:> <a href="#">my file list</a> to see what files are available.   |
| Cannot find lserverc  | You should not encounter this message. If you do, please contact Thales Technical Support for assistance.  |
| Invalid licensed feature                                      | The license string is corrupted in the feature attribute. Confirm that you saved the license string without modification after activating the upgrade in the portal.         |
| Invalid licensed feature version                              | The license string is corrupted in the feature version attribute. Confirm that you saved the license string without modification after activating the upgrade in the portal. |
| Invalid licensed HSM serial number                            | The license string is for an HSM with a different serial number. Ensure that you transferred the correct license string file to the appliance.                               |
| <feature> not licensed for this appliance                     | The license string is for an HSM with a different serial number. Ensure that you transferred the correct license string file to the appliance.                               |
| License is already applied                                    | The license string matches an entitlement already applied on this HSM appliance.   |
| LUNA_RET_HSM_TAMPERED   | The HSM is in a tampered state and must be cleared of the tampered state before the upgrade can be applied.  |
| Update Result : 12 (Error detecting HSM)                      | The HSM Security Officer is not logged in.   |
| License is unknown/not available (feature)                    | The HSM appliance software needs to be updated to support a newer feature.   |
| Upgrades not available for this model of HSM                  | Only 750 and 790 models of HSM support upgrades.   |
| Upgrade to <#> partitions not available for this model of HSM | Applying the upgrade would exceed the upper limit for the maximum number of partitions on the HSM.   |
| Unable to determine model of HSM                              | You should not encounter this message. If you do, please contact Thales Technical Support for assistance.  |

# CHAPTER 11: Functionality Modules

Functionality Modules (FMs) consist of your own custom-developed code, loaded and operating within the logical and physical security of a Luna Network HSM 7 as part of the HSM firmware. FMs allow you to customize your Luna Network HSM 7's functionality to suit the needs of your organization. Custom functionality provided by your own FMs can include:

- > new cryptographic algorithms
- > security-sensitive code, isolated from the rest of the HSM environment
- > keys and critical parameters managed by the FM, independent from standard PKCS#11 objects, held in tamper-protected persistent storage

To create FMs, you will need the Functionality Module Software Development Kit (SDK), which is included with the Luna HSM Client software. Applications that use FM functions are supported on Windows and Linux.

This chapter describes how to prepare the Luna Network HSM 7 to use FMs, and manage FMs on the HSM. For detailed information on the FM architecture and how to use FMs with your applications, refer to [About the FM SDK Programming Guide](#).

**NOTE** This feature requires minimum [Luna HSM Firmware 7.4.0](#), [Luna Network HSM 7 Appliance Software 7.4.0](#), and [Luna HSM Client 7.4.0](#).

This feature has hardware dependencies described in "[Preparing the Luna Network HSM 7 to Use FMs](#)" on page 256.

This chapter contains the following sections:

- > ["FM Deployment Constraints" below](#)
- > ["Preparing the Luna Network HSM 7 to Use FMs" on page 256](#)
- > ["Building and Signing an FM" on page 258](#)
- > ["Loading an FM Into the HSM Firmware" on page 262](#)
- > ["Deleting an FM From the HSM Firmware" on page 263](#)
- > ["Recovering the HSM After FM Failure" on page 264](#)

## FM Deployment Constraints

This section describes important considerations and constraints associated with deploying your Functionality Modules (FMs). Your Luna Network HSM 7 must meet all the criteria described in "[Preparing the Luna Network HSM 7 to Use FMs](#)" on page 256.

Introducing FMs into your Luna Network HSM 7 deployment will change the functionality of certain HSM features. Please take the following constraints into consideration before using FMs:

- > ["FMs and FIPS Mode" on the next page](#)

- > "FMs and High-Availability (HA)" below
- > "FMs and Backup/Restore/Cloning" on the next page
- > "FMs and Secure Trusted Channel (STC)" on the next page
- > "FMs and Appliance Re-imaging" on the next page
- > "FMs and HSM Firmware Rollback" on page 255
- > "FM Configuration and Remote PED" on page 255
- > "FM-Enabled HSM Cannot be Verified With CMU" on page 255
- > "Key Attributes" on page 255
- > "No EDDSA or EC\_MONTGOMERY Private Keys with C\_CreateObject" on page 255
- > "FM Sample Applications Dependent on General Cryptoki Samples" on page 255
- > "Memory for FMs" on page 256

**CAUTION!** Enabling FMs (**HSM policy 50**) introduces changes to Luna HSM functionality, some of which are permanent; they cannot be removed by disabling the policy. FM-enabled status is **not** reversible by Factory Reset.

If you are using Crypto Command Center, ensure that your CCC version supports FM-enabled HSMs before you enable **HSM policy 50**. Refer to the CCC CRN for details.

## FMs and FIPS Mode

FMs change the abilities of the HSM firmware, adding new cryptographic algorithms or other functions. Since the new functionality is not certified by NIST, be sure that your FM does not break FIPS compliance. To be certain that your organization is meeting FIPS requirements, ensure that you are using a FIPS-certified version of the Luna HSM firmware, and that your Luna Network HSM 7 has the following HSM policy settings:

- > **HSM policy 12: "Allow non-FIPS algorithms" on page 159: OFF**
- > **HSM policy 50: "Allow Functionality Modules" on page 165: OFF**

**NOTE** Using [Luna HSM Firmware 7.4.2](#) and older, this restriction is enforced; it is not possible to set **HSM policy 50: "Allow Functionality Modules" on page 165** to **ON** while **HSM policy 12: "Allow non-FIPS algorithms" on page 159** is **OFF**. Using newer firmware versions, it is possible to enable FMs in FIPS mode, but your FM functionality may not be FIPS-compliant; refer to NIST standards to ensure compliance.

If FIPS compliance is not required, then enabling FMs does not present an issue for you. Enabling Functionality Modules (setting **HSM policy 50: "Allow Functionality Modules" on page 165** to **ON**) is not reversible. For more information about HSM policies, see ["HSM Capabilities and Policies" on page 156](#).

## FMs and High-Availability (HA)

FM-specific functions must specify the exact HSM that will handle the operations. Therefore, the Luna HSM Client's HA implementation currently cannot accommodate FM functionality. If you want your FM-specific operations to be load-balanced across multiple HSMs, you must program this functionality into your applications yourself.

HA will still work with standard Luna operations.

For HA to function with Functionality Modules, all HSMs with application partitions in the HA group must have the same algorithms and functionality available. If one member partition does not have a required algorithm available in HSM firmware, cryptographic objects using that algorithm cannot be cloned to that partition, and this will disrupt HA functions.

Therefore, all HSMs containing HA group members must have FMs enabled (as described in "[Preparing the Luna Network HSM 7 to Use FMs](#)" on page 256), and they must all have the same FM(s) loaded. HA login requires two FM-enabled HSMs.

For more information about HA, see [High-Availability Groups](#).

## FMs and Backup/Restore/Cloning

To back up and restore objects on FM-enabled partitions, you require the following minimum Luna Backup HSM firmware versions:

- > [Luna Backup HSM 7 Firmware 7.7.1](#)
- > [Luna Backup HSM G5 Firmware 6.28.0](#)

As a general rule, cryptographic objects can be cloned from a partition with less-secure settings to one with identical or more secure settings. Therefore, it is not possible to clone objects from a standard partition to an FM-enabled partition.

To back up keys stored in the SMFS, your application must provide all the functions to back up and restore these keys.

## FMs and Secure Trusted Channel (STC)

To use functionality modules (FMs) with STC client connections, you require the newer version of STC, which is used in Client-V0/V1 partition connections. For more information, refer to [Secure Trusted Channel](#).

## FMs and Appliance Re-imaging

The FM-ready configuration required to make FMs work makes it impossible to re-image the appliance to the baseline version. This restriction comes into effect once **HSM policy 50: Enable Functionality Modules** is set to **1**, and it continues to apply even if the policy is set back to **0**. Attempting to re-image the appliance software once **HSM policy 50** has been enabled will return the following:

```
lunash:>sysconf reimage start

The HSM Administrator is logged in. Proceeding...

The HSM Functionality Module policy (policy 50) has
previously been enabled.
Enabling this policy at any time causes the Appliance Re-image feature
to become unavailable.
ERROR, Not all required pre-conditions to re-image the appliance were satisfied

Command Result : 65535 (Luna Shell execution)
```

## FMs and HSM Firmware Rollback

Enabling **HSM Policy 50** permanently disables the ability to roll back the HSM firmware to a version older than [Luna HSM Firmware 7.4.0](#). Attempting to roll back the firmware once **HSM policy 50** has been enabled will return the following error:

```
ERROR, failed to roll back HSM F/W!!!
```

```
Command Result : 65535 (Luna Shell execution)
```

## FM Configuration and Remote PED

Various FM functions require HSM resets (for example, creating a partition or enabling an FM).

If you are configuring FMs while authenticating with Remote PED, the Remote PED connection is broken with each reset. LunaCM continues to show an active Remote PED connection until you restart LunaCM. You must close that apparent connection with `lunash:> hsm ped disconnect` and then open it again with `lunash:> hsm ped connect` before you can resume remote configuration.

This might be required several times during Luna Network HSM 7 setup for FMs. To prevent this, enable **HSM Policy 51: "Allow SMFS Auto Activation"** on [page 166](#). If SMFS is not auto-activated, then the SMFS will require further individual PED prompts during the configuration process (SMFS is deactivated upon HSM reset if SMFS auto-activation is off).

**NOTE** Thales recommends that first time configuration of FM's be done locally, to minimize the issues mentioned above.

## FM-Enabled HSM Cannot be Verified With CMU

The FM-enabled Luna Network HSM 7 does not currently support confirming the HSM's authenticity using `cmu verifyhsm`, as described in [Verifying the HSM's Authenticity](#), or retrieving and confirming a Public Key Confirmation from the HSM using `cmu getpkc` and `cmu verifypkc`.

## Key Attributes

On an HSM with FMs enabled, keys that are derived or generated have the "always-sensitive" and the "never-extractable" attributes set to "false".

## No EDDSA or EC\_MONTGOMERY Private Keys with C\_CreateObject

This release of the Luna Network HSM 7 firmware does not allow FMs to use `C_CreateObject` to create EDDSA or EC\_MONTGOMERY private keys. Use `C_GenerateKeyPair` to create these types of key.

## FM Sample Applications Dependent on General Cryptoki Samples

When you install the FM SDK, the installation script ensures that the general Luna (PKCS) SDK and samples are also installed (first). This satisfies source dependencies for the FM samples. If you later delete or remove the Luna SDK, you might break those dependencies, and the FM samples will not build. You can manually correct this by performing a manual `rpm -i` of the `cksample` package.

## Memory for FMs

Multiple FMs can be loaded into the FM space of the HSM, with a total memory limit of:

- > 8 megabytes for FMs
- > 4 megabytes of SMFS

Unused FMs can be deleted, to free some memory space.

## Preparing the Luna Network HSM 7 to Use FMs

This section provides information on how to prepare your Luna Network HSM 7 to accept Functionality Modules (FMs). FMs require a specific factory configuration, the correct firmware version, a license upgrade, and the correct policy settings, as described below:

- > ["Step 1: Ensure You Have FM-Ready Hardware" below](#)
- > ["Step 2: Update Your HSM" on the next page](#)
- > ["Step 3: Purchase and Apply the FM Capability License" on the next page](#)
- > ["Step 4: Apply HSM Policy Settings" on the next page](#)

**CAUTION!** Enabling FMs (**HSM policy 50**) introduces changes to Luna HSM functionality, some of which are permanent; they cannot be removed by disabling the policy. FM-enabled status is **not** reversible by Factory Reset. Refer to ["FM Deployment Constraints" on page 252](#) for details before enabling.

If you are using Crypto Command Center, ensure that your CCC version supports FM-enabled HSMs before you enable **HSM policy 50**. Refer to the CCC CRN for details.

### Step 1: Ensure You Have FM-Ready Hardware

The FM feature requires a specific Luna Network HSM 7 hardware configuration that must be created by Thales at the factory. Luna Network HSM 7s that have this configuration are "FM-ready". If your Luna Network HSM 7 is not FM-ready, contact your Thales representative or Thales Customer Support for further guidance.

#### Determining Whether the HSM is FM-Ready

Currently, all Luna Network HSM 7s are FM-ready from the factory. HSMs older than this factory update are not. To determine if your HSM is FM-ready, check the Product Part # on the appliance label:

Product Part #:  
908-XXXXXX-003-A  
Product Serial #:  
XXXXXXXX



If the last 3-digit section of the Product Part # is **003** or higher, your HSM is FM-ready. If **002** or lower, contact your Thales representative or Thales Customer Support for guidance on how to obtain FM-ready hardware.



**NOTE Exception:** If your Luna Network HSM 7 includes 10GB optical Ethernet ports, your HSM is FM-Ready, even though the Product Part # ends in **001**.

## Step 2: Update Your HSM

To use FMs, you require [Luna Network HSM 7 Appliance Software 7.4.0](#) or newer, and [Luna HSM Firmware 7.4.0](#) or newer. You can download the latest software/firmware packages from the Thales Support Portal (see [Updating the Luna Network HSM 7 Appliance Software](#) and ["Updating the Luna HSM Firmware" on page 233](#)).

When you have completed the upgrade, you can check the output from `lunash:>hsm show` to ensure that the HSM is FM-ready:

```
Functionality Module HW:           FM Ready
=====
```

## Step 3: Purchase and Apply the FM Capability License

To use FMs, contact your Thales sales representative to purchase the FM capability license. You can validate the license on the Thales Licensing Portal (GLP) and install it with LunaSH. Refer to ["Upgrading HSM Capabilities and Partition Licenses" on page 236](#) for the procedure.

When you have activated your license on the HSM, you can use `lunash:>hsm displaylicenses` to check that it is installed:

```
HSM CAPABILITY LICENSES
License ID      Description
=====
621000068-000  K7 Base
621010185-003  Key backup via cloning protocol
621000046-002  Maximum 100 partitions
621000134-002  Enable 32 megabytes of object storage
621000135-002  Enable allow decommissioning
621000021-002  Maximum performance
621000138-001  Controlled tamper recovery
621000154-001  Enable decommission on tamper with policy off
621000074-001  Enable Functionality Modules
```

## Step 4: Apply HSM Policy Settings

Applying the FM capability license allows you to set 4 new HSM policies that affect FMs on the Luna Network HSM 7 (see ["HSM Capabilities and Policies" on page 156](#)). Use `lunash:>hsm showpolicies` to list HSM policies.

| Description                         | Value | Code  | Destructive |
|-------------------------------------|-------|-------|-------------|
| =====                               | ===== | ===== | =====       |
| Allow Functionality Modules         | Off   | 50    | Yes         |
| Allow SMFS Auto Activation          | Off   | 51    | Yes         |
| Restrict FM Privilege Level         | Off   | 52    | Yes         |
| Encrypt keys passing from FM to HSM | Off   | 53    | Yes         |

### HSM Policy 50: Allow Functionality Modules

With this policy enabled, Functionality Modules may be loaded to the HSM, permitting custom cryptographic operations. Allows use of the `ctfm` utility and FM-related commands, and the use of Functionality Modules in general with this HSM.

The HSM SO must set HSM policy 50 to 1 (ON) to use FMs on the Luna Network HSM 7. Changing this policy (OFF-to-ON or ON-to-OFF) will zeroize the HSM and it must be re-initialized.

**CAUTION!** Enabling FMs (**HSM policy 50**) introduces changes to Luna HSM functionality, some of which are permanent; they cannot be removed by disabling the policy. FM-enabled status is **not** reversible by Factory Reset. Refer to ["FM Deployment Constraints" on page 252](#) for details before enabling.

If you are using Crypto Command Center, ensure that your CCC version supports FM-enabled HSMs before you enable **HSM policy 50**. Refer to the CCC CRN for details.

### HSM Policy 51: Allow SMFS Auto Activation

With this policy enabled, the Secure Memory File System (SMFS) is automatically activated on startup, providing a secure, tamper-enabled location in the HSM memory where Functionality Modules can load keys and parameters. Auto-activation for SMFS, like auto-activation for multifactor quorum-authenticated partitions in general, persists through a power outage of up to 2 hours duration. If disabled, the HSM SO must manually activate the SMFS each time the HSM reboots or loses power.

Thales recommends setting HSM policy 51 to 1 (ON) to avoid having to manually re-activate the SMFS if you need to reboot the HSM. Changing this policy destroys all existing application partitions.

### HSM Policy 52: Restrict FM Privilege Level

With this policy enabled, FM privilege is restricted. By default, FM privilege permits FMs to see the sensitive key attributes (including key values) of cryptographic objects on application partitions. This privilege is necessary for most FMs, so that the Crypto Officer (CO) and Crypto User (CU) roles can use partition objects with the FM. However, some FMs might not require this privilege and it can be restricted to satisfy some certification requirements (such as Common Criteria).

FM privilege permits FMs to see the sensitive key attributes (including key values) of cryptographic objects on application partitions. This privilege is necessary for most FMs, so that the Crypto Officer (CO) and Crypto User (CU) roles can use partition objects with the FM. However, some FMs might not require this privilege and it can be restricted to satisfy some certification requirements (such as Common Criteria).

Unless you require CC certification, Thales does not recommend changing this policy from its default setting (OFF). Changing this policy destroys all existing application partitions.

### HSM Policy 53: Encrypt Keys Passing from FM to HSM

With this policy enabled, keys created by an FM are encrypted before crossing from the FM to the Functionality Module Crypto Engine interface (FMCE). This internal encryption may be required to satisfy some certification requirements (such as Common Criteria).

Unless you require CC certification, Thales does not recommend changing this policy from its default setting (OFF). Changing this policy (OFF-to-ON or ON-to-OFF) will destroy all existing application partitions.

## Building and Signing an FM

Once you have written your FM code, you must build the binary and then sign it using a private key on the HSM. A self-signed certificate is used to confirm the authenticity of the FM. This procedure will allow you to install the FM into your HSM firmware. Luna FMs must be built on a Linux system, so you can use the native **make**

command. The following example uses the **skeleton** sample FM, included with the Luna FM SDK.

The FM binary must be signed with a private key, and loaded into the HSM firmware with a self-signed certificate from the same keypair to verify its authenticity. You can use **mkfm**, included with the Luna HSM Client FM Tools, to sign your FM using a Luna application partition or your own Cryptoki signing station. The procedure below will show you how to use **mkfm**.

### Prerequisites

- > The FM binary must be built on a Linux client. You can use either a Windows or Linux client to perform the signing operation.
- > The FM Tools option in the Luna HSM Client software must be installed on the client or signing station.
- > The client must have access to an application partition on the Luna Network HSM 7. The Crypto Officer can create the keypair and certificate required.
- > **mkfm** requires access to a Cryptoki token (such as a Luna application partition) capable of using the CKM\_SHA512\_RSA\_PKCS mechanism.

### To build an FM binary

1. On your Linux client, navigate to the directory containing your FM code (<filename>.c). By default, FM samples provided with the Luna FM SDK are installed in **/usr/safenet/lunafmsdk/samples/**.

```
[user@myLunaClient ~]# cd /usr/safenet/lunafmsdk/samples/skeleton/fm/
[user@myLunaClient fm]# ls
hdr.c  makefile  skeleton.c
```

2. Use the Linux **make** command to build the FM binary.

#### # make

The **make** process creates two new sub-directories, **bin-ppc** and **obj-ppc**. Your FM binary is located in **bin-ppc**, named <filename>.bin.

```
[user@myLunaClient ~]# cd /usr/safenet/lunafmsdk/samples/skeleton/fm/bin-ppc/
[user@myLunaClient bin-ppc]# ls
skeleton.bin
```

### To create an FM signing certificate on an application partition

1. If this is the first FM you are signing, you must first create a keypair and self-signed certificate on the application partition. If you already have a certificate for FM signing stored on the appliance, skip this procedure.

**NOTE** A certificate used to sign an FM must have attribute CKA\_PRIVATE set as true.

If an existing certificate has Private=F, you can use the CMU tool to export that cert, then re-import it while setting **-private=T**.

Or, if the partition retains the FM signing keypair, you can run [cmu selfsigncertificate](#) again to re-create the certificate, this time setting **-private=T** explicitly.

To sign an FM with **mkfm**, you must use an RSA private key at least 2048 bits long. The Crypto Officer can use the **cmu** utility to create the keypair. You will be prompted for the CO credential.

**NOTE** Always provide unique labels for your keys. If multiple private keys exist with the same label, **mkfm** will use the newest key (with the greatest object handle value).

**cmu generatekeypair -labelpublic=<public\_key\_label> -labelprivate=<private\_key\_label> -keytype=rsa -sign=1 -verify=1**

```
[user@myLunaClient bin]# ./cmu generatekeypair -labelpublic=FMpub -labelprivate=FMpriv -
keytype=rsa -sign=1 -verify=1
Certificate Management Utility (64-bit) v7.4.0-208. Copyright (c) 2018 SafeNet. All rights
reserved.
```

```
Select token
[3] Token Label: myPartition
[4] Token Label: myPCIeHSM
Enter choice: 3
Please enter password for token in slot 3 : *****
```

```
Select RSA Mechanism Type -
[1] PKCS [2] FIPS 186-3 Only Primes [3] FIPS 186-3 Auxiliary Primes : 2
Enter modulus length (8 bit multiple) : 2048
```

**2. Check the contents of the partition to find the key handles.**

**cmu list**

```
[user@myLunaClient bin]# ./cmu list
Certificate Management Utility (64-bit) v7.4.0-208. Copyright (c) 2018 SafeNet. All rights
reserved.
```

```
Select token
[3] Token Label: myPartition
[4] Token Label: pcie7pwd45
Enter choice: 3
Please enter password for token in slot 3 : *****
```

```
handle=48      label=FMpriv
handle=45      label=FMpub
```

**3. Create a self-signed certificate on the partition by specifying a label, the public and private key handles, and any other attributes you wish to assign. You are prompted for required attributes (Common Name, serial number, start/end dates) that you do not specify.**

**cmu selfsigncertificate -slot <slot\_number> -label <cert\_label> -publichandle=<handle> -privatehandle=<handle>**

```
[user@myLunaClient bin]# ./cmu selfsigncertificate -slot 3 -publichandle=45 -
privatehandle=48 -label FMsign
Certificate Management Utility (64-bit) v7.4.0-208. Copyright (c) 2018 SafeNet. All rights
reserved.
```

```
Please enter password for token in slot 3 : *****
```

```
Enter certificate serial number : 1
Enter Subject 2-letter Country Code (C) : CA
Enter Subject State or Province Name (S) : ON
Enter Subject Locality Name (L) : Ottawa
Enter Subject Organization Name (O) : Thales
Enter Subject Organization Unit Name (OU) :
```

```

Enter Subject Common Name (CN) : FMsign
Enter EMAIL Address (E) :
Enter validity start date
  Year   : 2018
  Month  : 12
  Day    : 05
Enter validity end date
  Year   : 2019
  Month  : 12
  Day    : 31
Using "CKM_SHA256_RSA_PKCS" Mechanism

```

4. Export the certificate to the client file system, specifying the desired filename with **.cert** extension.

**cmu export** -slot <slot\_number> -label <cert\_label> -outputfile=<filename.cert>

```

[user@myLunaClient bin]# ./cmu export -slot 3 -label FMsign -outputfile=FMsign.cert
Certificate Management Utility (64-bit) v7.4.0-208. Copyright (c) 2018 SafeNet. All rights reserved.

```

Please enter password for token in slot 3 : \*\*\*\*\*

## To sign an FM

1. Use the **mkfm** utility included with the Luna HSM Client FM Tools to sign the FM, specifying the unsigned FM binary, the desired FM filepath/filename (with **.fm** extension), the slot number/name of the partition/token where the keypair is stored, and the private key label.

If you are specifying a slot number, include **-k SLOTID=<#>** instead of the partition name. If you are using a Cryptoki signing station other than a Luna 7.x application partition, include the **-c** option. You are prompted for the partition/token credential. By default, the Crypto Officer role is used; to use the Crypto User role instead, include the **-u** option.

**mkfm -f** <filepath/name>.bin **-o** <filepath/name>.fm **-k** <token\_or\_partition\_name/<private\_key\_label> [**-c**] [**-u**]

```

[root@k7tower bin-ppc]# ./mkfm -f /usr/safenet/lunafmsdk/samples/skeleton/fm/bin-ppc/skeleton.bin -o /usr/safenet/lunafmsdk/samples/skeleton/fm/bin-ppc/skeleton.fm -k myLunaPartition/FMpriv
Luna Functionality Module Signer Utility (64-bit) v7.4.0-208. Copyright (c) 2018 SafeNet. All rights reserved.

```

Please Enter the PIN: (for user 'co' on slot 3) \*\*\*\*\*

mkfm: Processing ELF file /usr/safenet/lunafmsdk/samples/skeleton/fm/bin-ppc/skeleton.bin

File successfully signed

The signed FM is now located in the directory you specified:

```

[user@myLunaClient ~]# cd /usr/safenet/lunafmsdk/samples/skeleton/fm/bin-ppc/
[user@myLunaClient bin-ppc]# ls
skeleton.bin skeleton.fm

```

Next, see ["Loading an FM Into the HSM Firmware" on the next page.](#)

## Loading an FM Into the HSM Firmware

A signed FM must be loaded into the HSM firmware to provide new functionality. The HSM SO can load FMs using LunaSH and the following procedure.

**NOTE** A certificate used to sign an FM must have attribute `CKA_PRIVATE` set as true. If an existing certificate has `Private=F`, you can use the CMU tool to export that cert, then re-import it while setting `-private=T`. Or, if the partition retains the FM signing keypair, you can run `cmu selfsigncertificate` again to re-create the certificate, this time setting `-private=T` explicitly.

### Prerequisites

- > Your HSM must meet the criteria described in "[Preparing the Luna Network HSM 7 to Use FMs](#)" on page 256.
- > **HSM policy 50: Allow Functionality Modules** must be enabled.
- > **HSM policy 51: Enable SMFS Auto Activation** must be enabled, if you intend to use auto-activation (recommended). Changing this policy later will erase all partitions and installed FMs.
- > Ensure that all destructive policies are set before you load FMs into the HSM firmware. Any change of a destructive policy will erase all loaded FMs.
- > The FM must be signed as described in "[Building and Signing an FM](#)" on page 258, using [Luna HSM Client 7.4.0](#) or newer. FMs built using the Luna 7.0.4 Tech Preview release are not compatible with this Luna version.
- > You require the FM signing certificate. If you have previously loaded an FM signed by the same key, the correct certificate is already present in the appliance **admin** files.

**NOTE** If you load an FM with the same FM ID as an already-loaded FM, it is considered an update, and replaces the existing FM.

### To load an FM into the HSM firmware

1. Use `pscp` or `scp` to transfer the signed FM to the appliance **admin** account.  
`pscp <signed_FM> admin@<host/IP>:`
2. Use `pscp` or `scp` to transfer the signing certificate to the appliance **admin** account. If you have previously loaded an FM signed by the same key, it should already be in the appliance **admin** files.
3. Connect to the appliance via SSH or a serial connection, and log in to LunaSH as **admin**.
4. Log in as HSM SO.  
`lunash:> hsm login`
5. [Optional] Confirm that the signed FM and the correct certificate are present in the **admin** files.  
`lunash:> my file list`
6. Load the FM to the HSM by specifying the FM and signing certificate files.  
`lunash:> hsm fm load -certFile <cert_file> -fmFile <FM_file>`

- Restart the HSM. It is not necessary to reboot the appliance.

```
lunash:> hsm restart
```

**NOTE** If you have FMs loaded, you must restart the HSM whenever you perform any of the following operations:

- > create a new partition and assign it to a client (even if it has the same slot number as a recently-deleted partition),
- > make a destructive change like re-initializing or zeroizing the HSM, or changing a destructive policy.

You will be unable to use the loaded FMs with new partitions until you restart the HSM. Use lunash:> **hsm restart**.

- Log back in as HSM SO.

```
lunash:> hsm login
```

- Activate the Secure Memory File System.

```
lunash:> hsm fm smfs activate
```

- [Optional] Confirm that the FM was loaded and is now enabled.

```
lunash:> hsm fm status
```

## Deleting an FM From the HSM Firmware

This procedure allows the HSM SO to delete a specified FM from the HSM firmware using LunaSH.

**NOTE** If you are replacing the currently-loaded FM with an updated version, you do not need to delete the old version. If the new version has the same FM ID, it will replace the original version in the HSM firmware (see "[Loading an FM Into the HSM Firmware](#)" on the previous page).

In addition to the procedure below, other actions can cause FMs to be deleted from the HSM and the SMFS to be erased. See "[Effects of Administrative Actions on Functionality Modules](#)" on page 265.

### Prerequisites

- > You require the FM ID of the FM you wish to delete.

### To delete an FM from the HSM firmware

- [Optional] List the FMs currently loaded on the HSM to obtain the desired FM ID.

```
lunash:> hsm fm status
```

- Log in as HSM SO.

```
lunash:> hsm login
```

- Delete the FM by specifying its FM ID.

```
lunash:> hsm fm delete -id <FM_ID>
```

4. [Optional] Check the FM status again. The deleted FM's status is listed as "Zombie". At this point the FM is disabled, and its data will be fully deleted the next time you restart the HSM.

```
lunash:> hsm fm status
```

```
Getting status of the FM on all available devices
```

```
Current Functionality Module Configuration for device 0:
```

```
Serial # : 66331
Model    : Luna K7
SMFS     : Activated

FM Label      : skeleton
FM ID         : a000
Version      : 1.01
Manufacturer  : Safenet Inc.
Build Time   : Wed Dec 5 14:44:47 2018 - EST
Fingerprint  : 78 7C E3 C2 01 54 B3 99 08 59
ROM size     : 7302
Status       : Zombie (reboot HSM to cleanup)
Startup Status: OK
```

```
Command Result : 0 (Success)
```

5. Restart the HSM. It is not necessary to reboot the appliance.

```
lunash:> hsm restart
```

## Recovering the HSM After FM Failure

In the event that an FM bug causes problems on the HSM, such as halting the HSM or other functionality issues, the HSM SO can take steps to recover the HSM. If you have important FM key objects stored in the Secure Memory File System (SMFS), you may be able to regain access to them. If you encounter issues with FM functionality, try the following before you proceed with recovery operations:

1. Debug your FM code. Build and sign the FM ("[Building and Signing an FM](#)" on page 258), and attempt to load it onto the HSM ("[Loading an FM Into the HSM Firmware](#)" on page 262). Loading an updated FM with the same FM ID will erase the old version and replace it.
2. If this does not fix the problem, or you are unable to load the patched FM, delete the old FM first ("[Deleting an FM From the HSM Firmware](#)" on the previous page).
3. If this does not work, continue to the recovery procedure below.

LunaSH includes the **hsm fm recover** command, which allows you to delete all FMs currently loaded on the HSM, erase the SMFS, or both. This provides a last resort for recovering HSM functionality when an FM causes a failure.

### Prerequisites

- > Try the methods above before continuing. If you are running multiple FMs, it may be simpler to delete and replace the one that is causing the issue.



## To recover the HSM after FM failure

1. Log in as HSM SO.

lunash:> **hsm login**

2. Erase all FMs currently loaded on the HSM. This will leave the SMFS intact and preserve any key material you may have stored there.

lunash:> **hsm fm recover -erase fm**

You may now attempt to load a patched version of your FM that addresses the cause of the issue. If this does not resolve the problem, continue to step 3.

3. Choose one of the following options:

**CAUTION!** Both of these options will erase the SMFS and any cryptographic objects you have stored there. If this is important key material, erasing the SMFS is a last resort to restore HSM functions.

- a. Erase the SMFS.

lunash:> **hsm fm recover -erase smfs**

- b. Erase both the loaded FMs and the SMFS

lunash:> **hsm fm recover -erase both**

4. Load your patched FM and restart the SMFS (see "[Loading an FM Into the HSM Firmware](#)" on page 262).

## Effects of Administrative Actions on Functionality Modules

| Action                                   | Deletes FMs |
|--|-------------|
| Destructive HSM Policy                   | Yes         |
| Zeroize on 3 bad SO attempts             | No          |
| <b>hsm zeroize</b> command               | No          |
| <b>hsm factoryReset</b> command          | Yes         |
| Decommission                             | Yes         |
| <b>hsm init</b> when already initialized | No          |
| Destructive CUF application              | Yes         |

NOTE: In all the above cases, the Secure Memory File System is re-initialized, destroying all contents.

**NOTE** Ensure that all destructive policies are set before you load FMs into the HSM firmware. Any change of a destructive policy will erase all loaded FMs.

# CHAPTER 12: Zeroizing or Resetting the HSM to Factory Conditions

During the lifetime of a Luna HSM, you might have cause to take the HSM out of service, and wish to perform actions to ensure that no trace of your sensitive material remains. Those events might include:

- > Placing the unit into storage, perhaps as a spare
- > Shipping to another location or business unit in your organization
- > Shipping the unit back to Thales for repair/re-manufacture
- > Removing the HSM permanently from operational use, for disposal at end-of-life

This chapter describes the available options in the following sections:

- > ["HSM Zeroization" below](#)
- > ["Resetting the Luna Network HSM 7 to Factory Condition" on the next page](#)
- > ["Comparing Zeroize, Decommission, Re-image, and Factory Reset" on page 269](#)
- > ["Comparison of Destruction/Denial Actions" on page 270](#)
- > ["Stored Data Integrity" on page 272](#)
- > ["Effects of Administrative Actions on Functionality Modules" on page 265](#)

See also [Re-Imaging or Decommissioning the HSM Appliance](#).

## HSM Zeroization

---

In the context of HSMs in general, the term "zeroize" means to erase all plaintext keys. Some HSMs keep all keys in plaintext within the HSM boundary. Luna HSMs do not.

In the context of Luna HSMs, keys at rest (keys or objects that are stored in the HSM/cryptographic module) are encrypted. Keys are decrypted into a volatile working memory space inside the HSM only while they are being used. Items in volatile memory disappear when power is removed. The action that we loosely call "zeroizing", or clearing, erases volatile memory as well as destroying the key that encrypts stored objects.

Any temporarily decrypted keys are destroyed, and all customer keys on the HSM are immediately rendered inaccessible and unrecoverable whenever you:

- > perform **hsm factoryreset**
- > make too many bad login attempts on the SO account
- > press the Decommission button on the Luna Network HSM 7 back panel
- > set a "destructive" HSM policy
- > perform HSM firmware rollback

The KEK (key encryption key that encrypts all user objects, partition structure, cloning vectors, masking vectors, etc.) is destroyed by a zeroization (erasure) or decommission event. At that point, any objects or identities in the HSM become effectively random blobs of bits that can never be decoded.

**NOTE** The next HSM power-up following a KEK zeroization automatically erases the contents of user storage, which were already an indecipherable blob without the original KEK. That is, any zeroizing event instantly makes encrypted objects unusable, and as soon as power is re-applied, the HSM immediately erases even the encrypted remains before it allows further use of the HSM.

The HSM must now be re-initialized in order to use it again, and initialization overwrites the HSM with new user parameters. Everything is further encrypted with a new KEK unique to that HSM.

Keys not encrypted by the KEK are those that require exemption and are not involved in user identities or user objects:

- > The Master Tamper Key, which enables tamper handling
- > The Remote PED Vector, to allow Remote PED-mediated recovery from tamper or from Secure Transport Mode
- > The hardware origin key that certifies the HSM hardware as having been built by Thales

## Resetting the Luna Network HSM 7 to Factory Condition

These instructions will allow you to restore your Luna Network HSM 7 to its original factory configuration. The HSM is zeroized, all partitions erased, and HSM policies are returned to their default settings. If you have performed firmware and appliance software updates, those remain in place, and are not affected by this procedure.

To revert to a baseline appliance software/firmware, see [Re-Imaging the Appliance to Factory Baseline](#).

To roll back the HSM firmware to the previous version, see ["Rolling Back the Luna HSM Firmware" on page 235](#).

For eIDAS compliance, **hsmrecover** function is added to factoryreset commands - see ["Stored Data Integrity" on page 272](#).

The standalone **hsmrecover** tool in the tools folder performs the same action, but can present additional messages that might be useful to Support engineers.

### Prerequisites

- > Only the HSM SO can perform factory reset.
- > If you have STC enabled on the HSM, disable it by turning off **HSM policy 39** before continuing (see ["Setting HSM Policies Manually" on page 170](#)).
- > You must access LunaSH via a serial console to execute **hsm factoryreset**.

### To reset the HSM to factory condition

1. Login as HSM SO.

```
lunash:> hsm login
```

2. Reset the HSM to factory settings.

lunash:> **hsm factoryreset**

3. Reset the appliance configuration (network settings, ssh, ntlm, etc.) to factory settings.

lunash:> **sysconf config factoryreset -service all**

4. Reboot the appliance.

## Comparing Zeroize, Decommission, Re-image, and Factory Reset

You can clear the contents of your Luna HSM, or the HSM may be cleared in response to an event. How this affects the contents and configuration of your HSM depends on whether the user partitions were deleted or whether the HSM was zeroized, decommissioned, re-imaged, or factory reset as detailed below:

| Action                | Command/Event   | Description  |
|-----------------------|---|--|
| Erase User Partitions | <ul style="list-style-type: none"> <li>&gt; Enable or disable a destructive HSM policy</li> </ul>   | <p>Destroy/erase all user partitions, but do not zeroize the HSM. Policy 46 "Disable Decommission" is the exception in that it zeroizes the HSM and erases all user partitions if the policy is changed. To bring the HSM back into service, you need to:</p> <ol style="list-style-type: none"> <li>1. Recreate the partitions</li> <li>2. Reinitialize the partition roles</li> </ol>                      |
| Zeroize               | <ul style="list-style-type: none"> <li>&gt; Too many bad login attempts on the HSM SO account</li> <li>&gt; Perform an HSM firmware rollback</li> <li>&gt; lunash:&gt; <b>hsm zeroize</b></li> </ul>      | <p>Deletes all partitions and their contents, but retains the HSM configuration (audit role and configuration, policy settings). To bring the HSM back into service, you need to:</p> <ol style="list-style-type: none"> <li>1. Reinitialize the HSM</li> <li>2. Recreate the partitions</li> <li>3. Reinitialize the partition roles</li> </ol>   |
| Decommission          | <ul style="list-style-type: none"> <li>&gt; Press the decommission button on the rear of the appliance.</li> <li>&gt; Enable <b>HSM Policy 40: Decommission on Tamper</b>, and tamper the HSM.</li> </ul> | <p>Deletes all partitions and their contents, the audit role, and the audit configuration. Retains the HSM policy settings. To bring the HSM back into service, you need to:</p> <ol style="list-style-type: none"> <li>1. Reinitialize the HSM</li> <li>2. Reinitialize the audit role and reconfigure auditing</li> <li>3. Recreate the partitions</li> <li>4. Reinitialize the partition roles</li> </ol> |

| Action                 | Command/Event                         | Description  |
|------------------------|---------------------------------------|--|
| Re-image the Appliance | lunash:> <b>sysconf reimage start</b> | <p>Formats the Luna Network HSM 7 file system, zeroizes the HSM, erases the appliance configuration, and resets the software/firmware to the baseline version. You will need to reconfigure the appliance and the HSM as if it were new, including setting a password for the <b>admin</b> role.</p> <div style="border: 1px solid orange; padding: 5px; margin-top: 10px;"> <p><b>CAUTION!</b> Re-imaging to an older appliance software version might expose vulnerabilities that were fixed in newer releases.</p> </div> |
| Factory Reset          | lunash:> <b>hsm factoryReset</b>      | Deletes all partitions and their contents, and resets all roles and policy configurations to their factory default values. To bring the HSM back into service, you need to completely reconfigure the HSM as though it were new from the factory.  |

## Comparison of Destruction/Denial Actions

Various operations on the Luna Network HSM 7 are intended to make HSM contents unavailable to potential intruders. The effect of those actions are summarized and contrasted in the following table, along with notes on how to recognize and how to recover from each scenario.

**Scenario 1:** MTK is destroyed, HSM is unavailable, but use/access can be recovered after reboot (See Note 1)

**Scenario 2:** KEK is destroyed (Real-Time Clock and NVRAM), HSM contents cannot be recovered without restore from backup See Note 2)

**Scenario 3:** Appliance admin password reset

| Event   | Scen. 1 | Scen. 2 | Scen. 3 | How to discover<br>(See Note 3)  | How to recover                  |
|---|---------|---------|---------|--|---------------------------------|
| <ul style="list-style-type: none"> <li>&gt; Three bad SO login attempts</li> <li>&gt; lunash:&gt; <b>hsm zeroize</b></li> <li>&gt; lunash:&gt; <b>hsm factoryreset</b></li> <li>&gt; Any change to a destructive policy</li> <li>&gt; Firmware rollback (See Note 4)</li> </ul> | NO      | YES     | NO      | <ul style="list-style-type: none"> <li>&gt; Log entry</li> <li>&gt; "HSM IS ZEROIZED" in HSM Details (from <b>hsm show</b>)</li> </ul> | Restore HSM objects from Backup |

| Event   | Scen. 1 | Scen. 2 | Scen. 3 | How to discover<br>(See Note 3)   | How to recover   |
|---|---------|---------|---------|---|--|
| Log in to Luna Network HSM 7 "recover" account (local serial connection)  | NO      | NO      | YES     | Log entry shows login by "recover"  | Log into appliance as admin, using the reset password "PASSWORD" and change to a secure password |
| <p>Hardware tamper</p> <ul style="list-style-type: none"> <li>&gt; Undervoltage or overvoltage during operation</li> <li>&gt; Under-temperature or over-temperature during operation</li> <li>&gt; Chassis interference (such as cover, fans, etc.)</li> </ul> <p>Software (command-initiated) tamper</p> <ul style="list-style-type: none"> <li>&gt; <code>lunash:&gt; hsm stm transport</code></li> </ul> | YES     | NO      | NO      | <p>Parse logs for text like "tamper", "TVK was corrupted", or "Generating new TVK", indicating that a tamper event was logged.</p> <p>Example:</p> <pre>RTC: external tamper latched/ MTK: security function was zeroized on previous tamper event and has not been restored yet</pre> <p>Also, keywords in logs like: "HSM internal error", "device error"</p> <p>Luna Network HSM 7 appliance front panel flashes error 30.</p> | Reboot<br>[See Note 1]   |
| <p>Decommission</p> <ul style="list-style-type: none"> <li>&gt; Pressing the Decommission button on the back of the appliance</li> </ul>  | NO      | YES     | NO      | <p>Look for log entry like:</p> <pre>RTC: tamper 2 signal/Zeroizing HSM after decommission...LOG (INFO): POWER-UP LOG DUMP END</pre>  | Restore HSM objects from Backup  |

| Event | Scen. 1 | Scen. 2 | Scen. 3 | How to discover<br>(See Note 3) | How to recover |
|-------|---------|---------|---------|---------------------------------|----------------|
|-------|---------|---------|---------|---------------------------------|----------------|

**Note 1:** MTK is an independent layer of encryption on HSM contents, to manage tamper and Secure Transport Mode. A destroyed MTK is recovered on next reboot. If MTK cannot be recovered, only restoring from backup onto a new or re-manufactured HSM can retrieve your keys and HSM data.

**Note 2:** KEK is an HSM-wide encryption layer that encrypts all HSM objects, excluding only MTK, RPK, a wrapping key, and a couple of keys used for legacy support. A destroyed KEK cannot be recovered. If the KEK is destroyed, only restoring from backup can retrieve your keys and HSM data.

**Note 3:** To check the health of a remote HSM, script a frequent login to the HSM host and execution of a subset of HSM commands. If a command fails, check the logs for an indication of the cause.

**Note 4:** These actions all create a situation where **hsm init** is required, or strongly recommended before the HSM is used again.

In addition, another event/action that has a destructive component is HSM initialization. See "[Initializing the HSM](#)" on page 149.

## Stored Data Integrity

Beginning with [Luna HSM Firmware 7.7.0](#), a new eIDAS-supporting feature called SDI, Stored Data Integrity, has been added that checks the integrity of the stored data. The HSM firmware will halt if it detects that objects have been corrupted. An *hsmrecover* function has been introduced, as part of the **hsm factoryReset** command to clear the storage and recover the HSM from the halt state without requiring RMA of the appliance.

If the HSM firmware halts because data in the volatile memory is corrupted, restarting the HSM using `lunash:>hsm restart` or rebooting the appliance (**sysconf appliance reboot**) should recover the HSM without losing data in permanent storage.

If the HSM firmware halts because data in the permanent flash storage is corrupted, the HSM is recovered by using the newly enhanced **hsm factoryReset** command which deletes all the partitions, zeroizes all the objects, and resets the policies.

Since **hsm factoryReset** is destructive, it is important to keep a regular backup of HSM objects in case the HSM ever goes into a state that requires factory reset.

Running the **hsm factoryReset** command, while the HSM is in normal working state, has the same behavior as before [Luna HSM Firmware 7.7.0](#).

Running the **hsm factoryReset** command, while the HSM is in a halt state (where the normal "factoryReset" fails), invokes the recovery process, which takes several minutes (6+ minutes) to complete. It is important to wait for the **hsm factoryReset** command to complete without interruption.

For an example of the output, see [hsm factoryreset](#). Also see "[Comparison of Destruction/Denial Actions](#)" on page 270.



