

## Luna HSM Client 10.2 for SafeNet Luna PCIe HSM HSM ADMINISTRATION GUIDE



## Document Information

<b>Product Version</b>	10.2
<b>Document Part Number</b>	007-000555-002
<b>Release Date</b>	26 May 2020

## Revision History

<b>Revision</b>	<b>Date</b>	<b>Reason</b>
Rev. A	26 May 2020	Initial release

## Trademarks, Copyrights, and Third-Party Software

Copyright 2001-2020 Thales Group. All rights reserved. Thales and the Thales logo are trademarks and service marks of Thales Group 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 Group 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

<b>Preface: About the HSM Administration Guide</b> .....	<b>10</b>
Customer Release Notes .....	10
Audience .....	11
Document Conventions .....	11
Support Contacts .....	13
<b>Chapter 1: SafeNet Luna PCIe HSM Hardware Installation</b> .....	<b>14</b>
Verifying the Integrity of Your Shipment .....	15
SafeNet Luna PCIe HSM Required Items .....	16
Basic SafeNet Luna PCIe HSM order items .....	16
PED-Authenticated SafeNet Luna PCIe HSM order items .....	17
Optional Items .....	19
Installing the SafeNet Luna PCIe HSM Hardware .....	20
Server Compatibility .....	20
Installing the SafeNet Luna PCIe HSM Card Into the Host Computer .....	20
Connecting a Chassis Intrusion Connector to the Tamper Header .....	22
Connecting a Local PED .....	23
Connecting a Remote PED .....	23
Replacing the SafeNet Luna PCIe HSM Battery .....	24
Required Items .....	24
Instructions .....	25
Prerequisites .....	25
Replacing the SafeNet Luna PCIe HSM Battery .....	25
<b>Chapter 3: Luna HSM Client Software Installation</b> .....	<b>27</b>
Windows Luna HSM Client Installation .....	28
Required Client Software .....	28
Prerequisites .....	28
Installing the Luna HSM Client Software .....	29
Modifying the Installed Windows Luna HSM Client Software .....	32
Java .....	33
SafeNet CSP and KSP .....	33
USB-powered PED .....	34
Modifying the Number of SafeNet Luna Backup HSM Slots .....	34
Uninstalling the Luna HSM Client Software .....	35
After Installation .....	37
Troubleshooting .....	37
Scripted/Unattended Windows Installation/Uninstallation .....	38
Command line options overview .....	38
Installing all components and features .....	40

Installing the Luna HSM Client for the SafeNet Luna Network HSM .....	41
Installing the Luna HSM Client for the SafeNet Luna PCIe HSM .....	41
Installing the Luna HSM Client for the SafeNet Luna USB HSM .....	41
Installing the Luna HSM Client for the SafeNet Luna Backup HSM .....	42
Installing the Luna HSM Client for Remote PED .....	42
Installation Location .....	42
Logging .....	43
Uninstalling the Luna HSM Client .....	43
Linux Luna HSM Client Installation .....	44
Installing the Luna HSM Client .....	44
Installing the Client Software .....	45
Controlling User Access to Your Attached HSMs and Partitions .....	48
Uninstalling the Client Software or Removing Components .....	49
Java .....	50
Scripted or Unattended Installation .....	50
Interrupting the Installation .....	51
Modifying the Number of SafeNet Luna Backup HSM Slots .....	51
Solaris Luna HSM Client Installation .....	52
Prerequisites .....	52
Installing the Client Software .....	53
Controlling User Access to Your Attached HSMs and Partitions .....	55
Uninstalling the Luna HSM Client Software .....	56
Java .....	56
Scripted or Unattended Installation .....	56
Interrupting the installation - [Ctrl] [C] .....	57
AIX Luna HSM Client Installation .....	58
Prerequisites .....	58
Installing the Client Software .....	58
Controlling User Access to Your Attached HSMs and Partitions .....	61
Uninstalling the Luna HSM Client Software .....	62
Installing Java .....	62
Scripted or Unattended Installation .....	62
Interrupting the Installation .....	63
Adding a DPoD HSM on Demand Service .....	63
Configuration File Summary .....	66
Updating the Luna HSM Client Software .....	79

**Chapter 4: Secure Transport Mode .....** 80

Recovering an HSM From Secure Transport Mode .....	81
Placing an HSM Into Secure Transport Mode .....	83

**Chapter 5: PED Authentication .....** 84

PED Authentication Architecture .....	84
Comparing Password and PED Authentication .....	85
PED Keys .....	86
PED Key Types and Roles .....	86
Shared PED Key Secrets .....	87

M of N Split Secrets (Quorum) .....	88
New-CPU PED Behavior Notes .....	89
SafeNet Luna PED Received Items .....	90
SafeNet Luna PED Hardware Functions .....	92
Physical Features .....	92
Keypad Functions .....	93
Modes of Operation .....	94
Local PED Setup .....	95
Local PED Troubleshooting .....	96
About Remote PED .....	97
Remote PED Architecture .....	97
PEDserver-PEDclient Communications .....	100
Remote PED Setup .....	101
Initializing the Remote PED Vector (RPV) and Creating an Orange Remote PED Key (RPK) .....	101
Installing PEDserver and Setting Up the Remote Luna PED .....	102
Opening a Remote PED Connection .....	104
Ending or Switching the Remote PED Connection .....	107
Remote PED Troubleshooting .....	107
PED Key Management .....	111
Creating PED Keys .....	111
Performing PED Authentication .....	116
Consequences of Losing PED Keys .....	118
Identifying a PED Key Secret .....	120
Duplicating Existing PED Keys .....	121
Changing a PED Key Secret .....	122
PEDserver and PEDclient .....	124
The PEDserver Utility .....	124
The PEDclient Utility .....	125
pedserver .....	126
pedserver appliance .....	127
pedserver appliance delete .....	128
pedserver appliance list .....	129
pedserver appliance register .....	130
pedserver mode .....	131
pedserver mode config .....	132
pedserver mode connect .....	134
pedserver mode disconnect .....	135
pedserver mode show .....	136
pedserver mode start .....	138
pedserver mode stop .....	140
pedserver regen .....	142
pedclient .....	142
pedclient mode assignid .....	144
pedclient mode config .....	145
pedclient mode deleteid .....	147
pedclient mode releaseid .....	148
pedclient mode setid .....	149

pedclient mode show .....	150
pedclient mode start .....	151
pedclient mode stop .....	153
pedclient mode testid .....	154
<b>Chapter 6: Audit Logging .....</b>	<b>155</b>
Audit limitations and Controlled tamper recovery state .....	158
The Audit Role .....	158
Audit Log Records .....	160
Audit Log Message Format .....	161
Audit Logging General Advice and Recommendations .....	164
Logging In as Auditor .....	166
Configuring and Using Audit Logging .....	166
Configuring Audit Logging .....	166
Exporting the Audit Logging Secret and Importing to a Verifying HSM .....	168
Reading the Audit Log Records .....	169
Audit Role Authentication Considerations .....	170
Audit Log Categories and HSM Events .....	170
Audit Log Troubleshooting .....	177
<b>Chapter 7: Initializing the HSM .....</b>	<b>178</b>
Initializing a New or Factory-reset HSM .....	178
Re-initializing the HSM .....	181
PED-authenticated HSM Initialization Example .....	181
Password-authenticated HSM Initialization Example .....	187
<b>Chapter 8: HSM Roles .....</b>	<b>189</b>
Logging In as HSM Security Officer .....	190
Changing a Role Credential .....	191
Name, Label, and Password Requirements .....	191
HSM Labels .....	192
Cloning Domains .....	192
Partition Labels .....	192
Role Passwords or Challenge Secrets .....	192
<b>Chapter 9: HSM Capabilities and Policies .....</b>	<b>193</b>
Setting HSM Policies Manually .....	200
Setting HSM Policies Using a Template .....	201
Creating an HSM Policy Template .....	202
Editing an HSM Policy Template .....	202
Applying an HSM Policy Template .....	203
<b>Chapter 10: Application Partitions .....</b>	<b>204</b>
Creating or Deleting an Application Partition .....	204
<b>Chapter 11: Security in Operation .....</b>	<b>206</b>
Security Effects of Administrative Actions .....	206

Tamper Events .....	211
Recovering from a Tamper Event .....	212
<b>Chapter 12: Monitoring the HSM .....</b>	<b>214</b>
HSM Status Values .....	214
System Operational and Error Messages .....	215
SNMP Monitoring .....	217
MIB .....	217
Installing the SafeNet SNMP Subagent .....	217
The SafeNet Chrysalis-UTSP MIB .....	219
The SafeNet Luna HSM MIB .....	220
hsmPolicyTable .....	223
hsmPartitionPolicyTable .....	223
hsmClientRegistrationTable .....	224
hsmClientPartitionAssignmentTable .....	224
SNMP output compared to SafeNet tools output .....	225
Frequently Asked Questions .....	226
Performance Monitoring .....	226
Partition Utilization Metrics .....	227
Rules of acquisition .....	227
Availability of Partition Utilization Metrics .....	228
Keycard and Token Return Codes .....	229
Library Codes .....	247
Vendor-Defined Return Codes .....	251
HSM Alarm Codes .....	257
Alarm Generation and Handling .....	257
FRAM LOG .....	258
List of HSM Alarm Codes .....	258
HSM Alarm Code Samples .....	263
Temperature - High Warning .....	263
Temperature – High Soft Tamper .....	263
Temperature – High Hard Tamper .....	264
Hard Tampers During Storage .....	265
Decommission with power on .....	265
<b>Chapter 13: HSM Updates and Upgrades .....</b>	<b>268</b>
Updating the SafeNet Luna PCIe HSM Firmware .....	268
Changing the Firmware Upgrade Permissions (Linux only) .....	269
Rolling Back the SafeNet Luna HSM Firmware .....	269
Upgrading HSM Capabilities .....	270
<b>Chapter 14: Functionality Modules .....</b>	<b>272</b>
FM Deployment Constraints .....	272
FMs and High-Availability (HA) .....	273
FMs and Backup/Restore/Cloning .....	273
FMs and HSM Firmware Rollback .....	274
FM Configuration and Remote PED .....	274

FM-Enabled HSM Cannot be Verified With CMU .....	274
Key Attributes .....	274
No EDDSA or EC_MONTGOMERY Private Keys with C_CreateObject .....	274
FM Sample Applications Dependent on General Cryptoki Samples .....	274
Memory for FMs .....	275
Preparing the SafeNet Luna PCIe HSM to Use FMs .....	275
Step 1: Ensure You Have FM-Ready Hardware .....	275
Step 2: Update to Luna HSM Firmware 7.4.0 or Higher .....	276
Step 3: Purchase and Apply the FM Capability License .....	276
Step 4: Apply HSM Policy Settings .....	276
Building and Signing an FM .....	278
Loading an FM Into the HSM Firmware .....	280
Deleting an FM From the HSM Firmware .....	282
Recovering the HSM After FM Failure .....	283
Effects of Administrative Actions on Functionality Modules .....	284
<b>Chapter 15: Zeroizing or Resetting the HSM to Factory Conditions .....</b>	<b>285</b>
HSM Zeroization .....	285
Decommissioning the HSM Card .....	286
Disabling Decommissioning .....	287
Resetting the SafeNet Luna PCIe HSM to Factory Condition .....	287
Comparing Zeroize, Decommission, and Factory Reset .....	288
Comparison of Destruction/Denial Actions .....	288
RMA and Shipping Back to Thales Group .....	290
End of Service and Disposal .....	290

# 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:

- > "SafeNet Luna PCIe HSM Hardware Installation" on page 14
- > "Luna HSM Client Software Installation" on page 27
- > "Secure Transport Mode" on page 80
- > "PED Authentication" on page 84
- > "Audit Logging" on page 155
- > "Initializing the HSM" on page 178
- > "HSM Roles" on page 189
- > "HSM Capabilities and Policies" on page 193
- > "Application Partitions" on page 204
- > "Security in Operation" on page 206
- > "Monitoring the HSM" on page 214
- > "HSM Updates and Upgrades" on page 268
- > "Functionality Modules" on page 272
- > "Zeroizing or Resetting the HSM to Factory Conditions" on page 285

The preface includes the following information about this document:

- > "Customer Release Notes" below
- > "Audience" on the next page
- > "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 this release that is not included in the customer documentation. Read the CRN to fully understand the capabilities, limitations, and known issues for this release. You can view or download the latest version of the CRN from the Technical Support Customer Portal at <https://supportportal.thalesgroup.com>.

## Audience

---

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

All products manufactured and distributed by Thales Group 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] [<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} {<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] [<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 to this service is governed by the support plan arrangements made between Thales and your organization. Please consult this support plan for further information about 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. The Customer Support Portal is 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. You can also use the portal to create and manage support cases.

**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: SafeNet Luna PCIe HSM Hardware Installation

This chapter describes how to install and connect a SafeNet Luna PCIe HSM. To ensure a successful installation, perform the following tasks in the order indicated:

1. Before unpacking your new hardware, refer to ["Verifying the Integrity of Your Shipment" on page 15](#) for safe unpacking instructions.
2. Ensure that you have all of the required components, as listed in ["SafeNet Luna PCIe HSM Required Items" on page 16](#)
3. Install and connect the hardware, as described in ["Installing the SafeNet Luna PCIe HSM Hardware" on page 20](#)
4. The SafeNet Luna PCIe HSM uses a 3.6V non-rechargeable lithium battery to provide backup power to its memory. If you need to replace this battery, see ["Replacing the SafeNet Luna PCIe HSM Battery" on page 24](#).

**CAUTION!** This product uses semiconductors that can be damaged by electro-static discharge (ESD). When handling the device, avoid contact with exposed components, and always use an anti-static wrist strap connected to an earth ground. In rare cases, ESD can trigger a tamper or decommission event on the HSM. If this happens, all existing roles and cryptographic objects are deleted.

The SafeNet Luna PCIe HSM has been tested with a variety of representative systems/servers with compliant PCI express slots. When a compatibility problem with a current brand and model computer arises, that information is made available via the Thales Support Portal.

If you encounter any issues when installing the SafeNet Luna PCIe HSM into a new server/host computer, first try a different PCI express slot. The design of certain motherboards or the associated BIOS may prevent proper communication with a SafeNet Luna PCIe HSM. For example, certain PCI express physical slots are intended for use only with a video card or another specific type of hardware, and the SafeNet Luna PCIe HSM may not work correctly in these slots.

If you encounter further issues, please contact Thales Group Technical Support.

# Verifying the Integrity of Your Shipment

**CAUTION!** Thales Group employs a number of security measures to allow you to verify that your new hardware was not intercepted in transit or otherwise tampered with before you received it. To verify the authenticity and handling history of your received items, review the following checklist before you unpack your new hardware, and then follow the checklist as you unpack each received item.

Step	Yes	No
<p>1. Do the items received (individual items, part numbers) match those listed in the enclosed packing list? If yes, go to the next step. If no, contact Thales support.</p>		
<p>2. Before you received the product, did you receive an advanced shipping notification providing details regarding the shipment (part numbers and serial numbers for the product and tamper-evident bags)? If yes, go to the next step. If no, contact Thales support.</p>		
<p>3. Are all of the tamper-evident bag serial numbers and tamper-evident label serial numbers listed in the advanced shipping notification present, and do they match the actual tamper-evident bag/label serial numbers received? If yes, go to the next step. If no, contact Thales support.</p>		
<p>4. Did you receive any tamper-evident bag/label serial numbers that are not listed on the advance shipping notification? If yes, contact Thales support. If no, go to the next step.</p>		
<p>5. </p> <p>Are there any signs of physical tampering? If tamper-evident labels are affixed to the received product, have any of these labels been damaged? Have the tamper evident bags been damaged in any way? The tamper seals on the sides indicate tampering if they show the <b>ALERT</b> markings as illustrated below. If yes, contact Thales support. If no, go to the next step.</p>		
<p>6. Once you have verified all of the received items, you can proceed with the installation.</p>		

# SafeNet Luna PCIe HSM Required Items

This section provides a list of the components you should have received with your SafeNet Luna PCIe HSM order. The specific items you received depend on whether you ordered a password-authenticated or a PED-authenticated SafeNet Luna PCIe HSM, and whether your order included a backup device or other options as described below.

## Basic SafeNet Luna PCIe HSM order items

The standard items that you should have received as your basic order for a SafeNet Luna PCIe HSM are:

Qty	Item
1	<b>SafeNet Luna PCIe HSM</b>  <p>The HSM comes fitted with a full-height mounting bracket.</p>
1	<b>Anti-Static Wrist Strap</b> 

Qty	Item
1	<b>Half-height mounting bracket</b>  <p>Use this bracket if you need to install the SafeNet Luna PCIe HSM into a half-height slot.</p>

## PED-Authenticated SafeNet Luna PCIe HSM order items

If you ordered a PED-authenticated SafeNet Luna PCIe HSM, you should have received some combination of the following items in addition to the items in the basic order.

Qty	Item
1+	<b>SafeNet Luna PED</b>  <p>Your order should include at least one PED device.</p> <p>If you intend to back up your SafeNet Luna PCIe HSM to a SafeNet Luna Backup HSM, then you require a Luna PED to connect to that Backup HSM.</p> <p>If you intend to combine remote operation and backup, you might prefer to have a second PED. It is possible to use a single Luna PED for both connections, and to simply change between local and remote mode as needed.</p> <p>Note that you can use PED keys that you already own and use with other HSMs if appropriate. You should purchase the number you need for your own convenient operation, and for backup/standby units as your security policies might require.</p>

Qty	Item
1	<p data-bbox="225 268 427 296"><b>Luna PED cable</b></p>  <p data-bbox="225 772 1417 835">Both the standard and remote-capable PED devices connect to your HSM using a Type A to Mini B USB cable.</p>
1	<p data-bbox="225 877 751 905"><b>SafeNet Remote PED Power Supply Kit [*]</b></p>  <p data-bbox="225 1381 1449 1476">If you ordered a Luna PED, your order should include a Luna PED power supply kit with the appropriate connection for your region. The power supply is auto-sensing and includes replaceable mains plug modules for international use.</p> <p data-bbox="225 1486 1449 1549">[* If you received a refreshed PED (updated internal hardware, and PED firmware 2.8.0 or newer), it is powered via the USB connection and does not require a separate, external power supply; none is supplied.]</p>

Qty	Item
1	<p><b>Ten-pack of iKey 1000 PED keys, and sheets of peel-and-stick labels</b></p> <p>Your order should include a set of iKey PED keys and peel-and-stick labels.</p>

## Optional Items

Your order may include a SafeNet Luna Backup HSM.

Qty	Item
1	<p><b>SafeNet Luna Backup HSM B700/B790</b></p> <p>You can back up your selected SafeNet Luna PCIe HSM partition contents (root keys, certificates, other items) to a SafeNet Luna Backup HSM. The SafeNet Luna Backup HSM is suitable for off-site storage and for backing up multiple HSM partitions. It can back up contents of password-authenticated or of PED-authenticated HSMs.</p> <p>Refer to <a href="#">Backup and Restore Using a G7-Based Backup HSM</a>.</p>

---

# Installing the SafeNet Luna PCIe HSM Hardware

---

This section describes how to perform the following tasks:

- > Install the SafeNet Luna PCIe HSM card into the host computer. See "[Installing the SafeNet Luna PCIe HSM Card Into the Host Computer](#)" below.
- > Connect a chassis intrusion connector to the tamper header on the card, if necessary. See "[Connecting a Chassis Intrusion Connector to the Tamper Header](#)" on page 22
- > Connect a local PED, if necessary. See "[Connecting a Local PED](#)" on page 23
- > Connect a remote PED, if necessary. See "[Connecting a Remote PED](#)" on page 23

## Server Compatibility

The SafeNet Luna PCIe HSM conforms to the PCIe 2.0 standard and requires a PCIe x4 or higher slot. There are no known incompatible servers at this time.

**NOTE** Do not install the SafeNet Luna PCIe HSM into a slot reserved for a dedicated function, such as video. If you do, the host system might not boot successfully.

## Installing the SafeNet Luna PCIe HSM Card Into the Host Computer

Install the SafeNet Luna PCIe HSM card into an open PCIe slot on the host computer.

**CAUTION!** This product uses semiconductors that can be damaged by electro-static discharge (ESD). When handling the device, avoid contact with exposed components, and always use an anti-static wrist strap connected to an earth ground. In rare cases, ESD can trigger a tamper or decommission event on the HSM. If this happens, all existing roles and cryptographic objects are deleted.

### Prerequisites

- > Ensure that the PCIe slot is unpowered before you proceed with the installation.

---

### To install the SafeNet Luna PCIe HSM hardware

1. Open your computer, and remove the slot-cover bracket from an available PCIe slot. If the bracket is secured by a screw, keep that screw.
2. Use the provided anti-static wrist-strap to ground yourself to an exposed metal part of the computer chassis.
3. Remove the SafeNet Luna PCIe HSM from its anti-static packaging and prepare to insert the card into your computer.

Your SafeNet Luna PCIe HSM comes fitted with a full-height mounting bracket, but if you have no full-height slots available, the card can fit into a half-height slot. A half-height mounting bracket is included for this purpose. To install the half-height bracket, remove the two screws connecting the full-height bracket to the card, and use them to mount the half-height bracket in its place.

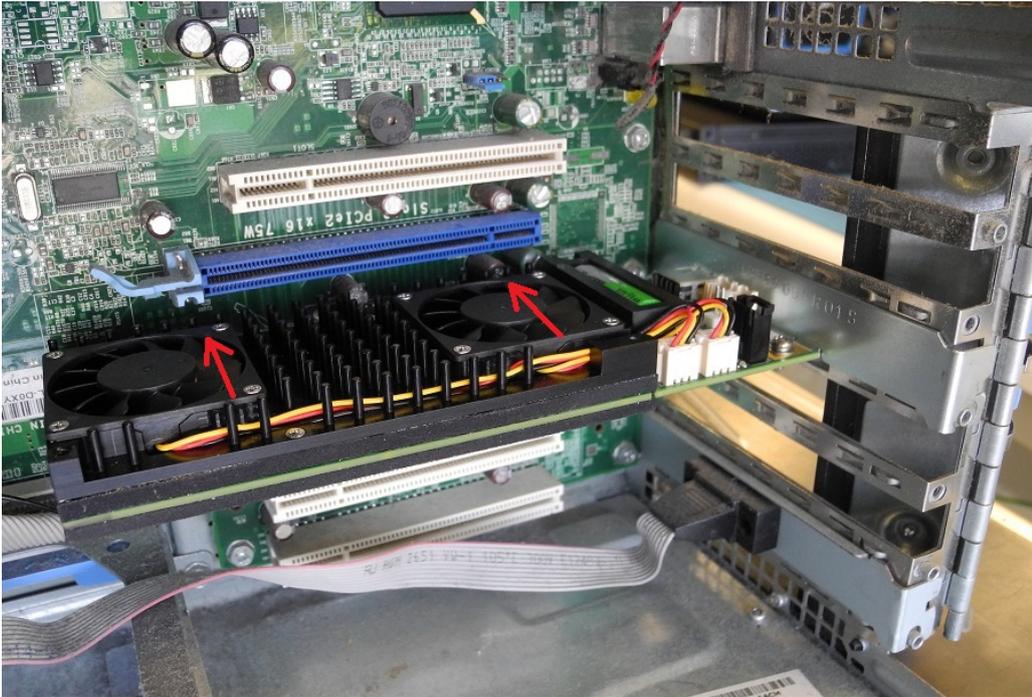


4. Align the SafeNet Luna PCIe HSM card with the vacant, unpowered slot. You might need to introduce the tip of the card-hold-down bracket first (the silver-metal part along the back edge of the card), in order to properly align the card with the connector.

You can use a PCIe X4 or larger slot, as long as it is wired for at least four PCI express channels, and not reserved for a dedicated function. For example, we do not recommend that you use your SafeNet Luna PCIe HSM card in a designated PCI express video slot - different models of computer and their BIOS firmware can differ in how faithfully they support the PCIe standard.



5. Insert the SafeNet Luna PCIe HSM card into the connector. It should go straight in – angling the card might cause it to bend. The card is properly seated when no portion of the gold-colored contacts of the card-edge protrudes above the connector socket.



6. Secure the card hold-down bracket with a screw or other restraint, as appropriate in your computer.

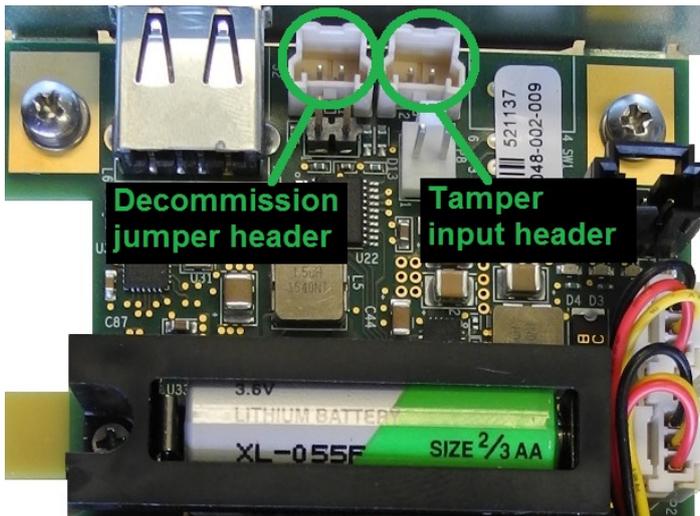
## Connecting a Chassis Intrusion Connector to the Tamper Header

The SafeNet Luna PCIe HSM is equipped with a two-pin tamper header which, when shorted, places the HSM in a tamper state with a status of Chassis Open. If your chassis is so equipped, you can connect the chassis intrusion connector to the tamper header so that the HSM is placed in a tamper state if the chassis is opened. Refer to the documentation provided by your chassis manufacturer for more information.

### To connect a chassis intrusion connector to the tamper header

1. Install the card as described in "[Installing the SafeNet Luna PCIe HSM Card Into the Host Computer](#)" on [page 20](#).
2. Connect the chassis intrusion connector to the tamper input header on the card, shown below.

**NOTE** If used, this pin pair would usually be wired to a chassis switch that is held open when the lid or panel is in place. Opening the lid or panel would allow the switch to close, and tamper the HSM. If you are constructing or ordering a cable for this purpose, the header has 2mm pin pitch and mates with a Molex connector ([https://www.molex.com/molex/products/datasheet.jsp?part=active/0355070200\\_CRIMP\\_HOUSINGS.xml](https://www.molex.com/molex/products/datasheet.jsp?part=active/0355070200_CRIMP_HOUSINGS.xml)) or equivalent.



## Connecting a Local PED

The local Luna PED (or a Luna PED Remote used locally) connects directly to the USB port on the SafeNet Luna PCIe HSM card via a USB-to-MiniUSB cable.

### To connect a local PED to the SafeNet Luna PCIe HSM:

1. Use the Luna PED local cable (mini-USB to USB) to connect the Luna PED to the SafeNet Luna PCIe HSM card:
  - a. Plug the mini-USB connector on the cable into the mini-USB port on the PED.
  - b. Plug the USB connector on the cable into the USB port on the card.

## Connecting a Remote PED

The Remote-Capable PED can be used either locally, connected directly to a SafeNet Luna HSM (exactly as for the standard PED), or remotely when connected to a suitable workstation and to the electrical main power supply. The normal local use of a PED with Remote PED capability is to use it in local mode to prepare an HSM (imprint an RPK – the orange key with a Remote PED Vector) before shipping it to its remote location. Then you would switch to Remote PED mode.

To prepare an HSM for Remote PED operation you need to connect it locally and imprint the HSM with a Remote PED key (orange). Once the HSM can be reached via remote desktop connection, and the HSM is associated with an orange PED key, all further configuration and administration can be performed remotely.

### To connect a remote PED to the SafeNet Luna PCIe HSM:

1. Use the Luna PED local cable to connect the Luna PED to the SafeNet Luna PCIe HSM card. This step is required to imprint the HSM with a Remote PED Vector (RPV) using the orange PED key (RPK). This should be the only time you need to connect a PED locally to the HSM. Once the orange PED key is imprinted with the same RPV as the HSM, all future PED operations can be performed remotely.
2. Follow the instructions in the *Administration Guide* to configure the remote PED. Note that you must install at least the Remote PED optional component of the Luna HSM Client software before you can configure the remote PED. See ["Luna HSM Client Software Installation" on page 27](#).

# Replacing the SafeNet Luna PCIe HSM Battery

The SafeNet Luna PCIe HSM uses a 3.6V non-rechargeable lithium battery to provide backup power to its memory. This enables the HSM to preserve cryptographic material even when the host system loses power. The battery may need replacement over the course of the HSM's lifetime. To see if your battery needs to be replaced, run **hsm envshow** in LunaCM. A warning is returned if the battery's voltage drops below 2.75 V.

**CAUTION!** Unless temporary battery power is supplied to the HSM while the main battery is replaced, all cryptographic material will be erased. Use the SafeNet Luna PCIe HSM Temporary Battery Holder to ensure a continuous power supply.

## Required Items

To replace the battery, you will need the following items. Battery manufacturer information is suggested.

Qty	Item	Description/Specifications	Manufacturer	Part Number
1	SafeNet Luna PCIe HSM replacement battery	2/3AA, 3.6V, 1650 mAh, Li-COCl <sub>2</sub> , length 33.5 mm, diameter 14.55 mm	OmniCel	ER14335/S
			Xeno Energy	XL-055F
1	Temporary Battery Holder	Used with a temporary battery to maintain power to the SafeNet Luna PCIe HSM during the replacement process. Can be requested from Thales Group.  	Thales Group	908-000408-001
1	Temporary Battery	AA, 3.6V, 1650 mAh, Li-COCl <sub>2</sub> , length 50.3 mm, diameter 14.55 mm	Saft	LS14500-AA

---

# Instructions

---

**CAUTION!** Back up any important cryptographic material on the HSM before proceeding. Removing the card from the host system will cause a tamper event. If **HSM policy 40: Decommission on Tamper** is enabled, the application partition and all roles are destroyed, and you must reconfigure the HSM after this procedure.

## Prerequisites

To replace the battery, you must first remove the SafeNet Luna PCIe HSM card from the host system.

**CAUTION!** This product uses semiconductors that can be damaged by electro-static discharge (ESD). When handling the device, avoid contact with exposed components, and always use an anti-static wrist strap connected to an earth ground. In rare cases, ESD can trigger a tamper or decommission event on the HSM. If this happens, all existing roles and cryptographic objects are deleted.

1. Test the temporary and replacement batteries with a voltmeter or multimeter. If either battery's voltage is below 3.1 V, it is depleted and must be replaced.

**CAUTION!** You must use the temporary battery specified in "[Required Items](#)" on the [previous page](#). Standard AA voltage is too low to power the SafeNet Luna PCIe HSM.

2. [Optional] If the card will not be in your possession the entire time it is out of service, you can enable Secure Transport Mode (see "[Secure Transport Mode](#)" on [page 80](#)). This allows you to know if the card has been tampered with while it was out of your possession.
3. Power off the host machine and disconnect it from power.
4. Use an anti-static wrist strap (provided with your SafeNet Luna PCIe HSM) to ground yourself to an exposed metal part of the computer chassis.
5. Remove the SafeNet Luna PCIe HSM from its PCIe slot.

## Replacing the SafeNet Luna PCIe HSM Battery

To maintain HSM power, you must connect a temporary battery while replacing the main battery.

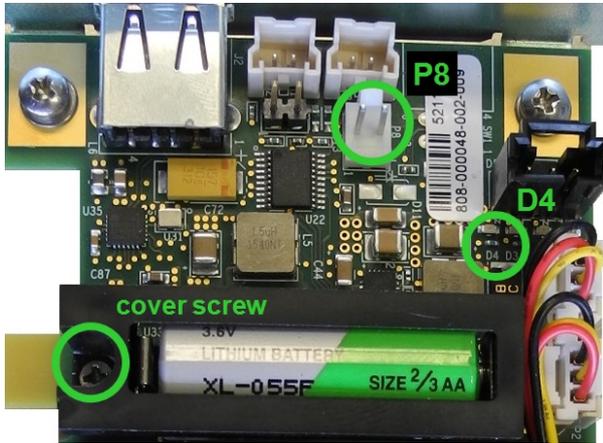
---

### To replace the SafeNet Luna PCIe HSM battery:

1. Install the temporary battery in the temporary battery replacement holder.
2. Install the 2-pin plug from the battery holder onto the 2-pin header marked **P8** on the SafeNet Luna PCIe HSM card.

**NOTE** The polarity on the **P8** header is not reversible. The jumper will only fit onto the header in the correct direction.

The SafeNet Luna PCIe HSM card's green **D4** LED is illuminated. This indicates that the card is receiving power from the temporary battery. If the LED appears dim, ensure that the temporary battery's voltage is greater than 3.1 V.



3. If necessary, remove the screw securing the battery cover.
4. Replace the 2/3AA battery on the card. Note the correct polarity.
5. Replace the battery cover and secure it with the screw.
6. Remove the jumper from the **P8** header to disconnect the temporary power.
7. Reinstall the SafeNet Luna PCIe HSM card.
8. Dispose of the depleted battery according to regional recycling regulations.

# CHAPTER 3: Luna HSM Client Software Installation

You can install the client for all SafeNet General Purpose HSMs, or for a specific type (Network or PCIe). Install the client as follows:

- > For SafeNet Luna Network HSM, install the Luna HSM Client on any computer that must connect to the appliance as a client.
- > For SafeNet Luna PCIe HSM, install the Luna HSM Client on the workstation into which the SafeNet Luna PCIe HSM is installed.
- > Install the Luna HSM Client on any computer that is to have a Remote Luna PED connected.
- > Install the Luna HSM Client on any computer that is to serve as a Remote Backup server.

For a list of supported operating systems by client version, refer to the CRN:

- > [Supported Luna HSM Client Operating Systems](#)

Choose the instructions for your operating system:

- > ["Windows Luna HSM Client Installation" on the next page](#)
  - ["Scripted/Unattended Windows Installation/Uninstallation" on page 38](#)
- > ["Linux Luna HSM Client Installation" on page 44](#)
- > ["AIX Luna HSM Client Installation" on page 58](#)
- > ["Solaris Luna HSM Client Installation" on page 52](#)
- > ["Adding a DPoD HSM on Demand Service" on page 63](#)
- > ["Configuration File Summary" on page 66](#)
- > ["Updating the Luna HSM Client Software" on page 79](#)

## Windows Luna HSM Client Installation

This section describes how to install the Luna HSM Client software on Windows. It contains the following topics:

- > "Required Client Software" below
- > "Prerequisites" below
- > "Installing the Luna HSM Client Software" on the next page
- > "Modifying the Installed Windows Luna HSM Client Software" on page 32
- > "Java" on page 33
- > "SafeNet CSP and KSP" on page 33
- > "Modifying the Number of SafeNet Luna Backup HSM Slots" on page 34
- > "Uninstalling the Luna HSM Client Software" on page 35
- > "After Installation" on page 37
- > "Troubleshooting" on page 37
- > "Scripted/Unattended Windows Installation/Uninstallation" on page 38

Applicability to specific versions of Windows is summarized in the Customer Release Notes for this release.

**NOTE** Before installing a SafeNet Luna HSM system, confirm that the product you have received is in factory condition and has not been tampered with in transit. Refer to the Startup Guide included with your product shipment. If you have any questions about the condition of the product that you have received, contact Technical Support immediately.

### Required Client Software

Each computer that connects to a SafeNet Luna Network HSM as a Client must have the cryptoki library, the **vtl** client shell and other utilities and supporting files installed.

Each computer that contains, or is connected to a SafeNet Luna PCIe HSM or a SafeNet Luna USB HSM must have the cryptoki library and other utilities and supporting files installed.

### Prerequisites

The Luna HSM Client installer requires the Microsoft Universal C Runtime (Universal CRT) to run properly. Universal CRT requires your Windows machine to be up to date. Before running the installer, ensure that you have the Universal C Runtime in Windows (KB2999226) update and its prerequisites installed on your machine. The following updates must be installed in order:

1. March 2014 Windows servicing stack update (See <https://support.microsoft.com/en-us/help/2919442>)
2. April 2014 Windows update (See <https://support.microsoft.com/en-us/help/2919355>)
3. Universal C Runtime update (See <https://support.microsoft.com/en-us/kb/2999226>)

## Installing the Luna HSM Client Software

Luna HSM Client can be installed on 64-bit Windows operating systems. Hardware drivers are 64-bit only. Older client versions include 32-bit libraries and binaries.

**NOTE** Luna HSM Client 10.1 and newer includes libraries for 64-bit operating systems only.

For compatibility of our HSMs with Windows CAPI we have SafeNet CSP, and for the newer Windows CNG we have SafeNet KSP. See "[SafeNet CSP and KSP](#)" on page 33 for more information.

Interactive (prompted, this page) and non-interactive (no prompts "[Scripted/Unattended Windows Installation/Uninstallation](#)" on page 38) installation options are available.

### To install the Luna HSM Client software

1. Log into Windows as "Administrator", or as a user with administrator privileges (see "[Troubleshooting](#)" on page 37).
2. Uninstall any previous versions of the Client software before you proceed (see "[Uninstalling the Luna HSM Client Software](#)" on page 35).

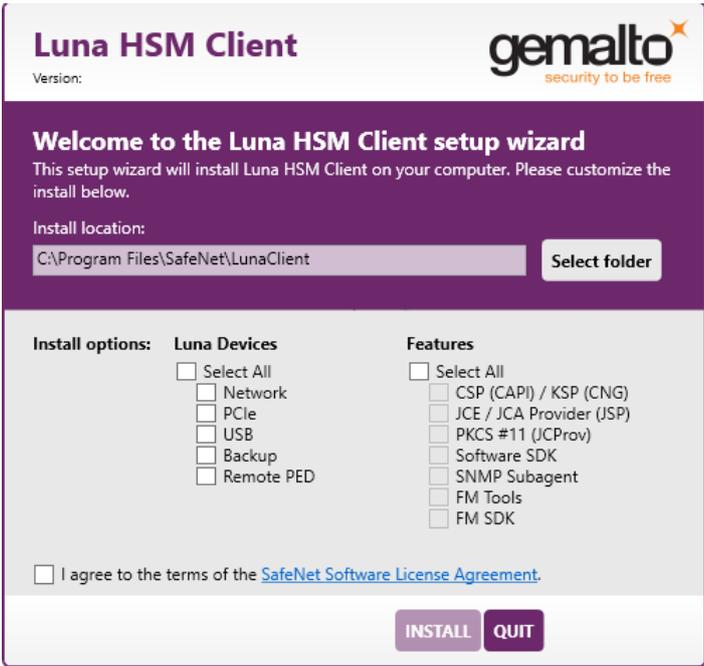
**NOTE** If you do not uninstall previous Luna HSM Client versions, you might face installation issues, such as failure to install the new client.

3. Download the Luna HSM Client from the Thales Group Support Portal at <https://supportportal.thalesgroup.com> and extract the .zip to an appropriate folder.
4. In the extracted directory, locate the folder for your Windows architecture and double click **LunaHSMClient.exe**.



5. The Custom Setup dialog allows you to choose which software components you wish to install. Click a product to select the components to install, or click Select All to install all available components.

The installer includes the SafeNet SNMP Subagent as an option with any of the SafeNet Luna HSMs, except SafeNet Luna Network HSM, which has agent and subagent built in. After installation of the SafeNet SNMP Subagent is complete, you will need to move the SafeNet MIB files to the appropriate directory for your SNMP application, and you will need to start the SafeNet subagent and configure for use with your agent, as described in "[SNMP Monitoring](#)" on page 217.

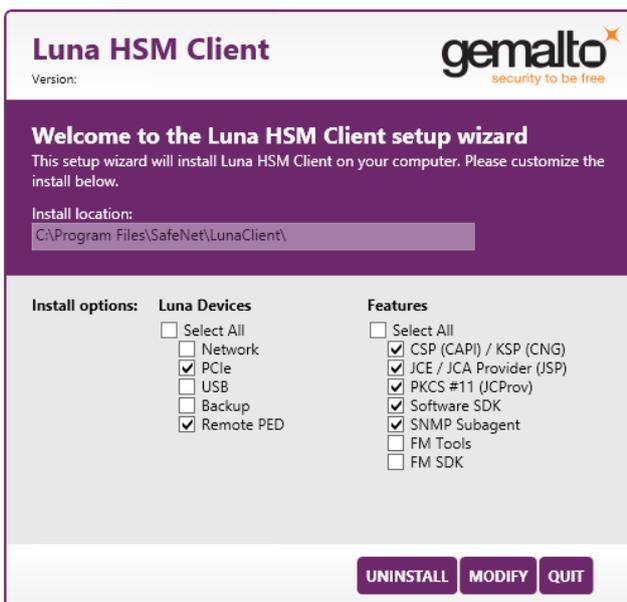


**NOTE Dependencies and considerations when installing:**

- > The FM Tools and FM SDK are useful to you only if you will be using or creating Functionality Modules, to add custom abilities to your HSMs.
- > The FM SDK requires that you install PCIe HSM software and drivers.
- > Similarly, if you are using third-party software to make standard cryptographic calls to the HSM, and are not creating application programs, then you can forego loading the Software Development Kit.
- > There is no harm in installing unneeded components; they do not conflict.
- > The FM SDK option remains gray/unselectable until "Software SDK" is selected, because some of the FM SDK samples have dependencies on General Cryptoki Samples that are part of "Software SDK".

After you select the components you want to install, click **Install**.

- a. Agree to the terms of the License Agreement to proceed with installation. To view the agreement text, click the link in the dialog. The installer loads a PDF version if a PDF reader is available; otherwise it launches a text editor and a plain-text version of the agreement.
  - b. If Windows presents a security notice asking if you wish to install the device driver from SafeNet, click "Always trust software from SafeNet Canada" and click **Install** to accept.
  - c. If you choose not to install the driver(s), your Luna HSM Client cannot function with any locally-connected SafeNet hardware (which includes SafeNet Luna PCIe HSM, SafeNet Luna USB HSM, or SafeNet Luna Backup HSMs).
6. When the installation completes, the button options are Uninstall, Modify, or Quit; click **Quit** to finish.



If you launch the installer again, you should see the final dialog, above, allowing you to modify the current Luna HSM Client installation if desired, or to uninstall.

7. [Optional] For easy use of the Luna HSM Client command-line tools, add the directory to the system PATH variable.

"C:\Program Files\SafeNet\Lunaclient"

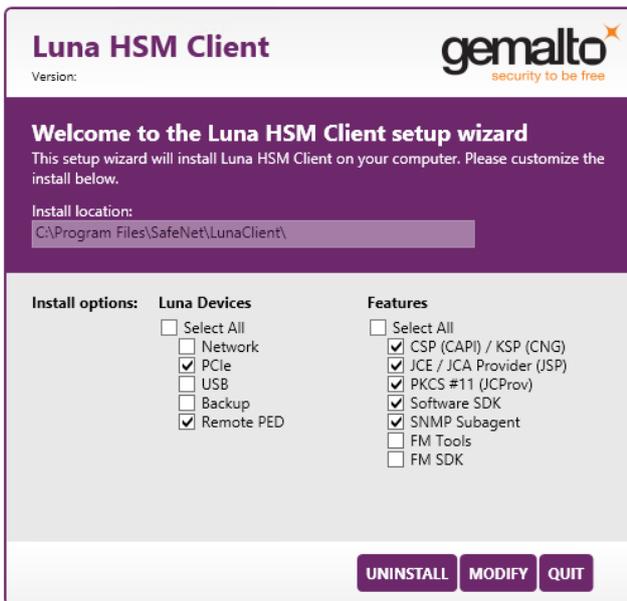
## Modifying the Installed Windows Luna HSM Client Software

If you wish to modify the installation (perhaps to add a component or product that you did not previously install), you must re-run the current installer and ensure that the desired options are selected.

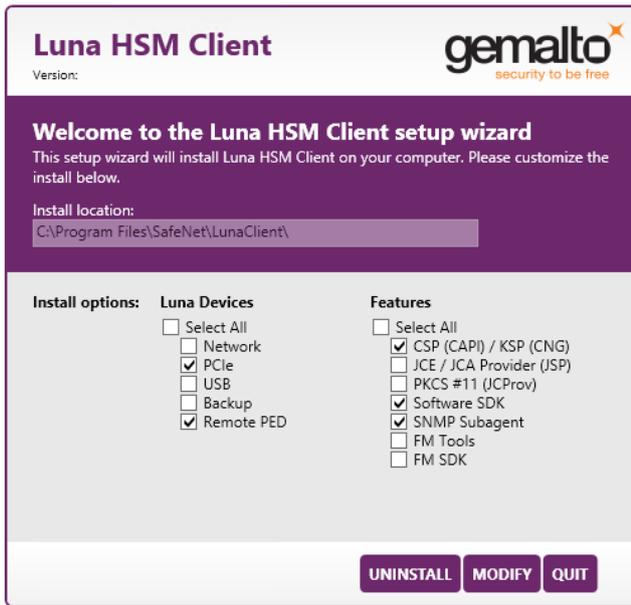
**NOTE** This feature requires minimum client version 7.2. See [Version Dependencies by Feature](#) for more information.

### To modify the installed Luna HSM Client software

1. Run the **LunaHSMClient.exe** program again. Because the software is already installed on your computer, the following dialog is displayed (in this example, devices and features were previously installed, and the task is to uninstall a couple of items):



2. Select or deselect individual Devices or Features, as desired.



3. Click **Modify**. The client software is updated (items are added or removed).

If you are uninstalling some items, or if you are adding features, the dialog shows a progress bar briefly, and then shows the current status.

If you are adding a Luna Device, then you might be prompted with the operating system pop-up to accept/trust the driver. Do so.

4. Click **Quit** when the modification is complete.

**NOTE** You can also use **Programs and Features** in the Windows Control Panel to launch the Uninstall/Modify dialog for the client software.

## Java

If you install the Luna Java Security Provider (JSP), refer to [SafeNet JSP Overview and Installation](#) for additional setup procedures for your operating system.

## SafeNet CSP and KSP

Thales Group provides SafeNet CSP for applications running in older Windows crypto environments running Microsoft Certificate Services (CAPI), and SafeNet KSP for newer Windows clients running Cryptography Next Generation (CNG). Consult Microsoft documentation to determine which one is appropriate for your client operating system.

- > [SafeNet CSP Registration Utilities](#)
- > [SafeNet KSP for CNG Registration Utilities](#)

If the **SafeNet CSP (CAPI) / SafeNet KSP(CNG)** option is selected at installation time, the **SafeNetKSP.dll** file is installed in **C:\Windows\System32** (used for 64-bit KSP). If you are installing a Luna HSM Client version older than 10.1, **SafeNetKSP.dll** is also installed in **C:\Windows\SysWOW64** (used for 32-bit KSP).

**NOTE** The **cryptoki.ini** file, which specifies many configuration settings for your HSM and related software, includes a line that specifies the path to the appropriate libNT for use with your application(s). Verify that the path is correct.

## USB-powered PED

The SafeNet Luna PIN Entry Device (PED) v2.8 contains new hardware that enables the PED to be USB-powered; there is no longer a requirement for an external DC power Adapter. PED v2.8 is functionally equivalent to your existing (previous-generation) PEDs and is compatible with HSM versions, 5.x, 6.x, and 7.x.

PED v2.8 ships with firmware 2.8.0. Note that you cannot upgrade existing PEDs to the 2.8.0 version; existing PEDs continue to need a separate DC power adapter for remote PED and upgrade use. The model number on the manufacturer's label identifies the refreshed PED: PED-06-0001. An installed driver is required; see step 1, below.

### To use the new USB-powered PED

1. Ensure the Luna HSM Client software is installed on the Windows computer that will act as the PED Server to your SafeNet Luna HSM. Installing the Remote PED component of the Luna HSM Client installs the required driver.

**NOTE** A USB connection, without the driver software, only illuminates the PED screen, with no menu. An installed and running PED driver, on the connected computer, is required for the PED to fully boot and to display its menu.

2. Connect the PED to the computer where you installed the Remote PED component of the Luna HSM Client, using the USB micro connector on the PED and a USB socket on your computer.
3. After you connect the PED to the host computer, it will take 30 to 60 seconds for initial boot-up, during which time a series of messages are displayed, as listed below:

**BOOT V.1.1.0-1**

**CORE V.3.0.0-1**

**Loading PED...**

**Entering...**

4. After the boot process is complete, the PED displays **Local PED mode** and the **Awaiting command...** prompt. Your new PED is now ready for use.
5. To enter Remote PED mode, if needed, exit Local PED mode with the "<" key, and from the **Select Mode** menu, select option **7 Remote PED**.

## Modifying the Number of SafeNet Luna Backup HSM Slots

By default, the Luna HSM Client allows for three slots reserved for each model of SafeNet Luna Backup HSM. You can edit **cryptoki.ini** to modify the number of reserved slots. See also "[Configuration File Summary](#)" on [page 66](#).

## To modify the number of reserved Backup HSM slots

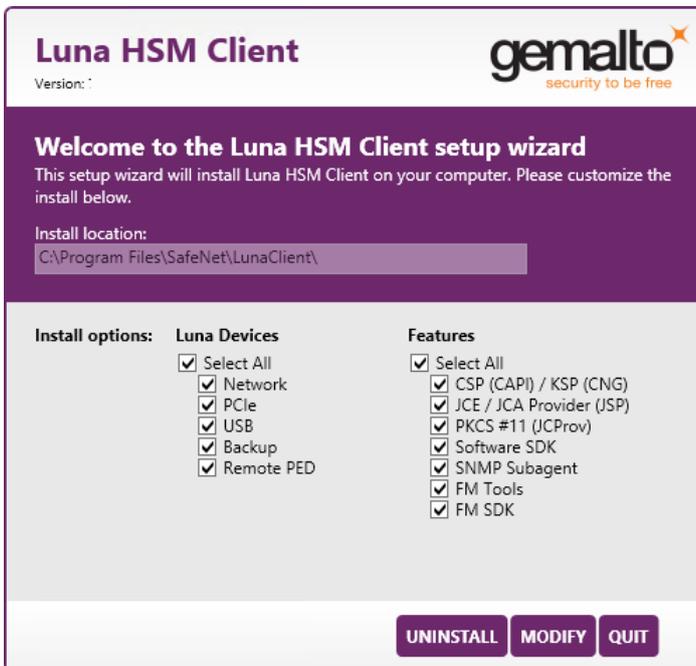
1. Navigate to the **crystoki.ini** file and open in a text editor.
2. Add the following line(s) to the **CardReader** section of the file:
  - For SafeNet Luna G5 Backup HSM:  
**LunaG5Slots = <value>;**
  - For SafeNet Luna G7 Backup HSM (B700/B750):  
**LunaG7Slots = <value>;**

## Uninstalling the Luna HSM Client Software

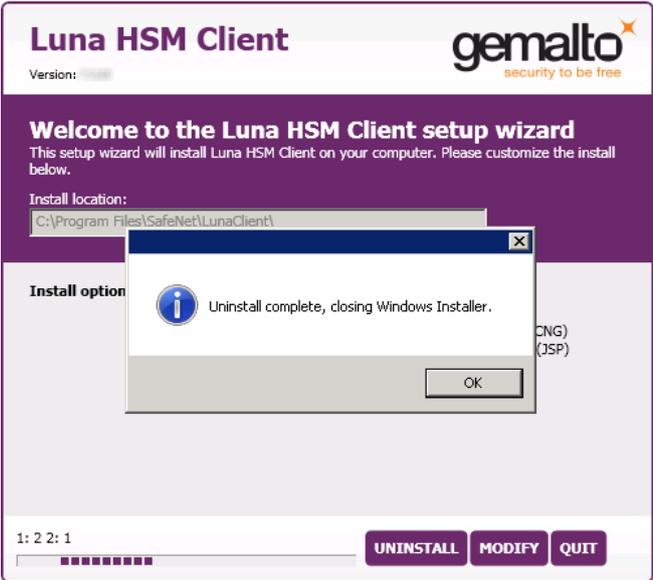
You need to uninstall Luna HSM Client before installing a new version. If you wish to modify the installation (perhaps to add a component or product that you did not previously install), you must uninstall the current installation and re-install with the desired options. If you have a SafeNet Luna Backup HSM connected to the client workstation, either disconnect it or stop the PEDclient service ("[pedclient mode stop](#)" on page 153) before you proceed.

## To uninstall the Luna HSM Client software

1. Run the **LunaHSMClient.exe** program again. Because the software is already installed on your computer, the following dialog is displayed, showing which components are currently installed (for this example, all Devices and all Features were previously installed):



2. Click **Uninstall**. The client software is uninstalled.

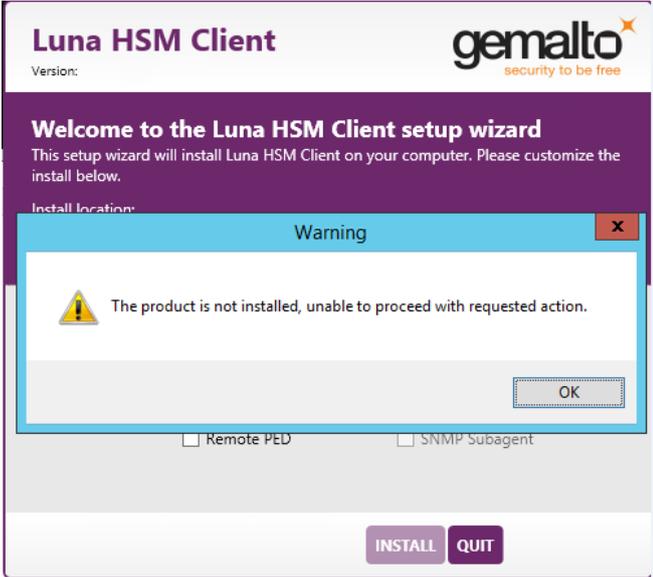


3. When the uninstallation is complete, click **OK** to dismiss the operating system's confirmation dialog.

**NOTE** You can also use **Programs and Features** in the Windows Control Panel to uninstall the client software.

**Uninstall if not present**

If the Luna HSM Client software has been uninstalled, and you launch the installer in uninstall mode, from the command line, the installer starts, looks for the installed software, fails to find it, and presents a Windows dialog to that effect.



If the Luna HSM Client software has been uninstalled, nothing related to the client appears in Windows Control Panel, so nothing exists to launch from that avenue.

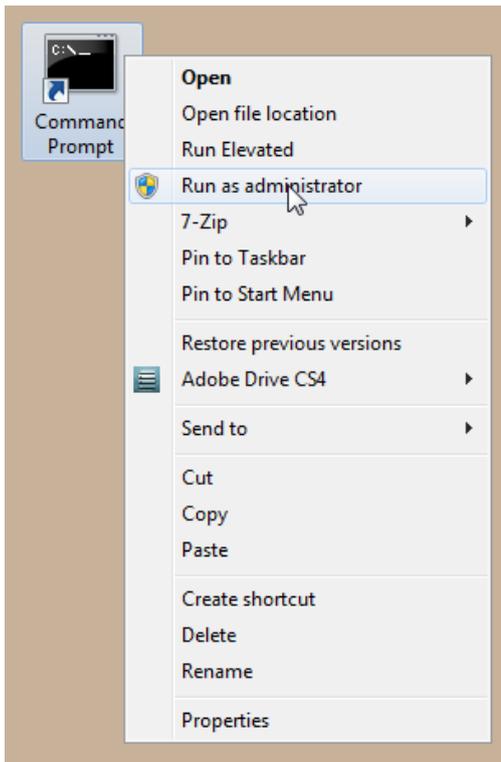
## After Installation

Open a new command-line/console window to allow the library path to be found before you run LunaCM or other utilities that require the library.

## Troubleshooting

If you are not the Administrator of the computer on which Luna HSM Client is being installed, or if the bundle of permissions in your user profile does not allow you to launch the installer with "Run as Administrator", then some services might not install properly. One option is to have the Administrator perform the installation for you.

Another approach might be possible. If you have sufficient elevated permissions, you might be able to right-click and open a Command Prompt window as Administrator.



If that option is available, then you can use the command line to move to the location of the **LunaHSMClient.exe** file and launch it there, which permits the needed services to load for PEDclient. See ["Scripted/Unattended Windows Installation/Uninstallation" on the next page](#) for instructions on how to install the client software from the command line.

## Scripted/Unattended Windows Installation/Uninstallation

This section describes how to perform unattended or scripted installations on Windows platforms. The following procedures are described:

- > ["Command line options overview" below](#)
- > ["Installing the Luna HSM Client for the SafeNet Luna Network HSM" on page 41](#)
- > ["Installing the Luna HSM Client for the SafeNet Luna PCIe HSM" on page 41](#)
- > ["Installing the Luna HSM Client for the SafeNet Luna USB HSM" on page 41](#)
- > ["Installing the Luna HSM Client for the SafeNet Luna Backup HSM" on page 42](#)
- > ["Installing the Luna HSM Client for Remote PED" on page 42](#)
- > ["Installation Location " on page 42](#)
- > ["Logging" on page 43](#)
- > ["Uninstalling the Luna HSM Client" on page 43](#)

If you want to perform an interactive installation, using the graphical, interactive installer, see ["Windows Luna HSM Client Installation" on page 28](#)

**NOTE** Unattended installation stores the root certificate in the certificate store and marks the publisher (in this case, SafeNet, Inc.) as trusted for future installations. You are not prompted to trust SafeNet Inc. as a driver publisher during unattended installation.

### Command line options overview

The following command-line options are available:

Option	Values	Description
addlocal=	Various (see below)	Takes one-or-more device values, and one-or-more feature values, as a comma-separated list. Case insensitive. Values may be quoted or not.
installdir=	A fully qualified folder path to install the client software	Case insensitive. Default value is "c:\program files\safenet\lunaclient". Enclose paths containing spaces in "".
/install	N/A	Install the product and features.
/uninstall	N/A	Remove the product and features.
/quiet	N/A	Performs a silent installation; no prompts or messages. (See Note below this table)
/norestart	N/A	Prevents a reboot, post-installation. Any reboots must be performed manually.

Option	Values	Description
/log	The name of a log file	Generates a highly detailed series of logs of the installation progress. This is required only for product support.

**NOTE** Windows defaults to launching the interactive graphical installer, unless you specify **/quiet** at the command line. Always include the **/quiet** option for scripted/unattended Luna HSM Client installation.

The following devices or components are available for use with the `addlocal=` option:

Device identifier value	Can be used with these installable features
NETWORK	CSP_KSP, JSP, SDK, JCProv (*)
PCI	CSP_KSP, JSP, SDK, JCProv, SNMP
USB	CSP_KSP, JSP, SDK, JCProv, SNMP
BACKUP	SNMP (this device performs backup and restore operations and is not enabled for cryptographic applications)
PED	N/A (Used for remotely authenticating to PED-authenticated HSMs; not used by cryptographic applications - use of this device requires hands-on presence)

The device names are not case-sensitive.

(\* The Network HSM appliance contains its own SNMP support; therefore the SNMP feature is not installed on clients where the Network HSM is the only HSM to be used.)

The following features are available for use with the `addlocal=` option :

Feature identifier value	Can be installed with these Luna devices	Description
CSP_KSP	NETWORK, PCI, USB	Microsoft CSP and KSP
FMSDK	NETWORK, PCIe *	Functionality Modules Software Development Kit
FMTTOOLS	NETWORK, PCIe *	Tools for use when preparing Functionality Modules
JCProv	NETWORK, PCIe, USB	JC PROV PKCS#11
JSP	NETWORK, PCIe, USB	Java Provider component
SDK	NETWORK, PCIe, USB	Software SDK – Java / C++ samples
SNMP	PCIe, USB, Backup	SNMP subagent

The features can be installed together with the listed device(s) only - they cannot be installed separately - and need to be included only once in the command line. For example, if you are installing the NETWORK and PCI devices and you wish to install the CSP / KSP feature, specify CSP\_KSP one time. The feature names are not case-sensitive.

**NOTE** \* If you install FMTOOLS for NETWORK only, then just **mkfm** and the **library** are installed.

If you install FMTOOLS for PCI, then **mkfm** and the **library** along with **ctfm** and **fmrecover** are installed.

If you install FMTOOLS for both NETWORK and PCIe devices, then all four elements are installed.

If you install the FM SDK, the Luna SDK is installed as well, to satisfy dependencies.

Options for **addlocal=** are separated by spaces. Device and feature values are separated by commas, with no spaces, unless the whole list is enclosed between quotation marks. If a space is encountered, outside of paired quotation marks, the next item found is treated as a command option.

## Installing all components and features

Subsequent sections detail how to install the Luna HSM Client software, drivers (if necessary), and optional features (like Java support and the SDK), for individual HSMs. This section describes how to install everything at once, so that all SafeNet Luna HSMs and Remote PED are supported and all the optional features are available.

Use the **ADDLOCAL=** option together with the value **all** to install the base client software and the drivers for all SafeNet Luna devices, along with all the features.

### To install the Luna HSM Client software and drivers for *all* SafeNet Luna devices and *all* features

From the location of **LunaHSMClient.exe** run the following command:

- > Install the full Luna HSM Client software with drivers for all SafeNet Luna HSMs (Network HSM (no driver), PCIe HSM, Backup HSM, Remote PED), as well as all the features (CSP/KSP, JSP, JCProv, C++ SDK, SNMP Subagent)

**LunaHSMClient.exe /install /quiet ADDLOCAL=all**

**NOTE** You can omit the **/quiet** option to see all options in the GUI dialog.

- > [Optional logging] Install the full Luna HSM Client software with drivers for all SafeNet Luna HSMs (Network HSM (no driver), PCIe HSM, Backup HSM, Remote PED), as well as all the features (CSP/KSP, JSP, JCProv, C++ SDK, SNMP Subagent), and log the process.

**LunaHSMClient.exe /install /log install.log /quiet ADDLOCAL=all**

**NOTE** The setting **/log** is optional and saves the installation logs to the file named **install.log** in the example. The **install.log** file (whatever name you give it) is required only if troubleshooting an issue with Technical Support.

## Installing the Luna HSM Client for the SafeNet Luna Network HSM

Use the **ADDLOCAL=NETWORK** option to install the base client software for the SafeNet Luna Network HSM. Include the values for any optional, individual software components you desire. The base software must be installed first.

### To install the Luna HSM Client for the SafeNet Luna Network HSM

From the location of **LunaHSMClient.exe** run one of the following commands:

- > Install the base Luna HSM Client software necessary to communicate with SafeNet Luna Network HSM  
**LunaHSMClient.exe /install /quiet ADDLOCAL=NETWORK**
- > [Optional] Install the base Luna HSM Client software and any of the optional components for the SafeNet Luna Network HSM that you desire:

For example, the following command installs the base software and all of the optional components:

**LunaHSMClient.exe /install /quiet ADDLOCAL=NETWORK,CSP\_KSP,JSP,SDK,JCProv**

If you wish to install only some of the components, just specify the ones you want after the product name (NETWORK in this example).

## Installing the Luna HSM Client for the SafeNet Luna PCIe HSM

Use the **ADDLOCAL=PCI** option to install the base client software for the SafeNet Luna PCIe HSM. Include any features you desire. The base software must be installed first.

### To install the Luna HSM Client for the SafeNet Luna PCIe HSM

From the location of **LunaHSMClient.exe** run one of the following commands:

- > Install the base Luna HSM Client software for SafeNet Luna PCIe HSM  
**LunaHSMClient.exe /install /quiet ADDLOCAL=PCI**
- > Install the base Luna HSM Client software and any of the optional features for the SafeNet Luna PCIe HSM that you desire:

For example, the following command installs the base software and all of the optional components:

**LunaHSMClient.exe /install /quiet ADDLOCAL=PCI,CSP\_KSP,JSP,SDK,JCProv,SNMP**

If you wish to install only some of the components, just specify the ones you want after the product name (PCI in this example).

## Installing the Luna HSM Client for the SafeNet Luna USB HSM

Use the **ADDLOCAL=USB** option to install the base client software for the SafeNet Luna USB HSM. Include any features you desire. The base software must be installed first.

### To install the Luna HSM Client for the SafeNet Luna USB HSM

From the location of **LunaHSMClient.exe** run one of the following commands:

- > Install for SafeNet Luna USB HSM  
**LunaHSMClient.exe /install /quiet ADDLOCAL=USB**

- > Install the base Luna HSM Client software and any of the optional features for the SafeNet Luna USB HSM that you desire:

For example, the following command installs the base software and all of the optional components:

**LunaHSMClient.exe /install /quiet ADDLOCAL=USB,CSP\_KSP,JSP,SDK,JCProv,SNMP**

If you wish to install only some of the components, just specify the ones you want after the product name (USB in this example).

## Installing the Luna HSM Client for the SafeNet Luna Backup HSM

Use the **ADDLOCAL=BACKUP** option to install the base client software for the SafeNet Luna Backup HSM, and the optional feature, if desired. For the Backup HSM, which performs backup and restore operations and is not enabled for use with cryptographic applications, the feature you might add is SNMP, if applicable in your environment.

### To install the Luna HSM Client for the SafeNet Luna Backup HSM

From the location of **LunaHSMClient.exe** run one of the following commands:

- > Install the base Luna HSM Client software for SafeNet Luna Backup HSM

**LunaHSMClient.exe /install /quiet /norestart ADDLOCAL=BACKUP**

- > Install the base Luna HSM Client software and an optional component for the SafeNet Luna Backup HSM:

For example, the following command installs the base software and the optional component:

**LunaHSMClient.exe /install /quiet /norestart ADDLOCAL=backup,snmp**

## Installing the Luna HSM Client for Remote PED

Use the **ADDLOCAL=** option with component value **PED** to install the client software for the SafeNet Luna Backup HSM.

### To install the Luna HSM Client for the SafeNet Luna Backup HSM

- > From the location of **LunaHSMClient.exe** run the following command:

**LunaHSMClient.exe /install /quiet addlocal=ped**

## Installation Location

Specify the installation location, if the default location is not suitable for your situation.

This applies to installation of any Luna Device. Provide the **INSTALLDIR=** option, along with a fully qualified path to the desired target location. For example:

**LunaHSMClient.exe /install /quiet addlocal=all installdir=c:\lunaclient**

That command silently installs all of the SafeNet Luna device software and features to the folder `c:\lunaclient` (in this example). The software is installed into the same subdirectories per component and feature, under that named folder, as would be the case if **INSTALLDIR** was not provided. That is, **INSTALLDIR** changes the prefix or primary client installation folder to the one you specify, and the libraries, devices, tools, certificate folders, etc. are installed in their predetermined relationship, but under the new main folder location.

## Logging

If problems are encountered during installation or uninstallation of the software and you wish to determine the reason, or if Thales Group Technical Support has requested you to do so, detailed logs can be generated and captured by specifying the `/log` option and providing a filename to capture the log output. Two logs are generated – one according to the name given and the other similarly named, with a number appended. Both log files must be sent to Thales Group support if assistance is required.

Example commands that include logging are:

```
LunaHSMClient.exe /install /quiet /log install.log /norestart ADDLOCAL=backup,snmp
```

```
LunaHSMClient.exe /uninstall /quiet /log uninstall.log
```

## Uninstalling the Luna HSM Client

You can also perform scripted/unattended uninstallation.

### To uninstall the Luna HSM Client

> From the location of **LunaHSMClient.exe** run the following command:

```
LunaHSMClient.exe /uninstall /quiet
```

> To log the uninstallation process, run the following command:

```
LunaHSMClient.exe /uninstall /quiet /log uninstall.log
```

---

# Linux Luna HSM Client Installation

---

## Installing the Luna HSM Client

---

You must install the Luna HSM Client software on each client workstation you will use to access a SafeNet Luna HSM. This section describes how to install the client on a workstation running Linux, and contains the following topics:

- > ["Prerequisites" below](#)
- > ["Installing the Client Software" on the next page](#)
- > ["Controlling User Access to Your Attached HSMs and Partitions" on page 48](#)
- > ["Uninstalling the Client Software or Removing Components" on page 49](#)
- > ["Java" on page 50](#)
- > ["Scripted or Unattended Installation" on page 50](#)
- > ["Interrupting the Installation" on page 51](#)
- > ["Modifying the Number of SafeNet Luna Backup HSM Slots" on page 51](#)

Refer to the Customer Release Notes for a complete list of the supported Linux operating systems. These instructions assume that you have already acquired the Luna HSM Client software.

### Prerequisites

Before starting the installation, ensure that you have satisfied the following prerequisites:

#### **Components Required to Build the PCIe Driver and the Backup HSM Driver**

On Linux, the PCIe driver module (and optionally the Backup HSM driver) is built by the client as part of the installation if you choose to install the Luna PCIe HSM component or the Backup HSM. To build the driver, the client requires the following items:

- > Kernel headers for build
- > kernel-devel package
- > rpmbuild package
- > C and C++ compilers
- > make command

If any one of these items is missing, the driver build will fail and the client software will not be installed.

**NOTE** The installed *kernel* and *kernel-devel* versions on the Client system must match, in order for the drivers to compile successfully. In general, if the versions do not match, or if you are not sure, use this command **yum install kernel-devel-`uname -r`** before installing Luna HSM Client. Note the required backticks, (the key to the left of the 1/! key on the keyboard) surrounding **`uname -r`** (or equivalent command **yum install kernel-devel-\$(uname -r)**). To check installed versions related to the currently running kernel: **rpm -qa kernel \* | grep \$(uname -r)**.

### Debian Requires alien

The Luna HSM Client software is provided as RPM packages. If you are installing on a Debian system, you must have **alien** installed to allow the Luna HSM Client installation script to convert the RPM packages to DEB packages. The installation script will stop with a message if you attempt to install on a Debian system without **alien** installed. This applies to any other supported Debian-based Linux distribution, such as Ubuntu.

### SUSE Linux on IBM PPC

JCE un-restriction files must be downloaded from IBM, not from SUN, for this platform. Attempting to use SUN JCE un-restriction files on IBM PowerPC systems with SUSE Linux causes signing errors.

## Installing the Client Software

It is recommended that you refer to the SafeNet Luna HSM Customer Release Notes for any installation-related issues or instructions before installing the client software.

**CAUTION!** You must install the client software using root-level privileges. For security reasons, we recommend that you do not log in as root (or use `su root`) to run the installation script, but instead use the `sudo` command to run the installation script, as detailed below.

### The installation script

The installation script is **install.sh** and is usually launched with **sh install.sh** followed by any options or parameters.

- > interactive: **sh install.sh [-install\_directory <prefix>]**
- > all: **sh install.sh all [-install\_directory <prefix>]**
- > scriptable: **sh install.sh -p [network|pci|usb|backup|ped] [-c sdk|jsp|jcpov|ldpc|snmp] [-install\_directory <prefix>]**

The options on the script are:

- > device(s)
  - "network" is the SafeNet Luna Network HSM (software only, no drivers)
  - "pci" is the SafeNet Luna PCIe HSM (software plus driver for the PCI HSM)
  - "usb" is the SafeNet Luna USB and Backup HSMs (software plus driver for the G5-based and G7-based HSMs)
  - "backup" is software to enable Remote Backup
  - "ped" is software for the SafeNet Luna Remote PED

- > components include the optional Software Development kit, Java providers, SNMP instance (not needed for Network HSM which has it built in)

By default, the Client programs are installed in the **/usr/safenet/lunaclient** directory.

### Flexible Install paths

You can change the installation path for scriptable (non-interactive) installs by changing the prefix with the script option **-install\_directory** <prefix>

The prefix, or major location is your choice, and replaces the /usr default portion.

#### NOTE

Avoid the use of space characters in directory names.

The script option **-install\_directory** <prefix> is available for scriptable installation, where either "all" or a list of products and components is specified on the command line. The script option **-install\_directory** <prefix> is not used with interactive installation; instead, you are prompted.

The **/safenet/lunaclient** portion is appended by the install script, and provides a predictable structure for additional subdirectories to contain certificate files, and optionally STC files.

Regardless of **-install\_directory** <prefix> provided, some files are not affected by that option (for example, the Chrystoki.conf configuration file goes under /etc, service files need to be in the service directory expected by Linux in order to run at boot time, and so on).

### To install the Luna HSM Client software on a Linux workstation

1. Ensure that you have **sudo** privileges on the client workstation.
2. Access the installation software:
 

Copy or move the **.tar** archive to a suitable directory where you can untar the archive and extract the contents:

```
tar xvf <filename>.tar
```
3. Go to the untarred directory for your operating system (**32** or **64**-bit):
 

```
cd /<untarred_dir>/<32/64>
```
4. To install the software, run the **install.sh** installation script. You can run the script in interactive mode, or you can script the installation, as described in "[Scripted or Unattended Installation](#)" on page 50.
  - To display the help, or a list of available installer options, type:
 

```
sudo sh install.sh -? or sudo sh install.sh help
```
  - To install all available products and optional components, type:
 

```
sudo sh install.sh all
```
  - To selectively install individual products and optional components, type the command without arguments:
 

```
sudo sh install.sh
```

**NOTE** Do not interrupt the installation script in progress. An uninterruptible power supply (UPS) is recommended. See ["Interrupting the Installation" on page 51](#) for more information.

5. Type **y** if you agree to be bound by the license agreement. You must accept the license agreement before you can install the software.
6. A list of installable SafeNet devices is displayed. Select as many as you require, by typing the number of each (in any order) and pressing **Enter**. As each item is selected, the list updates, with a \* in front of any item that has been selected.

This example shows items 1 and 3 have been selected, and item 4 is about to be selected. The selections work as a toggle - if you wish to make a change, simply type a number again and press **Enter** to de-select it.

Products

Choose Luna Products to be installed

\*[1]: Luna Network HSM

[2]: Luna PCIe HSM

\*[3]: Luna USB HSM

[4]: Luna Backup HSM

[5]: Luna Remote PED

[N|n]: Next

[Q|q]: Quit

Enter selection: 4

When selection is complete, type **N** or **n** for "Next", and press **Enter**. The "Advanced" menu is displayed.

Advanced

Choose Luna Components to be installed

[1]: Luna SDK

[2]: Luna JSP (Java)

[3]: Luna JProv (Java)

[4]: Luna SNMP subagent

[5]: Luna Functionality Module Tools

[6]: Luna Functionality Module Software Development Kit

[B|b]: Back to Products selection

[I|i]: Install

[Q|q]: Quit

Enter selection:

7. Select or de-select any additional items you want to install. Selected items are indicated with a \*. Some items might be pre-selected to provide the optimum experience for the majority of customers, but you can change any selection in the list. When the Components list is adjusted to your satisfaction, press **Enter**.

**NOTE** The installer includes the Luna SNMP Subagent as an option. If you select this option, you will need to move the SafeNet MIB files to the appropriate directory for your SNMP application after installation is complete, and you will need to start the SafeNet subagent and configure it for use with your agent.

**Luna SDK required with FMs** - If you choose the Functionality Module (FM) options, the interactive `install.sh` script populates the Luna SDK as well, because of dependencies in the FM samples. If you run the installer with command-line options (non-interactive), and you choose FM items without also choosing Luna SDK, the script just gives a warning and stops. ELDK (the Embedded Linux Development Kit) is installed with FMs - The ELDK package is installed as part of the FM SDK component, for Linux, and must reside at `/opt/eldk-5.6`. It is not relocatable.

If the script detects an existing cryptoki library, it stops and suggests that you uninstall your previous SafeNet software before starting the Luna HSM Client installation again.

8. The system installs all packages related to the products and any optional components that you selected.
9. [Optional] For easy use of the Luna HSM Client tools, add their directories to the `$PATH`.
- a. Edit your system's **bash\_profile** file using an editing tool.  
`vi ~/.bash_profile`
  - b. Add the following lines to the end of the file:  
`export PATH="$PATH:/usr/safenet/lunaclient/bin"`  
`export PATH="$PATH:/usr/safenet/lunaclient/sbin"`
  - c. Source the updated **bash\_profile**.  
`source ~/.bash_profile`

## Controlling User Access to Your Attached HSMs and Partitions

By default, only the root user has access to your attached HSMs and partitions. You can specify a set of non-root users that are permitted to access your attached HSMs and partitions, by adding them to the **hsmusers** group.

**NOTE** The client software installation automatically creates the `hsmusers` group if one does not already exist on your system. The `hsmusers` group is retained when you uninstall the client software, allowing you to upgrade your client software while retaining your `hsmusers` group configuration.

### Adding users to hsmusers group

To allow non-root users or applications access your attached HSMs and partitions, assign the users to the **hsmusers** group. The users you assign to the `hsmusers` group must exist on the client workstation. Users you add to the `hsmusers` group are able to access your attached HSMs and partitions. Users who are not part of

the hsmusers group are not able to access your attached HSMs and partitions.

---

### To add a user to hsmusers group

1. Ensure that you have **sudo** privileges on the client workstation.
2. Add a user to the hsmusers group:

```
sudo gpasswd --add <username> hsmusers
```

where <username> is the name of the user you want to add to the hsmusers group.

### Removing users from hsmusers group

Should you wish to rescind a user's access to your attached HSMs and partitions, you can remove them from the hsmusers group.

**NOTE** The user you delete will continue to have access to the HSM until you reboot the client workstation.

---

### To remove a user from hsmusers group

1. Ensure that you have **sudo** privileges on the client workstation.
2. Remove a user from the hsmusers group:

```
sudo gpasswd -d <username> hsmusers
```

where <username> is the name of the user you want to remove from the hsmusers group. You must log in again to see the change.

## Uninstalling the Client Software or Removing Components

You may need to uninstall the client software before upgrading to a new version, or if it is no longer required.

---

### To uninstall the client software

1. Ensure that you have **sudo** privileges on the client workstation.
2. Go to the client installation directory:

```
cd /usr/safenet/lunaclient/bin
```

3. Run the uninstall script:

```
sudo sh uninstall.sh
```

**CAUTION!** The hsmusers group is not removed when the client software is uninstalled. Should you install the client again on the same system, all users previously in the group will have access to your attached HSMs and partitions by default. You must remove users from the group if you want to restrict their access. See ["Removing users from hsmusers group" above](#).

## To remove individual components

To uninstall the JSP component or the SDK component, you must uninstall Luna HSM Client completely, then re-run the installation script without selecting the unwanted component(s).

## Java

If you install the Luna Java Security Provider (JSP), refer to [SafeNet JSP Overview and Installation](#) for additional setup procedures for your operating system.

## Scripted or Unattended Installation

If you prefer to run the installation from a script, rather than interactively, run the command with the options **-p** <list of SafeNet products> and **-c** <list of SafeNet components>. To see the syntax, run the command with **help** like this:

```
[myhost]$ sudo sh install.sh help
[sudo] password for fred
```

At least one product should be specified.

usage:

```
install.sh      - Luna Client install through menu
install.sh help - Display scriptable install options
install.sh all  - Complete Luna Client install

install.sh -p [network|pci|usb|backup|ped] [-c sdk|jsp|jcprov|ldpc|snmp]

-p <list of Luna products>
-c <list of Luna components> - Optional. All components are installed if not provided
```

Luna products options

```
network - Luna Network HSM
pci      - Luna PCIe HSM
usb      - Luna USB HSM
backup   - Luna Backup HSM
ped      - Luna Remote PED
```

Luna components options

```
sdk      - Luna SDK
jsp      - Luna JSP (Java)
jcprov   - Luna JCPROV (Java)
snmp     - Luna SNMP subagent
```

```
[myhost]$
```

For scripted/automated installation, your script will need to capture and respond to the License Agreement prompt, and to the confirmation prompt. For example:

```
[myhost]$ sudo sh install.sh all
```

**IMPORTANT:** The terms and conditions of use outlined in the software license agreement (Document #008-010005-001\_053110) shipped with the product ("License") constitute a legal agreement between you and SafeNet Inc. Please read the License contained in the packaging of this product in its entirety before installing this product.

Do you agree to the License contained in the product packaging?

If you select 'yes' or 'y' you agree to be bound by all the terms and conditions set out in the License.

If you select 'no' or 'n', this product will not be installed.

(y/n) **y**

Complete Luna Client will be installed. This includes SafeNet Luna Network HSM, SafeNet Luna PCIe HSM, SafeNet Luna USB HSM, SafeNet Luna Backup HSM and SafeNet Luna Remote PED.

Select 'yes' or 'y' to proceed with the install.

Select 'no' or 'n', to cancel this install.

Continue (y/n)? **y**

## Interrupting the Installation

Do not interrupt the installation script in progress, and ensure that your host computer is served by an uninterruptible power supply (UPS). If you press [CTRL] [C], or otherwise interrupt the installation (OS problem, power outage, other), some components will not be installed. It is not possible to resume an interrupted install process. The result of an interruption depends on where, in the process, the interruption occurred (what remained to install before the process was stopped).

As long as the cryptoki RPM package is installed, any subsequent installation attempt results in refusal with the message "A version of Luna HSM Client is already installed."

If components are missing or are not working properly after an interrupted installation, or if you wish to install any additional components at a later date (following an interrupted installation, as described), you would need to uninstall everything first. If **sh uninstall.sh** is unable to do it, then you must uninstall all packages manually.

## Modifying the Number of SafeNet Luna Backup HSM Slots

By default, the Luna HSM Client allows for three slots reserved for each model of SafeNet Luna Backup HSM. You can edit **Chrystoki.conf** to modify the number of reserved slots. See also "[Configuration File Summary](#)" on page 66.

### To modify the number of reserved Backup HSM slots

1. Navigate to the **Chrystoki.conf** file and open in a text editor.
2. Add the following line(s) to the **CardReader** section of the file:
  - For SafeNet Luna G5 Backup HSM:  
**LunaG5Slots = <value>;**
  - For SafeNet Luna G7 Backup HSM (B700/B750):  
**LunaG7Slots = <value>;**

## Solaris Luna HSM Client Installation

These instructions assume that you have already acquired the Luna HSM Client software, in the form of a downloaded .tar archive.

You must install the Luna HSM Client software on each client workstation you will use to access a SafeNet Luna HSM. This section describes how to install the client on a workstation running Solaris, and contains the following topics:

- > ["Prerequisites" below](#)
- > ["Installing the Client Software" on the next page](#)
- > ["Controlling User Access to Your Attached HSMs and Partitions" on page 55](#)
- > ["Uninstalling the Luna HSM Client Software" on page 56](#)
- > ["Java" on page 56](#)
- > ["Scripted or Unattended Installation" on page 56](#)
- > ["Interrupting the installation - \[Ctrl\] \[C\]" on page 57](#)

Applicability to specific versions of Solaris is summarized in the Customer Release Notes for the current release.

**NOTE** Before installing a SafeNet system, you should confirm that the product you have received is in factory condition and has not been tampered with in transit. Refer to the Startup Guide included with your product shipment. If you have any questions about the condition of the product that you have received, contact Thales Group Support.

Each computer that connects to the SafeNet Luna Network HSM appliance as a client must have the cryptoki library, the vtl client shell and other utilities and supporting files installed.

Each computer that contains, or is connected to a SafeNet Luna USB HSM or a SafeNet Luna PCIe HSM must have the cryptoki library and other utilities and supporting files installed.

**NOTE** This example shows all the Luna HSM Client products and components. Some items are not supported on all operating systems and therefore do not appear as you proceed through the installation script.

### Prerequisites

Before starting the installation, ensure that you have satisfied the following prerequisites:

#### Random Number Generator (RNG) or Entropy Gathering Daemon (EGD)

Ensure that you have a Random Number Generator (RNG) or Entropy Gathering Daemon (EGD) on your system in one of the following locations:

- > /dev/egd-pool
- > /etc/egd-pool,
- > /etc/entropy

> /var/run/egd-pool

## RNG/EGD

Cryptographic algorithms, including those that assure the security of communication – such as in OpenSSL and other protocols – depend upon random numbers for the creation of strong keys and certificates. A readily available source of random data is the entropy that exists in complex computer processes. Utilities exist for every operating system, to gather bits of system entropy into a pool, which can then be used by other processes.

Windows and Linux have these installed by default. Other systems might not. See your system administrator.

## Entropy Pool

In the case of SafeNet Luna Network HSM, the Luna HSM Client administration tool (**vtl**) expects to find a source of randomness at **/dev/random**. If one is not found, **vtl** fails, because the link cannot be secured from the Client end.

If your system does have an entropy pool, but the random number generator (RNG) is not in the expected place, then you can create a symbolic link between the actual location and one of the following:

- > /dev/random
- > /dev/egd-pool
- > /etc/egd-pool
- > /etc/entropy
- > /var/run/egd-pool

If your system does not have an entropy-gathering daemon or random number generator, please direct your system administrator to install one, and point it to one of the named devices.

## Installing the Client Software

It is recommended that you refer to the SafeNet Luna HSM Customer Release Notes for any installation-related issues or instructions before you begin the following software installation process.

**CAUTION!** You must be logged in as **root** when you run the installation script.

By default, the Client programs are installed in the **/opt/safenet/lunaclient/bin** directory.

### To install the Luna HSM Client software on a Solaris workstation

1. Log on to the client system, open a console or terminal window, and use **su** to gain administrative permissions for the installation.
2. Access the Luna HSM Client software:
  - a. Copy or move the **.tar** archive to a suitable directory where you can untar the archive and launch the installation script.
  - b. Extract the contents from the archive:
 

```
tar xvf <filename>.tar
```
3. Go to the install directory for your architecture:

**NOTE** Luna HSM Client 10.1 and newer includes libraries for 64-bit operating systems only.

Architecture	Path
Solaris Sparc 32-bit	LunaClient_7.X.0_SolarisXXSparc/32
Solaris Sparc 64-bit	LunaClient_7.X.0_SolarisXXSparc/64
Solaris x86 32-bit	LunaClient_7.X.0_SolarisXXx86/32
Solaris x86 64-bit	LunaClient_7.X.0_SolarisXXx86/64

4. To see the help, or a list of available installer options, type:

**sh install.sh -?** or **sh install.sh --help**

To install all available products and optional components, type:

**sh install.sh all**

To selectively install individual products and optional components, type the command without arguments:

**sh install.sh**

5. Type **y** if you agree to be bound by the license agreement.
6. A list of installable SafeNet products is displayed (might be different, depending on your platform). Select as many as you require, by typing the number of each (in any order) and pressing **Enter**. As each item is selected, the list updates, with a "\*" in front of any item that has been selected. The following example shows that items 1 and 3 have been selected, and item 4 is about to be selected.

```
Products
Choose Luna Products to be installed
  * [1]: SafeNet Luna Network HSM
    [2]: SafeNet Luna PCIe HSM
  * [3]: SafeNet Luna USB HSM
    [4]: SafeNet Luna Backup HSM
  [N|n]: Next
  [Q|q]: Quit
Enter selection: 4
```

7. When the selection is complete, type **N** or **n** for "Next", and press **Enter**. If you wish to make a change, simply type a number again and press **Enter** to de-select a single item.
8. The next list is titled "Advanced" and includes additional items to install. Some items might be pre-selected to provide the optimum SafeNet Luna HSM experience for the majority of customers, but you can change any selection in the list. When the Components list is adjusted to your satisfaction, press **Enter**.

**NOTE** The installer includes the SafeNet SNMP Subagent as an option. If you select this option, you will need to move the SafeNet MIB files to the appropriate directory for your SNMP application after installation is complete, and you will need to start the SafeNet subagent and configure for use with your agent.

9. If the script detects an existing cryptoki library, it stops and suggests that you uninstall your previous SafeNet software before starting the Luna HSM Client installation again.
10. The system installs all packages related to the products and any optional components that you selected.
11. Although FMs are supported on Linux and Windows clients only in this release, the FM architecture requires a configuration file setting to allow partition login on an FM-enabled HSM. If the HSM you will be using with this client is FM-enabled (see ["Preparing the SafeNet Luna PCIe HSM to Use FMs" on page 275](#) for more information), you must add the following entry to the [Misc] section of the Chrystoki.conf file:

**[Misc]**

**LoginAllowedOnFMEnabledHSMs=1**

**NOTE** As a general rule, do not modify the Chrystoki.conf/crystoki.ini file, unless directed to do so by Gemalto Technical Support. If you do modify the file, never insert TAB characters - use individual space characters. Avoid modifying the PED timeout settings. These are now hardcoded in the appliance, but the numbers in the Chrystoki.conf file must match.

## Controlling User Access to Your Attached HSMs and Partitions

By default, only the root user has access to your attached HSMs and partitions. You can specify a set of non-root users that are permitted to access your attached HSMs and partitions, by adding them to the **hsmusers** group.

**NOTE** The client software installation automatically creates the **hsmusers** group if one does not already exist on your system. The **hsmusers** group is retained when you uninstall the client software, allowing you to upgrade your client software while retaining your **hsmusers** group configuration.

### Adding users to hsmusers group

To allow non-root users or applications access your attached HSMs and partitions, assign the users to the **hsmusers** group. The users you assign to the **hsmusers** group must exist on the client workstation. Users you add to the **hsmusers** group are able to access your attached HSMs and partitions. Users who are not part of the **hsmusers** group are not able to access your attached HSMs and partitions.

#### To add a user to hsmusers group

1. Ensure that you have **sudo** privileges on the client workstation.
2. Add a user to the **hsmusers** group:

```
sudo gpasswd --add <username> hsmusers
```

where <username> is the name of the user you want to add to the **hsmusers** group.

### Removing users from hsmusers group

Should you wish to rescind a user's access to your attached HSMs and partitions, you can remove them from the **hsmusers** group.

**NOTE** The user you delete will continue to have access to the HSM until you reboot the client workstation.

### To remove a user from hsmusers group

1. Ensure that you have **sudo** privileges on the client workstation.
2. Remove a user from the **hsmusers** group:

```
sudo gpasswd -d <username> hsmusers
```

where <username> is the name of the user you want to remove from the **hsmusers** group. You must log in again to see the change.

## Uninstalling the Luna HSM Client Software

1. **cd /opt/safenet/lunaclient/bin**
2. **sh uninstall.sh**

## Java

If you install the Luna Java Security Provider (JSP), refer to [SafeNet JSP Overview and Installation](#) for additional setup procedures for your operating system.

## Scripted or Unattended Installation

If you prefer to run the installation from a script, rather than interactively, run the command with the options **-p** <list of SafeNet products> and **-c** <list of SafeNet components>. To see the syntax, run the command with **help** like this:

```
[myhost]$ sudo sh install.sh help
[sudo] password for fred
```

At least one product should be specified.

usage:

```
install.sh      - Luna Client install through menu
install.sh help - Display scriptable install options
install.sh all  - Complete Luna Client install
```

```
install.sh -p [sa|pci|g5|rb] [-c sdk|jsp|jcprov|ldpc|snmp]
```

```
-p <list of Luna products>
```

```
-c <list of Luna components> - Optional. All components are installed if not provided
```

Luna products options

```
sa      - SafeNet Luna Network HSM
pci     - SafeNet Luna PCIe HSM
g5      - SafeNet Luna USB HSM
rb      - SafeNet Luna Backup HSM
```

Luna components options

```
sdk     - Luna SDK
jsp     - Luna JSP (Java)
jcprov  - Luna JC PROV (Java)
```

```
snmp - Luna SNMP subagent
```

```
[myhost]$
```

For scripted/automated installation, your script will need to capture and respond to the License Agreement prompt, and to the confirmation prompt. For example:

```
[myhost]$ sudo sh install.sh all
```

```
IMPORTANT: The terms and conditions of use outlined in the software
license agreement (Document #008-010005-001_053110) shipped with the product
("License") constitute a legal agreement between you and SafeNet Inc.
Please read the License contained in the packaging of this
product in its entirety before installing this product.
```

```
Do you agree to the License contained in the product packaging?
```

```
If you select 'yes' or 'y' you agree to be bound by all the terms
and conditions se out in the License.
```

```
If you select 'no' or 'n', this product will not be installed.
```

```
(y/n) y
```

```
Complete Luna Client will be installed. This includes SafeNet Luna Network HSM,
SafeNet Luna PCIe HSM, SafeNet Luna USB HSM AND SafeNet Luna Backup HSM.
```

```
Select 'yes' or 'y' to proceed with the install.
```

```
Select 'no' or 'n', to cancel this install.
```

```
Continue (y/n)? y
```

## Interrupting the installation - [Ctrl] [C]

Do not interrupt the installation script in progress, and ensure that your host computer is served by an uninterruptible power supply (UPS). If you press [Ctrl] [C], or otherwise interrupt the installation (OS problem, power outage, other), some components will not be installed. It is not possible to resume an interrupted install process. The result of an interruption depends on where, in the process, the interruption occurred (what remained to install before the process was stopped).

As long as the cryptoki package is installed, any subsequent installation attempt results in refusal with the message "A version of Luna Client is already installed." Removing the library allows the script to clean up remaining components, so that you can install again.

## What to do if installation is incomplete or damaged

1. If SNFTlibcryptoki has been installed, uninstall it manually.
2. Run the Client install script again. Now that SNFTlibcryptoki is removed, the install script removes any stray packages and files.
3. Install again, to perform a clean installation.

## AIX Luna HSM Client Installation

These instructions assume that you have already acquired the Luna HSM Client software, usually in the form of a downloaded .tar archive.

You must install the Luna HSM Client software on each client workstation you will use to access a SafeNet Luna HSM. This section describes how to install the client on a workstation running AIX, and contains the following topics:

- > ["Prerequisites" below](#)
- > ["Installing the Client Software" below](#)
- > ["Controlling User Access to Your Attached HSMs and Partitions" on page 61](#)
- > ["Uninstalling the Luna HSM Client Software" on page 62](#)
- > ["Installing Java" on page 62](#)
- > ["Scripted or Unattended Installation" on page 62](#)
- > ["Interrupting the Installation" on page 63](#)

Applicability to specific versions of AIX is summarized in the Customer Release Notes for the current release.

**NOTE** Before installing a SafeNet system, you should confirm that the product you have received is in factory condition and has not been tampered with in transit. Refer to the Content Sheet included with your product shipment. If you have any questions about the condition of the product that you have received, please contact Thales Group Technical Support.

### Prerequisites

Each computer that connects to the SafeNet Luna HSM appliance as a Client must have the cryptoki library, the vtl client shell and other utilities and supporting files installed. Each computer that contains, or is connected to a SafeNet Luna PCIe HSM or a SafeNet Luna Remote Backup HSM must have the cryptoki library and other utilities and supporting files installed.

### Installing the Client Software

Check the SafeNet Luna HSM Customer Release Notes for any installation-related issues or instructions before you begin the following software installation process.

#### To install the Luna HSM Client software on AIX:

1. Log on to the client system, open a console or terminal window, and use **su** or **sudo** to gain administrative permissions for the installation.
2. If you downloaded the software, copy or move the .tar archive (which usually has a name like "LunaClient\_7.x.y-nn\_AIX.tar") to a suitable directory where you can untar the archive and launch the installation script.
3. Enter the following command to extract the contents from the archive:  
**tar xvf <filename>.tar**
4. Change directory to the software version suitable for your system.
5. Install the client software as follows:

- To see the 'help', or a list of available installer options, type:  
**sh install.sh -?** or **./sh install.sh --help**
- To install all available products and optional components, type:  
**sh install.sh all**
- To selectively install individual products and optional components, type the command without arguments:  
**sh install.sh**

**NOTE** Do not interrupt the installation script in progress. An uninterruptible power supply (UPS) is recommended. See ["Interrupting the Installation" on page 63](#) for more information.

**6. Type y if you agree to be bound by the license agreement:**

```
[mylunaclient-1 32]$ sh install.sh
```

```
IMPORTANT: The terms and conditions of use outlined in the software
license agreement (Document #008-010005-001_EULA_HSM_SW_revN) shipped with the product
("License") constitute a legal agreement between you and SafeNet.
Please read the License contained in the packaging of this
product in its entirety before installing this product.
```

```
Do you agree to the License contained in the product packaging?
```

```
If you select 'yes' or 'y' you agree to be bound by all the terms
and conditions set out in the License.
```

```
If you select 'no' or 'n', this product will not be installed.
```

```
(y/n)
```

**7. A list of installable SafeNet products appears (might be different, depending on your platform). Select as many as you require, by typing the number of each (in any order) and pressing Enter. As each item is selected, the list updates, with a "\*" in front of any item that has been selected. This example shows item 1 has been selected.**

```
Products
```

```
Choose Luna Products to be installed
```

```
*[1]: Luna Network HSM
[N|n]: Next
[Q|q]: Quit
```

```
Enter selection: 1
```

**NOTE** When the above was captured, the AIX client supported only SafeNet Luna Network HSM. To install the SafeNet Luna Backup HSM, you will need one of the other supported host platforms.

**8. When selection is complete, type N or n for "Next", and press Enter. If you wish to make a change, simply type a number again and press Enter to de-select a single item.**

9. The next list is called "Advanced" and includes additional items to install. Some items might be pre-selected to provide the optimum SafeNet Luna HSM experience for the majority of customers, but you can change any selection in the list.

```
Products
Choose Luna Products to be installed
  [1]: Luna Network HSM
  [N|n]: Next
  [Q|q]: Quit

Enter selection: 1
```

```
Advanced
Choose Luna Components to be installed

  [1]: Luna SDK
* [2]: Luna JSP (Java)
* [3]: Luna JCProv (Java)

  [B|b]: Back to Products selection

  [I|i]: Install

  [Q|q]: Quit

Enter selection:
```

If you wish to make a change, simply type a number again and press **Enter** to select or de-select a single item.

If the script detects an existing cryptoki library, it stops and suggests that you uninstall your previous SafeNet software before starting the Luna HSM Client installation again.

10. The system installs all packages related to the products and any optional components that you selected. By default, the Client programs are installed in the **/usr/safenet/lunaclient** directory.

**NOTE** When installing, ensure that the full path of a package does not contain any space characters. (The IBM examples do not show any spaces, implying that this might be a system requirement.)

11. Although FMs are supported on Linux and Windows clients only in this release, the FM architecture requires a configuration file setting to allow partition login on an FM-enabled HSM. If the HSM you will be using with this client is FM-enabled (see "[Preparing the SafeNet Luna PCIe HSM to Use FMs](#)" on page 275 for more information), you must add the following entry to the [Misc] section of the Chrystoki.conf file:

**[Misc]**

**LoginAllowedOnFMEnabledHSMs=1**

**NOTE** As a general rule, do not modify the `Chrystoki.conf/crystoki.ini` file, unless directed to do so by Gemalto Technical Support. If you do modify the file, never insert TAB characters - use individual space characters. Avoid modifying the PED timeout settings. These are now hardcoded in the appliance, but the numbers in the `Chrystoki.conf` file must match.

## Controlling User Access to Your Attached HSMs and Partitions

By default, only the root user has access to your attached HSMs and partitions. You can specify a set of non-root users that are permitted to access your attached HSMs and partitions, by adding them to the **hsmusers** group.

**NOTE** The client software installation automatically creates the `hsmusers` group if one does not already exist on your system. The `hsmusers` group is retained when you uninstall the client software, allowing you to upgrade your client software while retaining your `hsmusers` group configuration.

### Adding users to hsmusers group

To allow non-root users or applications access your attached HSMs and partitions, assign the users to the **hsmusers** group. The users you assign to the `hsmusers` group must exist on the client workstation. Users you add to the `hsmusers` group are able to access your attached HSMs and partitions. Users who are not part of the `hsmusers` group are not able to access your attached HSMs and partitions.

#### To add a user to hsmusers group

1. Ensure that you have **sudo** privileges on the client workstation.
2. Add a user to the `hsmusers` group:

```
sudo gpasswd --add <username> hsmusers
```

where `<username>` is the name of the user you want to add to the `hsmusers` group.

### Removing users from hsmusers group

Should you wish to rescind a user's access to your attached HSMs and partitions, you can remove them from the `hsmusers` group.

**NOTE** The user you delete will continue to have access to the HSM until you reboot the client workstation.

#### To remove a user from hsmusers group

1. Ensure that you have **sudo** privileges on the client workstation.
2. Remove a user from the `hsmusers` group:

```
sudo gpasswd -d <username> hsmusers
```

where `<username>` is the name of the user you want to remove from the `hsmusers` group. You must log in again to see the change.

## Uninstalling the Luna HSM Client Software

You may need to uninstall the Luna HSM Client software prior to upgrading to a new release, or if the software is no longer required.

### To uninstall the Luna HSM Client software:

1. Log in as root. (use sudo instead)
2. Go to the client installation directory:

```
cd /usr/safenet/lunaclient/bin
```

3. Run the uninstall script:

```
sudo sh uninstall.sh
```

## Installing Java

If you install the Luna Java Security Provider (JSP), refer to [SafeNet JSP Overview and Installation](#) for additional setup procedures for your operating system.

## Scripted or Unattended Installation

If you prefer to run the installation from a script, rather than interactively, run the command with the options **-p** <list of SafeNet products> and **-c** <list of SafeNet components>. To see the syntax, run the command with **help** like this:

```
[myhost]$ sudo sh install.sh help
[sudo] password for fred
```

At least one product should be specified.

usage:

```
install.sh      - Luna Client install through menu
install.sh help - Display scriptable install options
install.sh all  - Complete Luna Client install

install.sh -p [sa|pci|g5|rb] [-c sdk|jsp|jcprov|ldpc|snmp]

-p <list of Luna products>
-c <list of Luna components> - Optional. All components are installed if not provided
```

Luna products options

```
sa      - SafeNet Luna Network HSM
pci     - SafeNet Luna PCIe HSM
g5     - SafeNet Luna USB HSM
rb     - SafeNet Luna Backup HSM
```

Luna components options

```
sdk     - Luna SDK
jsp     - Luna JSP (Java)
jcprov  - Luna JC PROV (Java)
snmp    - Luna SNMP subagent
```

```
[myhost]$
```

For scripted/automated installation, your script will need to capture and respond to the License Agreement prompt, and to the confirmation prompt. For example:

```
[myhost]$ sudo sh install.sh all
```

```
IMPORTANT: The terms and conditions of use outlined in the software
license agreement (Document #008-010005-001_053110) shipped with the product
("License") constitute a legal agreement between you and SafeNet Inc.
Please read the License contained in the packaging of this
product in its entirety before installing this product.
```

```
Do you agree to the License contained in the product packaging?
```

```
If you select 'yes' or 'y' you agree to be bound by all the terms
and conditions se out in the License.
```

```
If you select 'no' or 'n', this product will not be installed.
```

```
(y/n) y
```

```
Complete Luna HSM Client will be installed. This includes SafeNet Luna Network HSM,
SafeNet Luna PCIe HSM, SafeNet Luna USB HSM AND SafeNet Luna Backup HSM.
```

```
Select 'yes' or 'y' to proceed with the install.
```

```
Select 'no' or 'n', to cancel this install.
```

```
Continue (y/n)? y
```

## Interrupting the Installation

Do not interrupt the installation script in progress, and ensure that your host computer is served by an uninterruptible power supply (UPS). If you press [Ctrl] [C], or otherwise interrupt the installation (OS problem, power outage, other), some components will not be installed. It is not possible to resume an interrupted install process. The result of an interruption depends on where, in the process, the interruption occurred (what remained to install before the process was stopped).

As long as the cryptoki RPM package is installed, any subsequent installation attempt results in refusal with the message "A version of Luna HSM Client is already installed."

If components are missing or are not working properly after an interrupted installation, or if you wish to install any additional components at a later date (following an interrupted installation, as described), you would need to uninstall everything first. If **sh uninstall.sh** is unable to do it, then you must uninstall all packages manually.

Because interruption of the install.sh script is not recommended, and mitigation is possible, this is considered a low-likelihood corner case, fully addressed by these comments.

## Adding a DPoD HSM on Demand Service

Luna HSM Client allows you to use both Luna partitions and Data Protection on Demand's HSM on Demand services. Using a single client workstation, you can back up or migrate your keys between Luna and HSMoD, or combine partitions and services into an HA group.

The standard Luna HSM Client configuration file requires some special editing to add an HSMoD service. This procedure will allow you to add an HSMoD service to your existing Luna HSM Client.

**NOTE** This feature requires minimum client version 10.1. See [Version Dependencies by Feature](#) for more information

## Prerequisites

- > DPoD supports Windows and Linux operating systems only. This procedure presumes that you have already set up Luna HSM Client on your Windows or Linux workstation:
  - "Windows Luna HSM Client Installation" on page 28
  - "Linux Luna HSM Client Installation" on page 44
- > You must be using Luna HSM Client software version 10.1 or higher (see "Updating the Luna HSM Client Software" on page 79).
- > HSMoD services are only compatible with password-authenticated SafeNet Luna PCIe HSM partitions. For more information on Luna/DPoD compatibility, refer to [Cloning Keys Between Luna 6, Luna 7, and HSM on Demand](#). You can still use HSMoD and PED-authenticated Luna partitions from the same client workstation, but they cannot clone cryptographic objects between them.
- > You must purchase an HSMoD service from SafeNet Data Protection on Demand:
 

<https://safenet.gemalto.com/data-protection-on-demand/>

## To add a DPoD HSM on Demand service to an existing Luna HSM Client

1. After purchasing an HSMoD service, refer to the DPoD documentation for instructions on downloading the DPoD client package. Transfer the .zip file to your Luna HSM Client workstation using **pscp**, **scp**, or other secure means.
2. Extract the .zip file into a directory on your client workstation.
3. Extract or untar the appropriate client package for your operating system. Do not extract to a new subdirectory; place the files in the DPoD client install directory. The other client package can be safely deleted.
  - [Windows] **cvclient-min.zip**
  - [Linux] **cvclient-min.tar**  
**# tar -xvf cvclient-min.tar**
4. Run the provided script to create a new configuration file containing information required by the HSMoD service.
  - [Windows] Right-click **setenv.cmd** and select **Run as Administrator**.
  - [Linux] Source the **setenv** script.  
**# source ./setenv**
5. Copy the server certificate from the DPoD client directory to your existing client certificates directory:
  - [Windows default] **C:\Program Files\Safenet\Lunaclient\cert\**
  - [Linux default] **/usr/safenet/lunaclient/cert/**

**server-certificate.pem**  
**partition-ca-certificate.pem**

**partition-certificate.pem**

6. Open the configuration file in the DPoD client directory.
  - [Windows] **crystoki.ini**
  - [Linux] **Chrystoki.conf**
7. Copy the following sections from the DPoD configuration file to the existing version in the Luna HSM Client install directory. Edit the entries to use the correct filepath to the certificates you copied in step 5:

```
[XTC]
Enabled=1
PartitionCAPath=<client_cert_directory>\partition-ca-certificate.pem
PartitionCertPath00=<client_cert_directory>\partition-certificate.pem
TimeoutSec=600
```

```
[REST]
ClientConnectIntervalMs=1000
ClientConnectRetryCount=900
ClientEofRetryCount=15
ClientPoolSize=32
ClientTimeoutSec=120
CVAppSpecificData=90vNGg10a8uVBmO8zmEVRA==
RestClient=1
ServerName=na.hsm.dpod.live
ServerPort=443
SSLClientSideVerifyFile=<client_cert_directory>\server-certificate.pem
```

Also copy the following entry from the **Misc** section and edit to use the correct filepath to the **plugins** directory:

```
[Misc]
PluginModuleDir=<client_plugins_directory>
```

- [Windows default] **C:\Program Files\Safenet\Lunaclient\plugins\**
- [Linux default] **/usr/safenet/lunaclient/plugins/**

**NOTE** The above example is taken from a Windows **crystoki.ini** file; for a Linux client platform, the **Chrystoki.conf** file uses the same entries in Linux syntax (**Misc = {** instead of **[Misc]**, etc).

Save the configuration file. If you wish, you can now safely delete the extracted DPoD client directory.

8. Manually reset the **ChrystokiConfigurationPath** environment variable back to the location of the original configuration file.
  - [Windows] In the Control Panel, search for "environment" and select **Edit the system environment variables**. Click **Environment Variables**. In both the list boxes for the current user and system variables, edit **ChrystokiConfigurationPath** to point to the **crystoki.ini** file in the original client install directory.
  - [Linux] Either open a new shell session, or reset the environment variable for the current session to the location of the original **Chrystoki.conf** file:
 

```
# export ChrystokiConfigurationPath=/etc/
```
9. Launch or relaunch LunaCM to verify that both your Luna partitions and HSMoD service are available.

You can now initialize the HSM on Demand service just as you would a password-authenticated Luna application partition. The cloning domain you set on the HSMoD service must match the partition(s) from which you will migrate keys. Refer to the Data Protection on Demand documentation for instructions and information on the capabilities of your HSMoD service.

- > [Initializing an Application Partition](#)
- > [Initializing the Crypto Officer and Crypto User Roles](#)

Refer to [Cloning Keys Between Luna 6, Luna 7, and HSM on Demand](#) before migrating keys or using the HSMoD service in an HA group. You can migrate keys to your new HSMoD service using direct slot-to-slot cloning, a SafeNet Luna Backup HSM, or by setting up an HA group.

- > [Cloning Objects to Another Application Partition](#)
- > [Backup and Restore Using a G5-Based Backup HSM](#)
- > [Setting Up an HA Group](#)

## Configuration File Summary

The Luna HSM Client software installation includes a configuration file that controls many aspects of client operation. The configuration file can be found in the following default locations:

- > **Windows:** `C:\Program Files\SafeNet\LunaClient\crystoki.ini`
- > **Linux/UNIX:** `/etc/Chrystoki.conf`

The configuration file is organized into named sections, containing various configuration entries. It is installed with the default settings described in the table below. In addition to the default sections and entries, some additional sections/entries can be added to customize functionality. Generally, Thales Group does not recommend editing the configuration file directly; many entries are changed by entering commands in LunaCM or `vtl`. However, some entries can only be edited manually.

If you update the Luna HSM Client software by running the uninstaller and then installing a newer version, the existing configuration file is saved. This preserves your configuration settings, including the location of certificates necessary for your partition NTLS/STC connections for Luna products.

The following table describes all valid sections and entries in the configuration file. When editing the file, ensure that you maintain the applicable syntax conventions for your operating system (use existing sections/entries as a template for new entries). Where applicable, entries are listed with the valid range of values and the default setting.

**NOTE** Some of the sections/entries listed do not appear in the configuration file by default; you must add these sections/entries to change the behavior described below.

Some of the entries listed include a default setting that is observed even if the entry is not included in the configuration file by default; you must add the entry to change the default behavior.

Section/Setting	Description
<b>Chrystoki2</b>	

Section/Setting	Description
LibNT	Path to the Chrystoki2 library on Windows operating systems. <b>Default: C:\Program Files\SafeNet\LunaClient\cryptoki.dll</b>
LibNT32	Path to the Chrystoki2 library on 32-bit Windows systems only. <b>Default: C:\Program Files\SafeNet\LunaClient\win32\libCryptoki2.dll</b>  <b>NOTE</b> Luna HSM Client 10.1 and newer includes libraries for 64-bit operating systems only.
LibUNIX64	Path to the Chrystoki2 library on 64-bit Linux/UNIX operating systems. <b>Default:</b> > <b>Linux/AIX: /usr/safenet/lunaclient/libs/64/libCryptoki2_64.so</b> > <b>Solaris: /opt/safenet/lunaclient/libs/64/libCryptoki2_64.so</b>
<b>Luna</b>	
CloningCommandTimeout	The amount of time (in milliseconds) the library allows for the HSM to respond to a cloning command. <b>Default: 300000</b>
CommandTimeoutPedSet	This is an exception to DefaultTimeout (below). It defines the time (in milliseconds) allowed for all PED-related HSM commands. PED-related commands can take longer than ordinary commands governed by DefaultTimeout. Generally, the following formula applies: CommandTimeOutPedSet = DefaultTimeout + PEDTimeout1 + PEDTimeout2 + PEDTimeout3 <b>Default: 720000</b>
DefaultTimeOut	Defines the time (in milliseconds) the HSM driver in the host system waits for HSM commands to return a result. If a result is not returned in that time, the driver halts the HSM and returns DEVICE_ERROR to all applications using the HSM. The only exceptions are when a command's timeout is hard-coded in the Cryptoki library, or the command falls into a class governed by one of the other timeout intervals described elsewhere in this section. <b>Default: 500000</b>
DomainParamTimeout	Timeout (in milliseconds) for Domain Parameter Generation. <b>Default: 5400000</b>

Section/Setting	Description
KeypairGenTimeOut	<p>Defines the time (in milliseconds) the library waits for a keypair generation operation to return a value. The randomization component of keypair generation can cause large keypairs to take a long time to generate, and this setting keeps the attempts within a reasonable time. You can change this value to manage your preferred balance between long waits and the inconvenience of restarting a keygen operation.</p> <p><b>Default: 2700000</b></p>
PEDTimeout1	<p>Defines the time (in milliseconds) the HSM attempts to ping the PED before sending a PED operation request. If the PED is unreachable, the HSM returns a code indicating that the PED is not connected.</p> <p><b>Default: 100000</b></p>
PEDTimeout2	<p>Defines the time (in milliseconds) that the HSM waits for the local PED to respond to a PED operation request. If the local PED does not respond to the request within the span of PEDTimeout2, the HSM returns an appropriate result code (such as PED_TIMEOUT). This is the timeout you might increase from the Default value if you were initializing larger MofN PED Key sets - the HSM allows M and N to each be up to 16 splits - maybe applying PED PINS, and making a duplicate set as well.</p> <p><b>Default: 200000</b></p>
PEDTimeout3	<p>Defines the additional time (in milliseconds) the HSM waits for a remote PED to respond to a PED operation request. Therefore, the actual time the firmware waits for a remote PED response is PEDTimeout2 + PEDTimeout3.</p> <p><b>Default: 20000</b></p>
<b>CardReader</b>	
LunaG5Slots	<p>Number of SafeNet Luna G5 Backup HSM slots reserved so that the library will check for connected devices.</p> <p><b>Valid Values:</b></p> <ul style="list-style-type: none"> <li>&gt; <b>0:</b> If you have no SafeNet Luna G5 Backup HSMs and wish to eliminate the reserved spaces in your slot list, use this setting.</li> <li>&gt; <b>1-N:</b> Can be set to any number, but is effectively limited by the number of external USB devices supported by your client workstation.</li> </ul> <p><b>Default: 3</b></p>

Section/Setting	Description
LunaG7Slots	<p>Number of SafeNet Luna G7 Backup HSM slots reserved so that the library will check for connected devices.</p> <p><b>Valid Values:</b></p> <ul style="list-style-type: none"> <li>&gt; <b>0:</b> If you have no SafeNet Luna G7 Backup HSMs and wish to eliminate the reserved spaces in your slot list, use this setting.</li> <li>&gt; <b>1-N:</b> Can be set to any number, but is effectively limited by the number of external USB devices supported by your client workstation.</li> </ul> <p><b>Default: 3</b></p>
RemoteCommand	<p>This setting was used when debugging older SafeNet products. For modern products it is ignored.</p> <p><b>Valid Values:</b></p> <ul style="list-style-type: none"> <li>&gt; <b>0:</b> false</li> <li>&gt; <b>1 (default):</b> true</li> </ul>
<b>RBS</b>	<b>NOTE</b> RBS is not supported with HSM on Demand services.
CmdProcessor	<p>The location of the RBS library.</p> <p><b>Default:</b></p> <ul style="list-style-type: none"> <li>&gt; <b>Windows:</b> C:\Program Files\SafeNet\LunaClient\rbs_processor2.dll</li> <li>&gt; <b>Linux/AIX:</b> /usr/safenet/lunaclient/rbs/lib/librbs_processor2.dll</li> <li>&gt; <b>Solaris:</b> /opt/safenet/lunaclient/rbs/lib/librbs_processor2.dll</li> </ul>
HostPort	<p>The port number used by the RBS server.</p> <p><b>Valid Values:</b> any unassigned port</p> <p><b>Default: 1792</b></p>
ClientAuthFile	<p>The location of the RBS Client authentication file.</p> <p><b>Default:</b></p> <ul style="list-style-type: none"> <li>&gt; <b>Windows:</b> C:\Program Files\SafeNet\LunaClient\config\clientauth.dat</li> <li>&gt; <b>Linux/AIX:</b> /usr/safenet/lunaclient/rbs/clientauth.dat</li> <li>&gt; <b>Solaris:</b> /opt/safenet/lunaclient/rbs/clientauth.dat</li> </ul>
ServerSSLConfigFile	<p>The location of the OpenSSL configuration file used by RBS Server or Client.</p> <p><b>Default:</b></p> <ul style="list-style-type: none"> <li>&gt; <b>Windows:</b> C:\Program Files\SafeNet\LunaClient\rbs\server.cnf</li> <li>&gt; <b>Linux/AIX:</b> /usr/safenet/lunaclient/rbs/server/server.cnf</li> <li>&gt; <b>Solaris:</b> /opt/safenet/lunaclient/rbs/server/server.cnf</li> </ul>

Section/Setting	Description
ServerPrivKeyFile	The location of the RBS Server certificate private key file. <b>Default:</b> > <b>Windows:</b> C:\Program Files\SafeNet\LunaClient\cert\server\serverkey.pem > <b>Linux/AIX:</b> /usr/safenet/lunaclient/rbs/server/serverkey.pem > <b>Solaris:</b> /opt/safenet/lunaclient/rbs/server/serverkey.pem
ServerCertFile	The location of the RBS Server certificate file. <b>Default:</b> > <b>Windows:</b> C:\Program Files\SafeNet\LunaClient\cert\server\server.pem > <b>Linux/AIX:</b> /usr/safenet/lunaclient/rbs/server/server.pem > <b>Solaris:</b> /opt/safenet/lunaclient/rbs/server/server.pem
NetServer	Determines whether RBS acts as a server or client. <b>Valid Values:</b> > <b>0:</b> Client > <b>1 (default):</b> Server
HostName	The hostname or IP address that the RBS server will listen on. <b>Valid Value:</b> any hostname or IP address <b>Default:</b> 0.0.0.0 (any IP on the local host)
Available	Lists the serial numbers of SafeNet Luna Backup HSMs available on the RBS server.
<b>LunaSA Client</b>	
ReceiveTimeout	Time in milliseconds before a receive timeout. <b>Default:</b> 20000
SSLConfigFile	Location of the OpenSSL configuration file. <b>Default:</b> > <b>Windows:</b> C:\Program Files\SafeNet\LunaClient\openssl.cnf > <b>Linux/AIX:</b> /usr/safenet/lunaclient/bin/openssl.cnf > <b>Solaris:</b> /opt/safenet/lunaclient/bin/openssl.cnf

Section/Setting	Description
ClientPrivKeyFile	<p>Location of the client private key. This value is set by <b>vtl</b> or <code>lunacm:&gt; clientconfig deploy</code>.</p> <p><b>Default:</b></p> <ul style="list-style-type: none"> <li>&gt; <b>Windows:</b> C:\Program Files\SafeNet\LunaClient\cert\client\<clientname&gt;key.pem< li=""> <li>&gt; <b>Linux/AIX:</b> /usr/safenet/lunaclient/cert/client/&lt;ClientName&gt;Key.pem</li> <li>&gt; <b>Solaris:</b> /opt/safenet/lunaclient/cert/client/&lt;ClientName&gt;Key.pem</li> </clientname&gt;key.pem<></li></ul>
ClientCertFile	<p>Location of the client certificate that is uploaded to SafeNet Luna Network HSM for NTLS. This value is set by <b>vtl</b> or <code>lunacm:&gt; clientconfig deploy</code>.</p> <p><b>Default:</b></p> <ul style="list-style-type: none"> <li>&gt; <b>Windows:</b> C:\Program Files\SafeNet\LunaClient\cert\client\<clientname&gt;cert.pem< li=""> <li>&gt; <b>Linux/AIX:</b> /usr/safenet/lunaclient/cert/client/&lt;ClientName&gt;Cert.pem</li> <li>&gt; <b>Solaris:</b> /opt/safenet/lunaclient/cert/client/&lt;ClientName&gt;Cert.pem</li> </clientname&gt;cert.pem<></li></ul>
ServerCAFile	<p>Location of the server certificate file on the client workstation. This value is set by <b>vtl</b> or <code>lunacm:&gt; clientconfig deploy</code>.</p> <p><b>Default:</b></p> <ul style="list-style-type: none"> <li>&gt; <b>Windows:</b> C:\Program Files\SafeNet\LunaClient\cert\server\CAFile.pem</li> <li>&gt; <b>Linux/AIX:</b> /usr/safenet/lunaclient/cert/server/CAFile.pem</li> <li>&gt; <b>Solaris:</b> /opt/safenet/lunaclient/cert/server/CAFile.pem</li> </ul>
NetClient	<p>Determines whether the library searches for network slots.</p> <p><b>Valid Values:</b></p> <ul style="list-style-type: none"> <li>&gt; <b>0:</b> The library does not search for network slots.</li> <li>&gt; <b>1 (default):</b> The library searches for network slots.</li> </ul>
TCPKeepAlive	<p>TCPKeepAlive is a TCP stack option, available at the Luna HSM Client and the SafeNet Luna Network HSM appliance. It is controlled via an entry in the Luna HSM Client configuration file, and an equivalent file on the SafeNet Luna Network HSM.</p> <p>The settings at the appliance and the client are independent. This allows a level of assurance, in case (for example) a firewall setting blocks communication in one direction.</p> <p><b>Valid Values:</b></p> <ul style="list-style-type: none"> <li>&gt; <b>0:</b> false</li> <li>&gt; <b>1 (default):</b> true</li> </ul>

Section/Setting	Description
ServerName##	These entries identify NTLS-linked SafeNet Luna Network HSM servers/ports, and determines the order in which they are polled to create a slot list. These values are set by <code>vti</code> or <code>lunacm:&gt; clientconfig deploy</code> .
ServerPort##	
<b>Presentation</b>	<b>NOTE</b> This section is not created automatically. To change any of the following values, you must first create this section in the configuration file.
OneBaseSlotId	Determines whether slot listing begins at <b>0</b> or <b>1</b> . <b>Default: 0</b>
ShowAdminTokens	Determines whether the Admin partitions of locally-installed SafeNet Luna PCIe HSMs are visible in the slot list. <b>Valid Values:</b> > <b>no</b> : Admin slots are hidden. > <b>yes</b> (default): Admin slots are visible.
ShowEmptySlots	Determines whether slot numbers are reserved for partitions that have not yet been created on the HSM. When this setting is enabled, slot numbers remain consistent over time, even when new partitions are created. <b>Valid Values:</b> > <b>no</b> (default): Only existing partitions are assigned slot numbers. > <b>yes</b> : Slot numbers are reserved for the maximum number of partitions that can be created on HSMs connected to the client.  <b>NOTE</b> This does not apply to SafeNet Luna Network HSM partitions assigned to the client, which will always appear in the lowest-numbered slots, causing locally-connected and DPoD slots to increment higher.
ShowUserSlots	Allows you to set permanent slot numbers for specific partitions or HA virtual partitions. If you use this setting, you must specify a slot for all partitions on a specific HSM, or the partitions not listed here will not be visible to the client. <b>Valid Values:</b> Comma-delimited list in the format <slotnum><serialnum> <b>Example:</b> <b>ShowUserSlots=1(351970018022),2(351970018021),3(351970018020),...</b>
<b>HAConfiguration</b>	

Section/Setting	Description
AutoReconnectInterval	<p>Specifies the interval (in seconds) at which the library will attempt to reconnect with a missing HA member, until the set number of attempts is reached. This value is set using lunacm:&gt; <a href="#">hagroup interval</a>.</p> <p><b>Valid Values:</b></p> <ul style="list-style-type: none"> <li>&gt; <b>60-1200:</b> Wait the specified number of seconds between reconnection attempts.</li> </ul> <p><b>Default:</b> 60 seconds</p>
HAOnly	<p>Determines whether individual HA member slots are visible to client applications. Hiding individual members helps prevent synchronization errors by preventing applications from directing calls to individual member partitions. If a member partition fails, the other slots in the system change, which can cause applications to send calls to the wrong slot number. This setting prevents this by hiding all physical slots from applications.</p> <p><b>Valid Values:</b></p> <ul style="list-style-type: none"> <li>&gt; <b>0</b> (default): All partitions are visible to applications as slots.</li> <li>&gt; <b>1:</b> Only HA virtual slots are visible to applications.</li> </ul> <div style="border: 1px solid black; padding: 5px; margin-top: 10px;"> <p><b>NOTE</b> This setting does not affect how slots are numbered in LunaCM; you can still configure individual member partitions with HAOnly mode enabled.</p> </div>
reconnAtt	<p>Specifies the number of reconnection attempts the client makes to a missing HA member. Once this number is reached, you must manually reconnect the member when it becomes available (see <a href="#">Manually Recovering a Failed HA Group Member</a>).</p> <p>This value is set using lunacm:&gt; <a href="#">hagroup retry</a>.</p> <p><b>Valid Values:</b></p> <ul style="list-style-type: none"> <li>&gt; <b>-1:</b> Perform infinite reconnection attempts.</li> <li>&gt; <b>0:</b> Disable HA auto-recovery.</li> <li>&gt; <b>1-500:</b> Perform the specified number of reconnection attempts.</li> </ul>
<b>Misc</b>	

Section/Setting	Description
CopyRSAPublicValuesFromPrivateTemplate	<p>Controls whether the public exponent of an RSA key can be copied from the private key template, if the public key template does not already have a public exponent attribute set.</p> <p><b>Valid Values:</b></p> <ul style="list-style-type: none"> <li>&gt; <b>0</b>: if no public exponent is provided in the public template, an error is returned (expected behavior).</li> <li>&gt; <b>1</b>(default): if no public exponent is provided in the public template, the private exponent is copied from the private template to populate the public template.</li> </ul> <p>For PKCS#11 compliance, this should be set to <b>0</b>.</p> <div style="border: 1px solid black; padding: 5px; margin-top: 10px;"> <p><b>NOTE</b> This functionality requires Luna HSM Client 7.1.0 or newer.</p> </div>
FunctionBindLevel	<p>Determines what action to take if a function binding fails during a CryptokiConnect() operation.</p> <p><b>Valid Values:</b></p> <ul style="list-style-type: none"> <li>&gt; <b>0</b> (default): fail if not all functions can be resolved</li> <li>&gt; <b>1</b>: do not fail but issue warning for each function not resolved</li> <li>&gt; <b>2</b>: do not fail and do not issue warning (silent mode)</li> </ul>
LoginAllowedOnFMEnabledHSMs	<p>Determines whether the client can log in to a partition on an HSM that uses Functionality Modules (FMs). FMs consist of custom-designed code that introduces new functionality, which can be more or less secure than standard HSM functions.</p> <p>Possible values include:</p> <ul style="list-style-type: none"> <li>&gt; <b>0</b>: the client does not allow login to an FM-enabled partition</li> <li>&gt; <b>1</b>: the client allows login to an FM-enabled partition</li> </ul> <p>This entry is added to the configuration file the first time you initialize or log in to an FM-enabled partition using LunaCM. You are prompted to confirm that you want to allow login.</p>
PE1746Enabled	<p>Enables the SafeXcel 1746 security co-processor on Luna 6 HSMs, which is used to offload packet processing and cryptographic computations from the host processor. Does not apply to Luna 7 HSMs or HSM on Demand services..</p> <p><b>Valid Values:</b></p> <ul style="list-style-type: none"> <li>&gt; <b>0</b>: SafeXcel co-processor is disabled on Luna 6 HSMs.</li> <li>&gt; <b>1</b> (default): SafeXcel co-processor is enabled on Luna 6 HSMs.</li> </ul>

Section/Setting	Description
PluginModuleDir	<p>Specifies the location of client plugins. This setting is required to use the DPoD plugin to access DPoD HSM on Demand services.</p> <p><b>Default:</b></p> <ul style="list-style-type: none"> <li>&gt; <b>Windows:</b> C:\Program Files\SafeNet\LunaClient\plugins</li> <li>&gt; <b>Linux:</b> /usr/safenet/lunaclient/libs/64/plugins</li> </ul>
ProtectedAuthenticationPathFlagStatus	<p>Specifies which role to check for challenge request status.</p> <p><b>Valid Values:</b></p> <ul style="list-style-type: none"> <li>&gt; <b>0</b> (default): no challenge request</li> <li>&gt; <b>1</b>: check for Crypto Officer challenge request</li> <li>&gt; <b>2</b>: check for Crypto User challenge request</li> </ul> <p><b>NOTE</b> This functionality requires Luna HSM Client 7.1.0 or newer.</p>
RSAKeyGenMechRemap	<p>This entry remaps calls to certain older mechanisms, no longer supported on the latest firmware, to use newer, more secure mechanisms instead.</p> <ul style="list-style-type: none"> <li>&gt; <b>0</b>: No re-mapping is performed.</li> <li>&gt; <b>1</b>: The following re-mapping occurs: <ul style="list-style-type: none"> <li>• PKCS Key Gen -&gt; 186-3 Prime key gen</li> <li>• X9.31 Key Gen -&gt; 186-3 Aux Prime key gen (see <a href="#">Mechanism Remap for FIPS Compliance</a>)</li> </ul> </li> </ul> <p><b>NOTE</b> This remapping is automatic if you are using Luna HSM Client 10.1 or newer, and the configuration file entry is ignored.</p>
RSAPre1863KeyGenMechRemap	<p>This entry remaps calls to newer mechanisms, when they are not available on older firmware, to use older mechanisms instead. Intended for evaluation purposes, such as with existing integrations that require newer mechanisms, before you update to firmware that actually supports the more secure mechanisms. Be careful with this setting, which makes it appear you are using a new, secure mechanism, when really you are using an outdated, insecure mechanism (see <a href="#">Mechanism Remap for FIPS Compliance</a>).</p> <ul style="list-style-type: none"> <li>&gt; <b>0</b>: No re-mapping is performed.</li> <li>&gt; <b>1</b>: The following re-mapping occurs if the HSM firmware permits: <ul style="list-style-type: none"> <li>• 186-3 Prime key gen -&gt; PKCS Key Gen</li> <li>• 186-3 Aux Prime key gen -&gt; X9.31 Key Gen</li> </ul> </li> </ul> <p><b>NOTE</b> This remapping is automatic if you are using Luna HSM Client 10.1 or newer, and the configuration file entry is ignored.</p>

Section/Setting	Description
ToolsDir	<p>The location of the Luna HSM Client tools.</p> <p><b>Default:</b></p> <ul style="list-style-type: none"> <li>&gt; <b>Windows:</b> C:\Program Files\SafeNet\LunaClient\</li> <li>&gt; <b>Linux/AIX:</b> /usr/safenet/lunaclient/bin/</li> <li>&gt; <b>Solaris:</b> /opt/safenet/lunaclient/bin/</li> </ul>
<b>Secure Trusted Channel</b>	<p><b>NOTE</b> Secure Trusted Channel is not supported with HSM on Demand Services.</p>
ClientTokenLib (for 64-bit Windows systems)	<p>Specifies the location of the token library on 64-bit Windows systems. This value must be correct in order to use a client token. If you are using a hard token, you must manually change this value to point to the hard token library for your operating system. The exact location of the hard token library may vary depending on your installer.</p> <p><b>Default:</b> C:\Program Files\SafeNet\LunaClient\softtoken.dll</p>
ClientTokenLib32 (for 32-bit Windows systems)	<p>Specifies the location of the token library on 32-bit Windows systems. This entry appears on Windows only.</p> <p>By default, <b>ClientTokenLib32</b> points to the location of the soft token library. If you are using a hard token, you must manually change this value to point to the hard token library for your operating system. The exact location of the hard token library may vary depending on your installer.</p> <p><b>Soft Token Default:</b> C:\Program Files\SafeNet\LunaClient\win32\softtoken.dll</p> <p><b>Hard Token Default:</b> C:\Windows\SysWOW64\etoken.dll</p> <div style="border: 1px solid black; padding: 5px; margin-top: 10px;"> <p><b>NOTE</b> Luna HSM Client 10.1 and newer includes libraries for 64-bit operating systems only.</p> </div>
<b>Session</b>	<p><b>NOTE</b> This section is not created automatically. To change any of the following values, you must first create this section in the configuration file.</p>
AutoCleanUpDisabled	<p>Determines whether AutoCleanUp closes orphaned sessions in the event that an application leaves sessions open. Useful for SafeNet Luna PCIe HSM hosts. AutoCleanUp runs during C_Finalize on the client. SafeNet Luna Network HSM sessions are tracked and closed by the NTLS service.</p> <p><b>Valid Values:</b></p> <ul style="list-style-type: none"> <li>&gt; <b>0</b> (default): Run AutoCleanUp if your application leaks sessions and you cannot rewrite the application.</li> <li>&gt; <b>1:</b> Disable AutoCleanUp if you have a SafeNet Luna PCIe HSM and your client application does proper housekeeping, or if your application is connecting via NTLS to a SafeNet Luna Network HSM.</li> </ul>
<b>Toggles</b>	<p><b>NOTE</b> This section is not created automatically. To change any of the following values, you must first create this section in the configuration file.</p>

Section/Setting	Description
legacy_memory_rep =	<p>Controls the manner in which the HSM reports the available RAM space.</p> <p><b>Valid Values:</b></p> <ul style="list-style-type: none"> <li>&gt; <b>0</b> (default): the public and private memory total/free values reported in the CK_TOKEN_INFO structure indicate the available flash memory for permanent (TOKEN) objects that are in either the public or private space respectively; this method is PKCS#11 compliant.</li> <li>&gt; <b>1</b>: the public memory values indicate the total/free RAM memory; this non-standard legacy method was used by some customers to determine space available for session based objects, and must be explicitly selected in order to continue using the legacy method.</li> </ul> <p><b>NOTE</b> This functionality requires minimum firmware version 7.1.0.</p>
lunacm_cv_ha_ui =	<p>Controls whether SafeNet Data Protection on Demand's HSM on Demand (HSMoD) services can be active members of an HA group.</p> <p><b>Valid Values:</b></p> <ul style="list-style-type: none"> <li>&gt; <b>0</b>: HSMoD services can be added as active HA members.</li> <li>&gt; <b>1</b>: (default): HSMoD services can be added to HA groups as standby members only. This is the default behavior to maximize HA performance, which may suffer due to network latency.</li> </ul> <p><b>NOTE</b> This functionality requires Luna HSM Client 10.1 or newer.</p>
<b>REST</b>	<p><b>NOTE</b> This section is not created automatically for clients obtained from the Thales Group Support Portal. For such clients, this section must be copied from a DPoD HSM on Demand client configuration file (see <a href="#">"Adding a DPoD HSM on Demand Service" on page 63</a>). This section governs DPoD functionality only and is not related to the Luna REST API. This functionality requires Luna HSM Client 10.1 or newer.</p>
ClientConnectIntervalMs	<p>Interval in milliseconds between client connection attempts.</p> <p><b>Default: 1000</b></p>
ClientConnectRetryCount	<p>Maximum connection attempts between the client and an HSMoD service.</p> <p><b>Default: 900</b></p>
ClientEofRetryCount	<p>Maximum command retries.</p> <p><b>Default: 15</b></p>
ClientPoolSize	<p>Number of threads in the thread pool available for client operations. This entry does not apply to Luna HSM Client 10.2 and newer – the pool size for these clients is always <b>64</b>. If the number of parallel connections is more than 64, old connections are closed to make space in the cache.</p> <p><b>Default: 32</b></p>

Section/Setting	Description
ClientTimeoutSec	<p>Time (in seconds) that the client waits for a response from an HSMoD service. This timeout applies to each retry attempt individually.</p> <p><b>Default: 120</b></p> <div style="border: 1px solid black; padding: 5px;"> <p><b>NOTE</b> This entry does not appear in the default configuration file, but the default value applies to this timeout. You can manually add the entry if you wish to edit the timeout.</p> </div>
CVAppSpecificData	String containing identifying information about your HSMoD service.
RestClient	Indicates that Luna HSM Client and associated tools are acting as REST clients.
ServerName	The name of the DPoD server providing HSMoD services.
ServerPort	The port used for DPoD server traffic.
SSLClientSideVerifyFile	Location of the DPoD server certificate chain file ( <b>server-certificate.pem</b> ). This parameter applies to Luna HSM Client versions 10.1 and older.
<b>XTC</b>	<p><b>NOTE</b> This section is not created automatically for clients obtained from the Thales Group Support Portal. For such clients, this section must be copied from a DPoD HSM on Demand client configuration file (see <a href="#">"Adding a DPoD HSM on Demand Service" on page 63</a>). This functionality requires Luna HSM Client 10.1 or newer.</p>
Enabled	<p>Indicates that XTC (Transferable Token Channel) is enabled. This channel must be enabled for the client to communicate with a DPoD service.</p> <p><b>Valid Values:</b></p> <ul style="list-style-type: none"> <li>&gt; <b>0</b>: XTC is disabled.</li> <li>&gt; <b>1</b> (default): XTC is enabled.</li> </ul>
PartitionCAPath	Location of the HSMoD partition origin certificate ( <b>partition-ca-certificate.pem</b> ) for clients version 10.1 and older.
PartitionCertPath00	Location of the HSMoD partition messaging certificate ( <b>partition-certificate.pem</b> ) for clients version 10.1 and older.
TimeoutSec	<p>Time (in seconds) before a cryptographic request expires. Timestamps are included in XTC headers, and the HSM rejects messages which have expired.</p> <p><b>Valid Values: 1-600</b></p>

## Updating the Luna HSM Client Software

---

To update the Luna HSM Client software, first uninstall any previous version of the Client. Then, run the new installer the same way you performed the original installation (refer to "[Luna HSM Client Software Installation](#)" on page 27).

The client uninstaller removes libraries, utilities, and other material related to the client, but does not remove configuration files and certificates. This allows you to install the newer version and resume operations without having to manually restore configuration settings and re-register client and appliance NTLS certificates.

# CHAPTER 4: Secure Transport Mode

SafeNet 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 Group 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 Group 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 Group 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.

## How does Secure Transport Mode work?

### When STM is enabled on the HSM (either at the factory or by customer)

- > 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).
- > 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.
- > 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).
- > 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.

**When you recover an HSM from STM:**

- > The HSM asks for the Random User String (which you received in an e-mail or by other means).
- > The HSM gathers the same sources of internal information and combines those with the Random User String that you just provided, and outputs a Verification String.
- > **Visually compare** the newly output Verification String with the original Verification String that was sent via e-mail (or other means).
  - If the original and the newly generated Verification Strings match, then the HSM has not been used or otherwise altered since STM was enabled.
  - If the original and the newly generated Verification Strings fail to match, then there might be a problem with the Random User String - such as an error in the string that was sent, or else an incorrect random user string was entered, or the HSM has been altered somewhere between the original sender and you.
- > If the HSM **has not** been altered (original and new Verification Strings match), then you can proceed to recovering the HSM from STM.
- > If the HSM might have been altered (original and new Verification Strings are different), then type "quit" at the prompt, and run the **stm recover** command again, to ensure that nothing was incorrectly entered on the first attempt.
- > If the Verification strings still do not match:
  - type "quit" to leave the HSM in STM, and contact Thales Group Technical Support for further guidance, or
  - if you feel that the Verification failure was benign, type "proceed" to release the HSM from Secure Transport Mode, and decide whether
    - you wish to proceed with using the HSM
    - or, instead,
    - you wish to perform factory reset and re-initialize the HSM as a safety precaution before proceeding further.

**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.

For information about the various tamper events, see "[Tamper Events](#)" on page 211.

**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

1. 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.
2. If the HSM is initialized, log in as the HSM SO (see "[Logging In as HSM Security Officer](#)" on page 190). If this is a new or zeroized HSM, skip to the next step.
3. 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:

```
lunacm:> 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.

Recovering a G7-based HSM from secure transport mode may take up to three minutes.

4. You are presented with a verification string:

If the verification string matches the original verification string, the HSM has not been altered or tampered, and can be safely re-deployed.

Enter **proceed** to recover from STM.

If the verification string does not match the original verification string, this might indicate that the HSM has been altered while in transit, or that an incorrect random user string has been entered.

### If the verification strings do not match

1. Reconfirm that you have entered the correct random user string for your HSM.
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 Group 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 Into 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!** If the HSM contains sensitive key material, ensure that you have a full backup of the HSM contents before proceeding.

### To place an HSM into Secure Transport Mode

1. Log in as the HSM SO (see "[Logging In as HSM Security Officer](#)" on page 190).
2. Backup the contents of all application partitions.

See [Backup and Restore Using a G5-Based Backup HSM](#) or [Backup and Restore Using a G7-Based Backup HSM](#) for details.

3. Enter the following command to place the HSM into STM:

```
lunacm:> stm transport
```

**NOTE** Placing a G7-based HSM into secure transport mode may take up to three minutes.

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.

This product uses semiconductors that can be damaged by electro-static discharge (ESD). When handling the device, avoid contact with exposed components, and always use an anti-static wrist strap connected to an earth ground. In rare cases, ESD can trigger a tamper or decommission event on the HSM. If this happens, all existing roles and cryptographic objects are deleted.

# CHAPTER 5: PED Authentication

The SafeNet Luna PIN Entry Device (Luna PED) provides PIN entry and secret authentication to a SafeNet Luna HSM that requires Trusted Path Authentication. The requirement for PED 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 PED-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 PED to the HSM via the independent, trusted-path interface. No password is entered via computer keyboard.

**NOTE** SafeNet Luna PCIe HSM 7.x requires Luna PED firmware version 2.7.1 or higher. This firmware is backward-compatible with SafeNet Luna PCIe HSM 6.x.

This chapter contains the following sections about PED authentication:

- > ["PED Authentication Architecture" below](#)
  - ["Comparing Password and PED Authentication" on the next page](#)
- > ["PED Keys" on page 86](#)
  - ["PED Key Types and Roles" on page 86](#)
  - ["Shared PED Key Secrets" on page 87](#)
  - ["Domain PED Keys" on page 88](#)
  - ["PED PINs" on page 88](#)
  - ["M of N Split Secrets \(Quorum\)" on page 88](#)
- > ["SafeNet Luna PED Received Items" on page 90](#)
- > ["SafeNet Luna PED Hardware Functions" on page 92](#)
- > ["Local PED Setup" on page 95](#)
- > ["About Remote PED" on page 97](#)
- > ["Remote PED Setup" on page 101](#)
- > ["PED Key Management" on page 111](#)
- > ["PEDserver and PEDclient" on page 124](#)

## PED Authentication Architecture

The PED Authentication architecture consists of the following components:

- > **SafeNet 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 ["SafeNet Luna PED Hardware Functions" on page 92](#)).

- > **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 87](#).
  - **PED PINs:** optional PINs associated with specific PED keys, set by the owner of the PED key at the time of creation. PED PINs offer an extra layer of security for PED keys which could be lost or stolen. See ["PED PINs" on page 88](#).
  - **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 ["M of N Split Secrets \(Quorum\)" on page 88](#).

## Comparing Password and PED Authentication

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

	Password-authentication	PED-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 PED 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; 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>
<b>Key-custodian responsibility</b>	<ul style="list-style-type: none"> <li>&gt; Password knowledge only</li> </ul>	<ul style="list-style-type: none"> <li>&gt; Linked to partition password knowledge</li> <li>&gt; Linked to black PED key(s) ownership and optional PED PIN knowledge</li> </ul>
<b>Two-factor authentication for remote access</b>	<ul style="list-style-type: none"> <li>&gt; Not available</li> </ul>	<ul style="list-style-type: none"> <li>&gt; Remote PED and orange (Remote PED Vector) PED key deliver highly secure remote management of HSM, including remote backup</li> </ul>

## PED Keys

A PED key is a USB authentication device, embedded in a molded plastic body. It 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. A PED key can contain only one authentication secret at a time, but it can be overwritten with a new authentication secret. See "[PED Key Management](#)" on page 111.

**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 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 189. The following table describes the keys associated with the various roles:

Lifecycle	PED Key	PED 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. <b>Mandatory</b>
	<b>Red</b> 	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 88. <b>Mandatory</b>
	<b>Orange</b> 	Remote PED Vector	Establishes a connection to a Remote PED server. <b>Optional</b>

Lifecycle	PED Key	PED Secret	Function
HSM Auditing	<b>White</b> 	Auditor (AU) secret	Authenticates the Auditor role, responsible for audit log management. This role has no access to other HSM services. <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. <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. <b>Mandatory</b>
	<b>Red</b> 	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" on the next page</a> . <b>Mandatory</b>
Partition Operation	<b>Black</b> 	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. <b>Mandatory</b>
	<b>Gray</b> 	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. <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. <b>Optional</b>

## 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.

**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.

### PED 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 PED keypad for all future authentication. The PED PIN provides two-factor authentication and ensures security in case a key is lost or stolen. If you forget your PED PIN, it is the same as losing the PED key entirely; you cannot authenticate the role.

PED 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 PED PINs, allowing multiple people access to the role (see ["Creating PED Keys" on page 111](#)). Copies made later are true copies with the same PED PIN, intended as backups for one person (see ["Duplicating Existing PED Keys" on page 121](#)). Duplicates of the PED key all have the same PED PIN.

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

**CAUTION!** Forgetting a PED 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 118](#).

### M of N Split Secrets (Quorum)

The Luna PED can split an authentication secret among multiple PED keys (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.

This can be likened to a club 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 between 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 to be 3 of 5. That is, the pool of individual holders of spits of that role secret is five persons, and from among them, a quorum of three must be available to achieve authentication.

In this scenario, the HSM SO authentication secret is split among five blue PED keys, and at least three of those keys must be presented to the Luna PED to log in as HSM SO.

This feature can be used to customize the level of security and oversight for all actions requiring PED authentication. You can elect to apply an 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.

### Activated Partitions and 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), allowing applications to perform cryptographic functions without having to present a black or gray PED key (see "[Activation and Auto-activation on PED-Authenticated Partitions](#)" on page 1). In this case, if the HSM is rebooted for maintenance or loses power due to an outage, the cached PED 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.

### New-CPU PED Behavior Notes

All of the following points apply to the newer-CPU 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 Network HSM 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-CPU 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-CPU PED will be unresponsive after a 7.x HMS firmware update or rollback, and/or the display might come up blank. The PED must be reset.

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

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

## SafeNet Luna PED Received Items

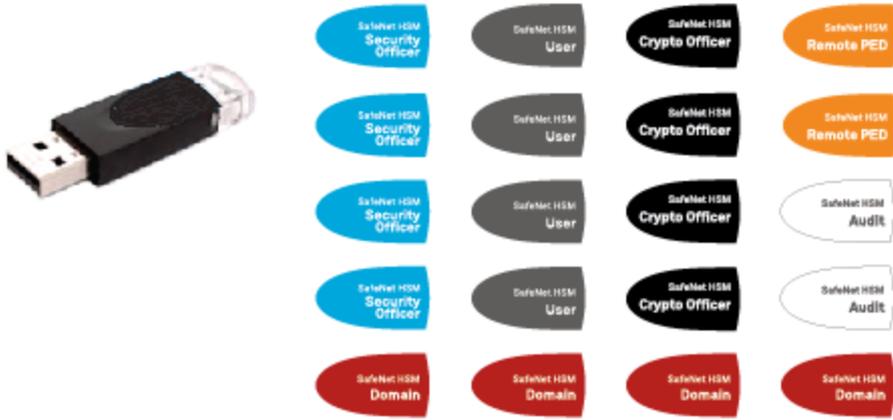
This chapter describes the items you received with your SafeNet Luna PED device. For instructions on setting up the PED, see ["PED Authentication" on page 84](#).

### Required Items

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

Qty	Item
1	<b>SafeNet Luna PED</b> (with firmware 2.7.1 or newer) 

Qty	Item
1	<p data-bbox="212 268 1474 331"><b>PED Power Supply</b> kit with replaceable mains plug modules for international use (employed when the PED is operated in Remote PED mode)</p> <p data-bbox="212 373 1426 436"><b>NOTE:</b> If your PED has firmware 2.8.0 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> 
1	<p data-bbox="212 974 1110 1005"><b>Cable, USB 2.0, Type A to Mini B connectors</b> (for Remote PED operation).</p> 

Qty	Item
1	<p><b>Cable, Data, 9-pin, Micro-D to Micro-D connectors</b> (for local PED operation prior to HSM firmware versions 7.x.).</p> 
1	<p><b>Ten-pack of iKey 1000 PED keys, and sheets of peel-and-stick labels</b></p> 

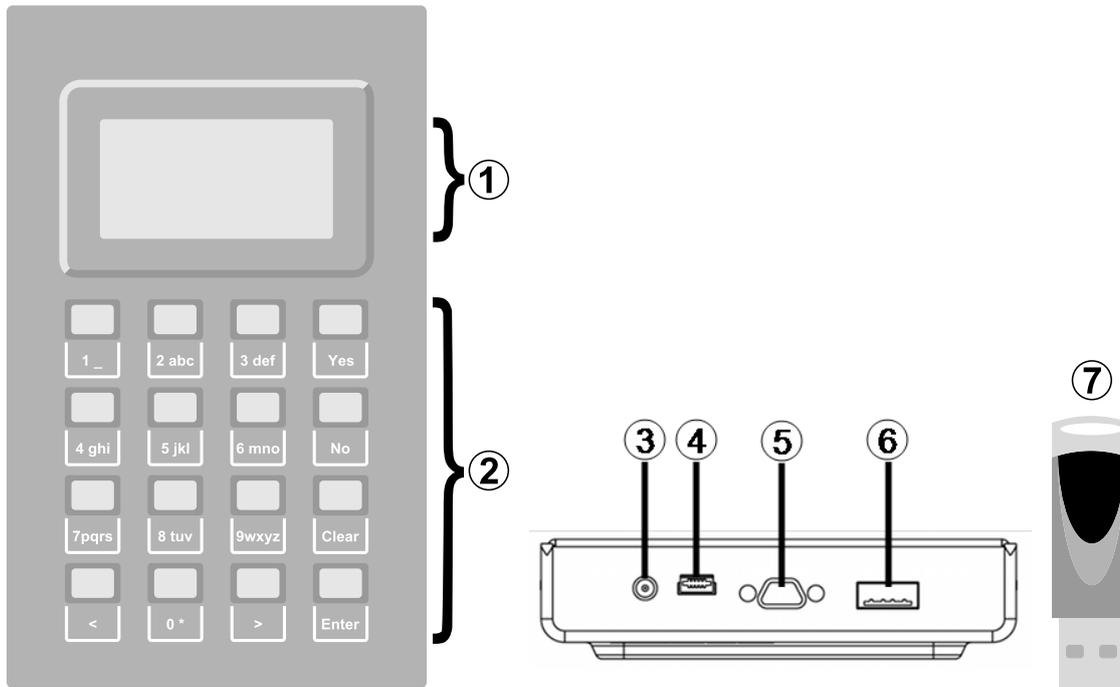
## SafeNet Luna PED Hardware Functions

The SafeNet 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" below](#)
- > ["Keypad Functions" on the next page](#)
- > ["Modes of Operation" on page 94](#)
- > ["Admin Mode Functions" on page 95](#)

### Physical Features

The SafeNet 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" below</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. PED version 2.8 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).

\* PEDs with firmware version 2.8 and above 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 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 PED 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>
<	<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>
>	<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 PED 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 SafeNet 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 the next page for instructions.
- > **Admin:** This mode is for upgrading the 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 SafeNet Luna PCIe HSM to be located in a data center or other location restricting physical access. See "[About Remote PED](#)" on page 97 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 Release 7.x SafeNet Luna PCIe HSM card, or LunaCM will return an error (CKR\_DEVICE\_ERROR) when you attempt authentication.

### Admin Mode Functions

In this mode, you can upgrade the 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 Group.
- > **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.

## Local PED Setup

A Local PED connection is the simplest way to set up the SafeNet 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 SafeNet Luna PCIe HSM administrator can use these directions to set up a Local PED connection. You require:

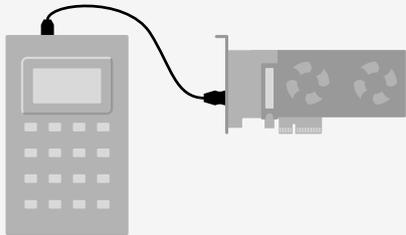
- > SafeNet Luna PED with firmware 2.7.1 or newer

- > 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 PED must be connected directly to the HSM card's USB port, and not one of the other USB connection ports on the host system.



2. PED version 2.8 and above is powered via the USB connection. If you are using PED version 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 94](#).

The Luna PED is now ready to perform authentication for the HSM. You may proceed with setting up or deploying your SafeNet Luna PCIe HSM. 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 LunaCM command (see ["Performing PED Authentication" on page 116](#))
- > Create copies of your PED keys (see ["Duplicating Existing PED Keys" on page 121](#))
- > Change to the Admin Mode to run tests or update PED software (see ["Changing Modes" on page 94](#))
- > Prepare to set up a Remote PED server (see ["About Remote PED" on the next page](#))

## Local PED Troubleshooting

If you encounter problems with Local PED, refer to this section.

### CKR\_PED\_UNPLUGGED error after hsm restart

After running **hsm restart**, LunaCM returns a CKR\_PED\_UNPLUGGED error when authentication is attempted.

```
lunacm:>role login -n so
```

```
Please attend to the PED.
```

Caution: You have only 3 so login attempts left. If you fail 3 more consecutive login attempts (i.e. with no successful logins in between) the HSM will be ZEROIZED!!!

Error in execution: CKR\_PED\_UNPLUGGED.

Command Result : 0x8000002e (CKR\_PED\_UNPLUGGED)

If you receive this error, disconnect the Luna PED from the HSM's USB port and reconnect it before issuing the login command again.

## About Remote PED

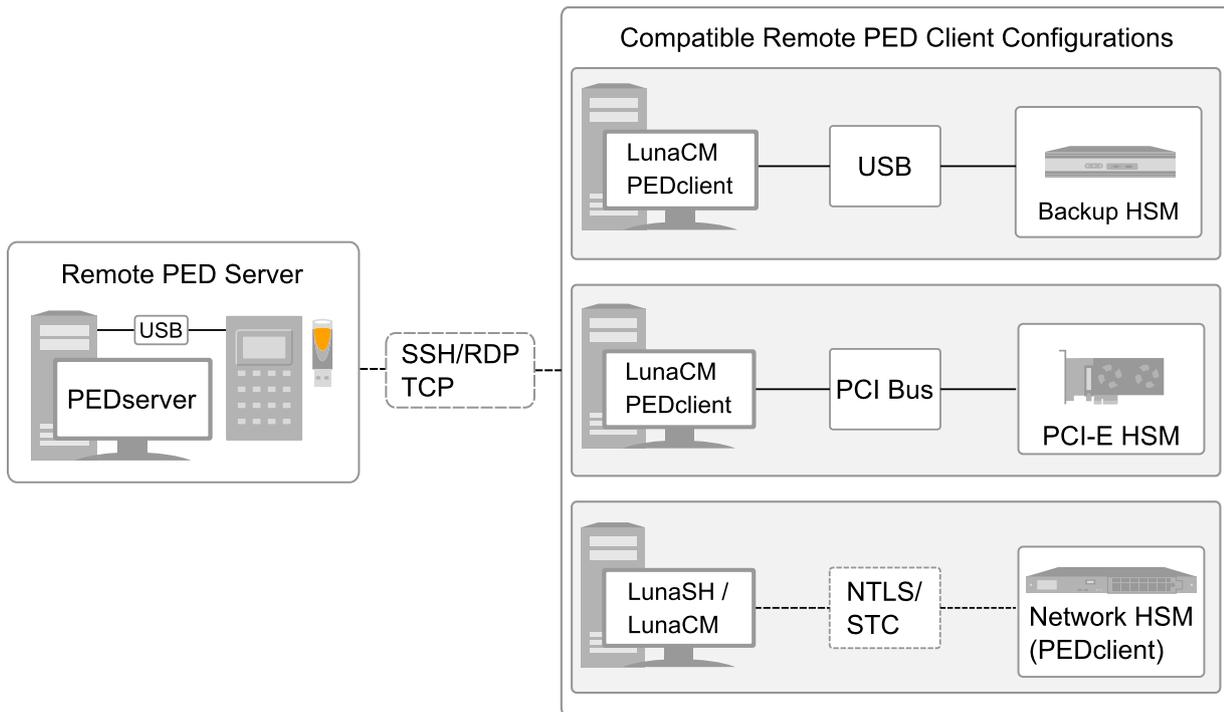
A Remote PED connection allows you to access PED-authenticated HSMs that are kept in a secure data center or other remote location where physical access is restricted or inconvenient. This section provides descriptions of the following aspects of Remote PED connections:

- > ["Remote PED Architecture" below](#)
- > ["Remote PED Connections" on the next page](#)
- > ["PEDserver-PEDclient Communications" on page 100](#)

## Remote PED Architecture

The Remote PED architecture consists of the following components:

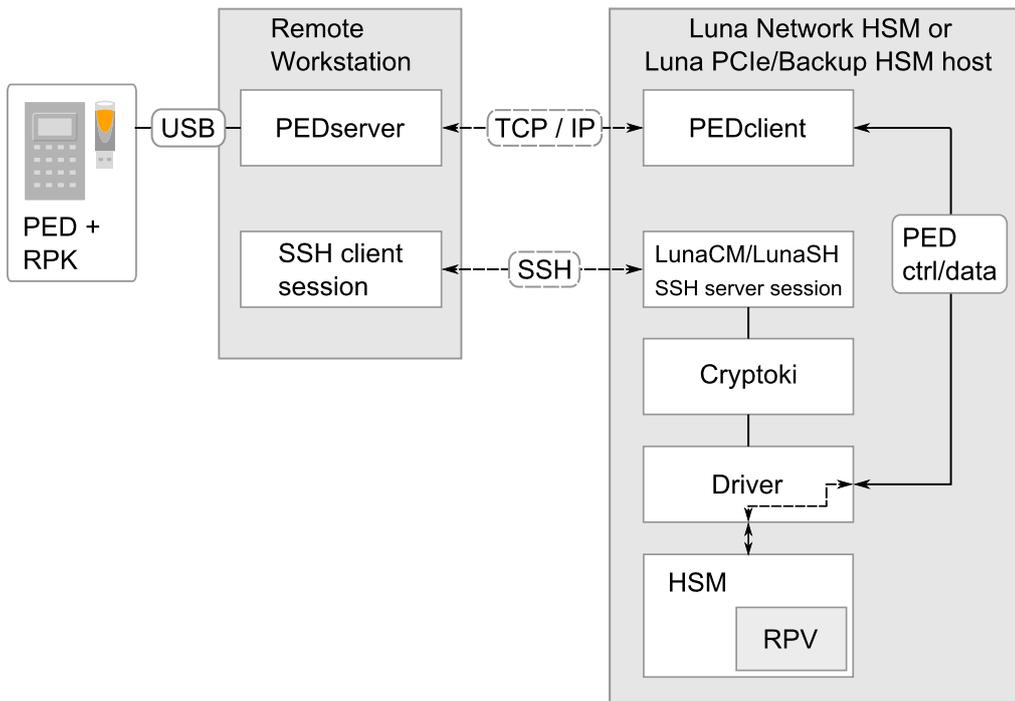
- > **Remote PED:** a Luna PED with firmware 2.7.1 or newer, connected to a network-connected workstation, powered on, and set to Remote PED mode.
- > **Remote PED Vector (RPV):** a randomly generated, encrypted value used to authenticate between a Remote PED (via PEDserver) and a SafeNet Luna HSM (via 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 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:
  - SafeNet Luna Network HSM
  - Host computer with SafeNet Luna PCIe HSM installed
  - Host computer with USB-connected SafeNet Luna Backup HSM, configured for remote backup



## Remote PED Connections

A SafeNet Luna PCIe HSM on a host computer running PEDclient can establish a Remote PED connection with any workstation that meets the following criteria:

- > PEDServer is running
- > a SafeNet Luna PED with firmware version 2.7.1 or newer is connected
- > The orange PED key containing the Remote PED Vector (RPV) for that HSM is available



### 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 107](#).

### 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 107](#).

### Timeout

PEDserver and PEDclient both have configurable timeout settings (default: 1800 seconds). See ["pedserver mode config" on page 132](#) or ["pedclient mode config" on page 145](#). The utilities are not aware of each other's timeout values, so the briefer value determines the actual timeout duration.

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)
- > SafeNet 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 **ped connect** in LunaCM to re-establish the Remote PED link. In a stable network situation, the link will remain available until timeout.

## PEDserver-PEDclient Communications

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 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.

## Remote PED Setup

A Remote PED connection allows you to access PED-authenticated HSMs that are kept in a secure data center or other remote location where physical access is restricted or inconvenient. This section provides instructions for setting up different Remote PED configurations.

The procedure for setting up a Remote PED connection can be broken down into the following general steps:

1. ["Initializing the Remote PED Vector \(RPV\) and Creating an Orange Remote PED Key \(RPK\)" below](#)
2. ["Installing PEDserver and Setting Up the Remote Luna PED" on the next page](#)
3. ["Opening a Remote PED Connection" on page 104](#)
4. [OPTIONAL] ["Ending or Switching the Remote PED Connection" on page 107](#)

If you encounter issues with Remote PED, see ["Remote PED Troubleshooting" on page 107](#).

Once Remote PED is set up, see ["PED Key Management" on page 111](#).

### Initializing the Remote PED Vector (RPV) and Creating an Orange Remote PED Key (RPK)

The Remote PED (via PEDserver) authenticates itself to the SafeNet Luna PCIe HSM 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 HSM being newly configured either

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

The orange key proves to the HSM that the Remote PED is authorized to provide authentication for HSM roles. A SafeNet Luna PCIe HSM administrator can create this key.

**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.

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

- > SafeNet Luna PED with 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 111](#) for more information.

## 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 95](#)).
2. Launch LunaCM on the SafeNet Luna PCIe HSM host workstation.
3. If the HSM is initialized, login as HSM SO (see ["Logging In as HSM Security Officer" on page 190](#)). If not, skip to the next step.

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

4. Ensure that you have the orange PED key(s) ready. Initialize the RPV.

```
lunacm:> ped vector
```

5. Attend to the Luna PED and respond to the on-screen prompts. See ["Creating PED Keys" on page 111](#) 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 PED 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" below](#).

## Installing PEDserver and Setting Up the Remote Luna PED

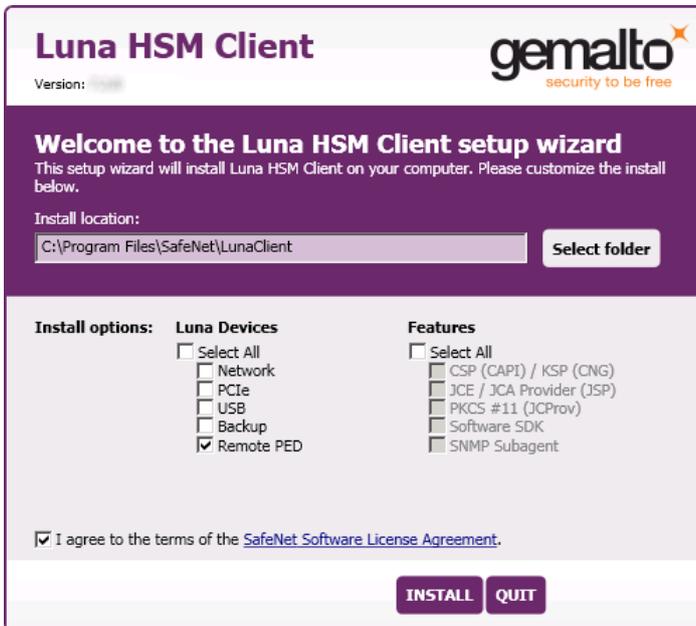
The PEDserver software, installed on the Remote PED host workstation, allows the USB-connected Luna PED to communicate with remotely-located HSMs. The Remote PED administrator can install PEDserver using the Luna HSM Client installer. You require:

- > Network-connected workstation with compatible operating system (refer to the release notes)
- > Luna HSM Client installer
- > SafeNet Luna PED with firmware 2.7.1 or higher
- > USB mini-B to USB-A connector cable
- > Luna PED DC power supply (PED 2.7.1 only; PED 2.8 and higher is powered by the USB connection)

**NOTE** To set up a Remote PED Server on Linux, you require Luna HSM Client 10.1 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](#)" on page 27, and select the **Luna Remote PED** option. Any additional installation choices are optional, for the purpose of this procedure.



2. On Windows, when you are prompted to install the driver, click **Install**.



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.

PED version 2.8 and above is powered via the USB connection. If you are using PED version 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 94](#).

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

**NOTE** For the SafeNet Luna Network HSM, 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 Network HSM 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.

If you encounter issues, see ["Remote PED Troubleshooting" on page 107](#).

The HSM/client administrator can use this procedure to establish an HSM-initiated Remote PED 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 102](#))
- > Administrative access to the SafeNet Luna PCIe HSM host via SSH
- > Orange PED key with the HSM's RPV (see ["Initializing the Remote PED Vector \(RPV\) and Creating an Orange Remote PED Key \(RPK\)" on page 101](#))

### To open a Remote PED connection

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 138 [-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 136**

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.**
- 6. Via SSH, launch LunaCM on the SafeNet Luna PCIe HSM host.**
- 7. Initiate the Remote PED connection.**

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

**NOTE** The **-slot** option may be required if you have multiple SafeNet Luna PCIe HSMs installed in one server. If you do not include this option, the currently-active slot is used.

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

```
Command Result : No Error
```

**8.** Issue the first command that requires authentication.

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

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

- If the HSM is uninitialized, you can initialize it now (see ["Initializing the HSM" on page 178](#)). Have blank or reusable blue and red PED keys ready (or multiple blue and red keys in case of M of N or if making multiple copies). See ["Creating PED Keys" on page 111](#) for more information.

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

**9.** 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.
```

**10.** 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 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 the next page](#).

**11.** [OPTIONAL] Set a default IP address and/or port for the SafeNet Luna PCIe HSM to look for a Remote PED host with PEDserver running.

```
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` to initiate the Remote PED connection. The orange PED key may be required if the RPK has been invalidated since you last used it.

## Ending or Switching the Remote PED Connection

PEDserver runs on the Remote PED host until explicitly stopped. PEDclient (running on the SafeNet Luna PCIe HSM host) has a default timeout period of 1800 seconds. 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 connection

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>`.

## 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:

- > ["No Menu Appears on PED Display: Ensure Driver is Properly Installed" below](#)
- > ["RC\\_SOCKET\\_ERROR: PEDserver Requires Administrator Privileges" below](#)
- > ["CKR\\_PED\\_UNPLUGGED: Reconnect Remote PED Before Issuing Commands" on the next page](#)
- > ["Remote PED Firewall Blocking" on the next page](#)
- > ["Remote PED Blocked Port Access" on page 110](#)
- > ["ped connect Fails if IP is Not Accessible" on page 110](#)
- > ["PEDserver on VPN fails" on page 110](#)

### No Menu Appears on 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 102](#).

### 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.

### CKR\_PED\_UNPLUGGED: Reconnect Remote PED Before Issuing Commands

As described in the connection procedures, Remote PED connections time out after a default period of 1800 seconds (30 minutes). If you attempt PED authentication 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:

```
lunacm:> role login -n so
```

```
Please attend to the PED.
```

```
Error in execution: CKR_PED_UNPLUGGED.
```

```
Command Result : 0x8000002e (CKR_PED_UNPLUGGED)
```

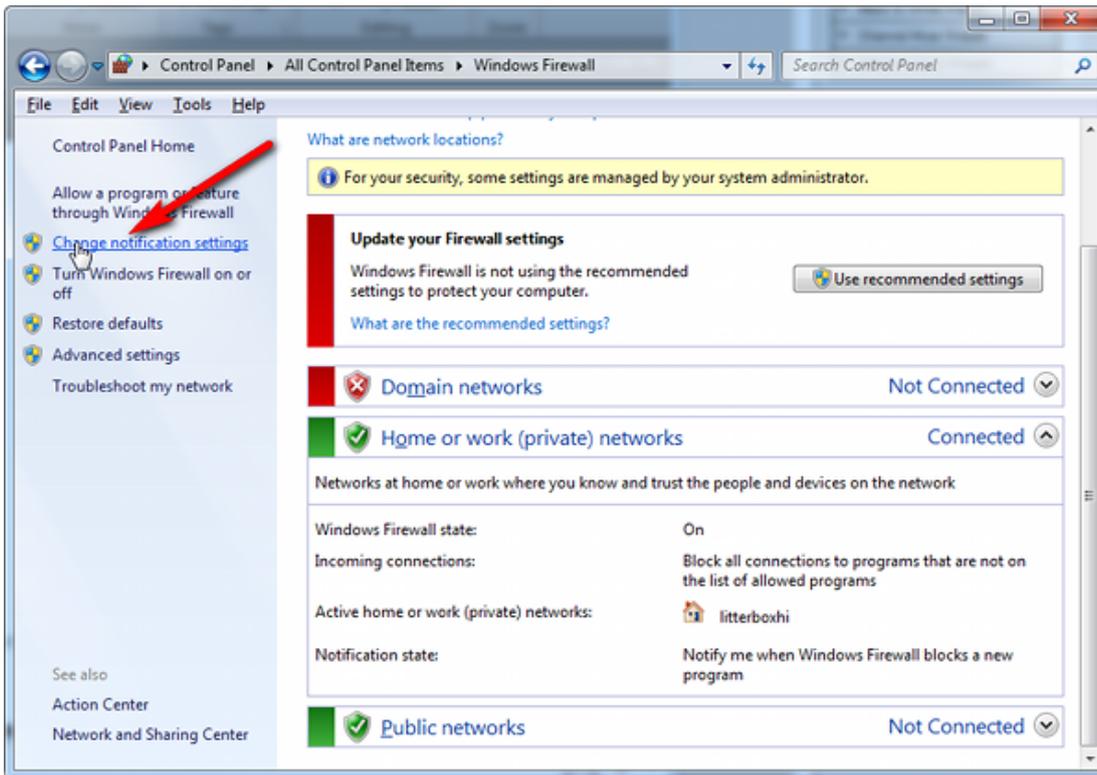
To avoid this error, re-initiate the connection before issuing any commands requiring PED authentication:

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

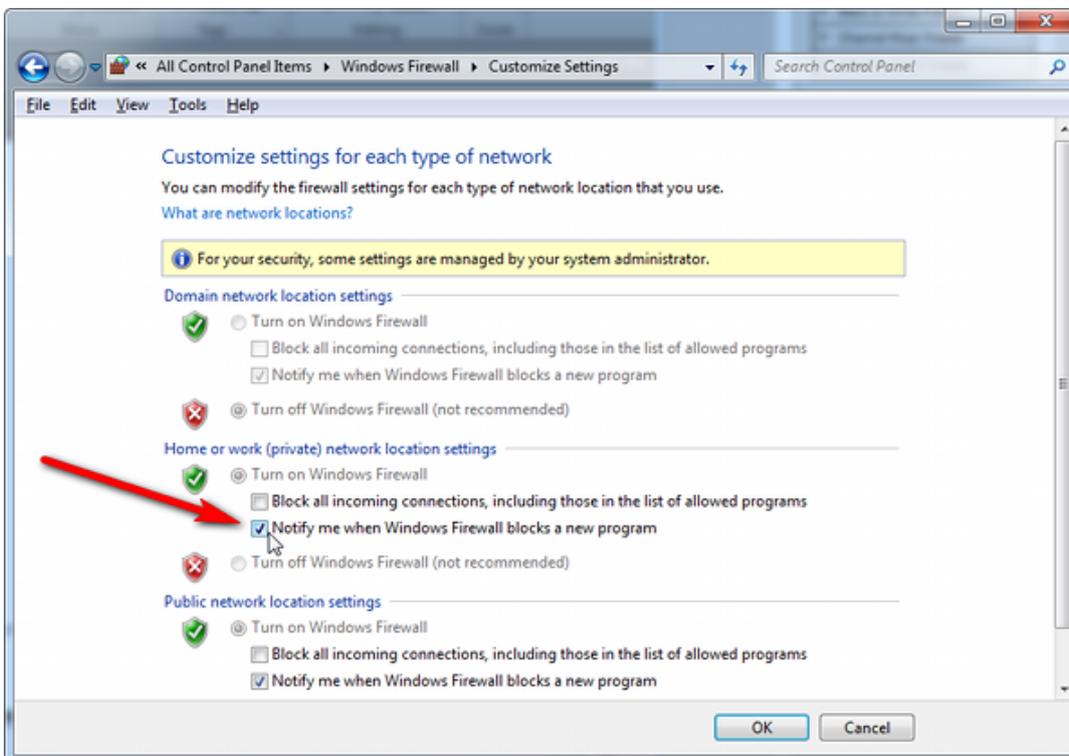
### Remote PED Firewall Blocking

If you experience problems while attempting to configure a SafeNet Remote PED session over VPN, you might need to adjust Windows Firewall settings.

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` 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 SafeNet Luna PCIe HSM(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. Launch LunaCM on the SafeNet Luna PCIe HSM host, and open the HSM-initiated connection.

```
lunacm:> 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 SafeNet Luna PCIe HSM 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 138 -ip <new\_IP> -port <port>**

## PED Key Management

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

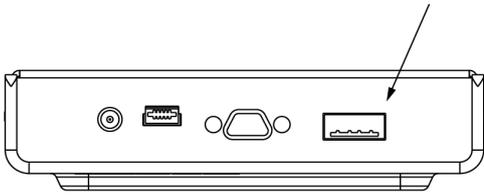
- > **"Creating PED Keys" below**
  - **"Stage 1: Reusing Existing PED Keys" on the next page**
  - **"Stage 2: Defining M of N" on page 114**
  - **"Stage 3: Setting a PED PIN" on page 114**
  - **"Stage 4: Duplicating New PED Keys" on page 115**
- > **"Performing PED Authentication" on page 116**
- > **"Consequences of Losing PED Keys" on page 118**
- > **"Identifying a PED Key Secret" on page 120**
- > **"Duplicating Existing PED Keys" on page 121**
- > **"Changing a PED Key Secret" on page 122**

### Creating PED Keys

When you initialize an HSM, partition, or role, the SafeNet 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 PED 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. 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 PED 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 LunaCM commands to initialize the applicable role, domain, or vector.

- **Blue HSM SO and Red HSM Domain Keys:**

```
lunacm:> hsm init
```

- **Orange Remote PED Key:**

```
lunacm:> ped vector init
```

- **Blue Partition SO and Red Partition Domain Keys:**

```
lunacm:> partition init
```

- **Black Crypto Officer Key:**

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

- **Gray Crypto User Key:**

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

- **White Audit User Key:**

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

The Luna PED responds, displaying:

```
Remote PED mode
Token found
```

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 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 87](#) and ["Domain PED Keys" on page 88](#) for more information.

1. The first 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 PED 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) 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 PED PIN](#)" below 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 "[M of N Split Secrets \(Quorum\)](#)" on page 88 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.

- 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
```

- 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
```

- Continue to "[Stage 3: Setting a PED PIN](#)" below. You must complete stage 3 for each key in the M of N scheme.

### Stage 3: Setting a PED PIN

If you are creating a new key or M of N split, you have the option of setting a PED PIN that must be entered by the key owner during authentication. PED PINs must be 4-48 digits long. Do not use 0 for the first digit. See "[PED PINs](#)" on page 88 for more information.

**CAUTION!** If you forget your PED PIN, it is the same as losing the PED key entirely; you cannot authenticate the role. See "[Consequences of Losing PED Keys](#)" on page 118.

- 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 PED 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 PED 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 PED PIN. Duplicates you create later are intended as backups, and will have the same PED 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 121.

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 PED PIN](#)" on page 114 for the duplicate keyset. You can set the same PED PIN to create a true copy, or set a different PED PIN for each duplicate.
2. If you specified an M of N scheme, you are prompted to repeat "[Stage 3: Setting a PED PIN](#)" on page 114 for each M of N split. Otherwise, the key creation process is complete.

## Performing PED Authentication

When connected, the SafeNet Luna PED responds to authentication commands in 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)

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

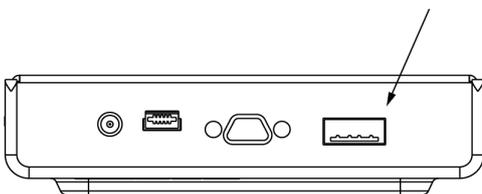
```
lunacm:>role login -name po
```

```
Please attend to the PED.
```

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 190](#) or [Logging In to the Application Partition](#).

## To perform PED authentication

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

```
Command Result : No Error
```

2. The PED prompts for the PED 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 PED PIN, return to step 2.

- Repeat steps 2 and/or 3 until the requisite M number of keys have been presented to the PED. At this point, authentication is complete and the PED returns control to the command interface.

Command Result : No Error

## Consequences of Losing PED Keys

PED keys are the only means of authenticating roles, domains, and RPVs on the PED-authenticated SafeNet Luna PCIe HSM. Losing a PED keyset effectively locks the user out of that role. Always keep secure backups of your PED keys, including M of N split secrets. Forgetting the PED 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 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 Key" below](#)
- > ["Red HSM Domain Key" on the next page](#)
- > ["Orange Remote PED Key" on the next page](#)
- > ["Blue Partition SO Key" on the next page](#)
- > ["Red Partition Domain Key" on the next page](#)
- > ["Black Crypto Officer Key" on the next page](#)
- > ["Gray Crypto User Key" on page 120](#)
- > ["White Audit User Key" on page 120](#)

### Blue HSM SO 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 Admin partition are unrecoverable. Take the following steps:

1. Contact all Crypto Officers and have them immediately make backups of their existing partitions.
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 Admin partition contents from a recent backup, if you have one.
5. Recreate the partitions and reassign them to their respective clients.
6. 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.
7. 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).
8. Crypto Officers can now restore all partition contents from backup.
9. If you are using Remote PED, you must recreate the Remote PED Vector (RPV). Reuse the original orange key.

### Red HSM Domain Key

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

### Orange Remote 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 \(RPV\) and Creating an Orange Remote PED Key \(RPK\)" on page 101](#).

### Blue Partition SO 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 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 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 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 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 a 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 PED PIN assigned
- > who the key belongs to

You require:

- > SafeNet Luna PED in Admin Mode (see ["Changing Modes" on page 94](#))
- > the key you want to identify

### To identify the type of secret stored on a 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 PED 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:

- > SafeNet Luna PED in Admin Mode (see ["Changing Modes" on page 94](#))
- > Enough blank or rewritable keys to make your copies

The PED key is duplicated exactly by this process. If there is a PED PIN assigned, the same PIN is assigned to the duplicate key. If the key is part of an 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 M of N keyset. See ["M of N Split Secrets \(Quorum\)" on page 88](#).

### 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 a PED Key Secret

It may be necessary to change the PED secret associated with a role. Reasons for changing credentials include:

- > Regular credential rotation as part of your organization's security policy
- > Compromise of a role 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, PED 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 PED 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 PED 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 Key" below](#)
- > ["Red HSM Domain Key" on the next page](#)
- > ["Orange Remote PED Key" on the next page](#)
- > ["Blue Partition SO Key" on the next page](#)
- > ["Red Partition Domain Key" on the next page](#)
- > ["Black Crypto Officer Key" on the next page](#)
- > ["Gray Crypto User Key" on page 124](#)
- > ["White Audit User Key" on page 124](#)

### Blue HSM SO 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 LunaCM, set the active slot to the Admin partition and login as HSM SO.

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

2. Initiate the PED key change.

```
lunacm:> role changepw -name so
```

3. You are prompted to present the original blue key(s) and then to create a new HSM SO keyset. See ["Creating PED Keys" on page 111](#).

### Red HSM Domain 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 Admin partition from backup.

### Orange Remote 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 LunaCM, set the active slot to the Admin partition and login as HSM SO.  
lunacm:> **role login -name so**
2. Initialize the RPV.  
lunacm:> **ped vector init**  
You are prompted to create a new Remote PED key.
3. Distribute a copy of the new orange key to the administrator of each Remote PED server.

### Blue Partition SO 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.

### Red Partition Domain Key

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.

### Black Crypto Officer 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.

### Gray Crypto User 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.

### White Audit User Key

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

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

1. In LunaCM, set the active slot to the Admin partition and login as Auditor.

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

2. Initiate the PED key change.

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

3. You are prompted to present the original white key(s) and then to create a new Audit User keyset.

## 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 SafeNet 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 SafeNet Luna Network HSM) is behind a firewall that forbids outgoing initiation of connections.

See "[pedserver](#)" on page 126.

## 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 SafeNet 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 G5 Remote Backup HSM Server](#) for more information.
- > It acts as the logging daemon for HSM audit logs.

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 [Configuring a G5 Remote Backup HSM Server](#) for more information.

See ["pedclient" on page 142](#).

## pedserver

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

**NOTE** The **pedserver** commands are available on Windows only.

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

### Syntax

#### pedserver

**appliance**  
**mode**  
**regen**

Option	Description
<b>appliance</b>	Registers or deregisters an appliance, or lists the registered appliances. Applies to server-initiated (peer-to-peer) mode only. See " <a href="#">pedserver appliance</a> " on the next page.
<b>mode</b>	Specifies the mode that the PED Server will be executed in. See " <a href="#">pedserver mode</a> " on page 131.
<b>regen</b>	Regenerates the client certificate. Applies to server-initiated (peer-to-peer) mode only. See " <a href="#">pedserver regen</a> " on page 142.

## 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 129.
<b>register</b>	Registers an appliance. See <a href="#">"pedserver appliance register"</a> on page 130

## 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 PED Server.
<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). <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 134.
<b>disconnect</b>	Disconnects from the appliance. See " <a href="#">pedserver mode disconnect</a> " on page 135.
<b>show</b>	Queries if PEDserver is currently running, and gets details about PEDserver. See " <a href="#">pedserver mode show</a> " on page 136.
<b>start</b>	Starts PEDserver. See " <a href="#">pedserver mode start</a> " on page 138.
<b>stop</b>	Shuts down PEDserver. See " <a href="#">pedserver mode stop</a> " on page 140

## 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>]  
[-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.

Option	Description
<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.
<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 to be 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 .

### Syntax

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

Option	Description
<b>-commonname</b> <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 145.</a>
<b>deleteid</b>	Deletes a PED ID mapping. See <a href="#">"pedclient mode deleteid" on page 147.</a>
<b>releaseid</b>	Releases a PED ID mapping from an HSM. See <a href="#">"pedclient mode releaseid" on page 148.</a>
<b>setid</b>	Creates a PED ID mapping. See <a href="#">"pedclient mode setid" on page 149.</a>
<b>show</b>	Queries if PEDclient is currently running and gets details about PEDclient. See <a href="#">"pedclient mode show" on page 150.</a>
<b>start</b>	Starts up PEDclient. See <a href="#">"pedclient mode start" on page 151.</a>
<b>stop</b>	Shuts down PEDclient. See <a href="#">"pedclient mode stop" on page 153.</a>
<b>testid</b>	Tests a PED ID mapping. See <a href="#">"pedclient mode testid" on page 154.</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 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 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 PED Server 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>] [-logfile <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>-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>-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 PED Client.

### 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 &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>-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.
<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 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 PED and PEDserver.

### Syntax

**pedclient mode testid -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 tested.
<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 testid -id 1234
```

# CHAPTER 6: 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:

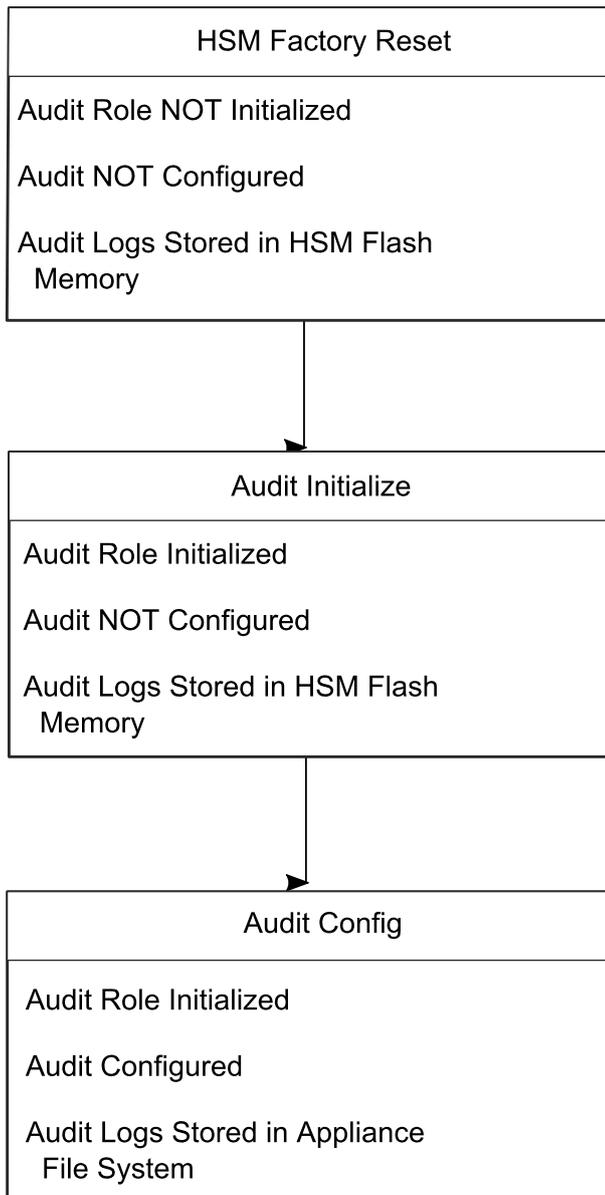
- > ["Audit Logging General Advice and Recommendations" on page 164](#)
- > ["Logging In as Auditor" on page 166](#)
- > ["Configuring and Using Audit Logging" on page 166](#)
- > ["Audit Log Categories and HSM Events" on page 170](#)
- > ["Audit Log Troubleshooting" on page 177](#)

## Audit Logging Features

The following list summarizes the functionality of the audit logging feature:

- > Log entries originate from the SafeNet Luna PCIe HSM - 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 SafeNet Luna PCIe HSM that is a member of the same domain.
- > Audit Logging can be performed on password-authenticated (FIPS 140-2 level 2) and PED-authenticated (FIPS 140-2 level 3) configurations, but these configurations may not validate each other's logs - see the "same domain" requirement, above.
- > 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 SafeNet Luna PCIe HSM 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
- > Log origin is assured.
- > 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 local file system, 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.

### 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

A SafeNet Luna PCIe HSM Audit role allows complete separation of Audit responsibilities from the Security Officer (SO or HSM Admin), the Partition User (or Owner), and other HSM roles. If the Audit role is initialized, the HSM and Partition administrators 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 LunaCM command **role init -name Auditor** to initialize the audit role, as described in ["role init" on page 1](#).

### Password-authenticated HSMs

For SafeNet Luna PCIe HSMs 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" on page 1](#) for the command syntax). This step is required

before setting logging parameters or the log filepath, or importing/exporting audit logs.

### PED-authenticated HSMs

For SafeNet Luna PCIe HSMs with PED 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 PED-authenticated HSMs) does not require the presence or cooperation of the HSM SO.

### Audit Role Available Commands

In LunaCM, all commands are visible to the person who launches the utility, and some can be used without specific authentication to the HSM, such as view/show/list commands, which might be classified as "monitoring" functions. Attempts to run operational or administrative commands that need role-specific authentication, without that authentication, result in an error message. The Audit role has a limited set of operations available to it, on the HSM, which constitutes any of the generally accessible monitoring commands, plus everything under the "audit" heading.

```
lunacm:>audit
```

The following sub commands are available:

Command	Short	Description
verify	v	Verify a block of log messages
config	c	Configure audit parameters
export	e	Read the wrapped log secret from the HSM
import	m	Import the wrapped log secret to the HSM
time	t	Sync HSM time to host, or get HSM time
status	s	Show status of logging subsystem
logmsg	logm	Write a message to the HSM's log

Syntax: audit <sub command>

Command Result : No Error

Anyone accessing the computer and running LunaCM can see the above commands, but cannot run them if they do not have the "audit" role authentication (password or PED key, as appropriate).

What is important is not the role you can access on the computer (a named user, admin, root), but the role you can access within the HSM.

## 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
350	1	Comma



## Log Capacity

The log capacity of SafeNet Luna PCIe HSMs varies depending upon the physical memory available on the device.

The HSM has approximately 16 MB available for Audit logging (or more than 200,000 records, depending on the size/content of each record).

The normal function of Audit logging is to export log entries constantly to the file system. Short-term, within-the-HSM log storage capacity becomes important only in the rare situations where the HSM remains functioning but the file system is unreachable from the HSM.

### LOG FULL condition

In the case of a log full condition on the host, most commands will return CKR\_LOG\_FULL. There are a few exceptions to this, as follows:

- > factory reset
- > zeroize
- > login as audit user
- > logout
- > initialize PIN for audit user
- > open session
- > close session
- > get audit config
- > set audit config

Since the “log full” condition can make the HSM unusable, these commands are required to be able to login as the audit user and disable logging, even if logging for those commands is enabled; and the log is full. All other commands will not execute if their results are supposed to be logged, but can't be, due to a log full condition.

If you receive CKR\_LOG\_FULL, then the HSM has filled its log space and is unable to export to the file system. Ensure that you have set **audit config** correctly. In particular:

- > filepath points to an existing location (no typos or other errors in specifying the filepath for log files)
- > writing to that location is permitted (check the folder/directory permissions)
- > the indicated location has sufficient space available to write log files (make some room if necessary).

## 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 SO cannot modify the logging configuration, and therefore cannot hide any activity from auditors.

## Audit Logging Stops Working if the Current Log File is Deleted

As a general rule, you should not delete a file while it is open and in use by an application. In Linux, deletion of a file is deletion of an inode, but the actual file itself, while now invisible, remains on the file system until the space is cleaned up or overwritten. If a file is in use by an application - such as audit logging, in this case - the application can continue using and updating that file, unaware that it is now in deleted status.

If you delete the current audit log file, the audit logging feature does not detect that and does not create a new file, so you might lose log entries.

The workaround is to restart the **pedclient** daemon, which creates a new log file.

### Example

1. You've configured audit logging, and the entire audit path is deleted. In Linux, the file isn't actually deleted until the last reference to the file has been destroyed. Since the pedclient has the file open, logging will continue, because technically the log file still exists. Applications, including the pedclient, will have no idea that anything is wrong.
2. On stopping the pedclient, the log file is deleted. When the pedclient gets started again, the HSM tries to tell the pedclient to use the old path. This path doesn't exist anymore, so it will not be able to offload log messages. At this point, it starts storing log messages internally. With 16 MB of Flash dedicated to this purpose, that works out to 198,120 messages max. This can actually fill up very quickly, in as little as a few minutes under heavy load.
3. At this point the user must set the audit log path to a valid value. and the HSM will offload all stored log messages to the host. This will take a couple of minutes, during which time the HSM will be unresponsive.
4. Once all messages have been offloaded, normal operation resumes with messages being sent to the host (i.e. not being stored locally).

## 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 Network HSM 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 `lunacm:> audit time sync` command at least once every 24 hours, provided the host has maintained its connection(s) to its configured NTP server(s).
- > 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.
- > 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.

## 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 logger daemon (**PEDclient**).
  - > "[pedclient mode stop](#)" on page 153
  - > "[pedclient mode start](#)" on page 151

To prevent the "disk full" situation, we recommend that the audit user routinely archive the audit logs and clear the audit log directory.

## 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 to the SafeNet Luna PCIe HSM's Admin partition as Auditor (AU), or relevant commands will fail.

### To log in as Auditor

1. Launch LunaCM on the SafeNet Luna PCIe HSM host workstation.
2. Set the active slot to the HSM Admin partition.

```
lunacm:> slot set -slot <slotnum>
```

3. Log in as Auditor.

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

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 a 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 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](#)
- > ["Exporting the Audit Logging Secret and Importing to a Verifying HSM" on page 168](#)
- > ["Reading the Audit Log Records" on page 169](#)
- > ["Audit Role Authentication Considerations" on page 170](#)

### Configuring Audit Logging

Configure audit logging using the LunaCM **audit** commands.

#### To configure audit logging:

1. Configure the SafeNet Luna PCIe HSM host computer to use network time protocol (NTP).
2. Ensure that the PEDclient service is running:

See ["pedclient mode show" on page 150](#) and ["pedclient mode start" on page 151](#).

- Set the slot focus to the HSM administrative partition of the desired HSM:

```
lunacm:> slot set -slot <slotnum>
```

- Initialize the Auditor role (you can also use the shortcut **au**):

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

- On password-authenticated HSMs, you are prompted for a password.
- On PED-authenticated HSMs, you are referred to Luna PED, which prompts for a white PED key.

- Now that the Auditor role exists on the HSM, the auditing function must be configured. However, before you can configure you must log in as the Auditor user (you can also use the shortcut **au**):

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

- On password-authenticated HSMs, you are prompted to enter the password for the Auditor user.
- On PED-authenticated HSMs, you are referred to Luna PED, which prompts for the white PED key for the Auditor user.

- Set the domain for the Audit role:

```
lunacm:> role setdomain
```

- 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.

```
lunacm:> audit time sync
```

- Set the filepath where log files are to be saved. You must complete this step before you can start event logging.

```
lunacm:> audit config path <filepath>
```

If you previously configured logging on the HSM and then made changes to your configuration that made that path invalid (such as deleting the path outside of LunaCM or reinstalling the HSM in a different host system), set a valid log path by running **audit config path** before restarting event logging. If the log path is set incorrectly, logs will be stored in the HSM's limited memory and not exported to the file system. Event logs may be lost if the HSM's memory runs out.

- 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:

```
lunacm:> audit config evmask <event_value>
```

**NOTE** Before you configure audit logging, we suggest using **audit config ?** 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 Auditor 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 Auditors 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, the command **audit config evmask all** will log everything the HSM does. This might be useful in some circumstances, but will quickly fill up log files.

10. Configure audit logging to specify how often you want to rotate the logs. Log entries are made within the HSM, and are written to the currently active log file. 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 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.

- a. Specify the rotation interval. You can rotate the logs hourly, daily, weekly, monthly, or never.

```
lunacm:> audit config interval <value>
```

- b. Specify the maximum log file size. When the log reaches the maximum size, it is automatically rotated, regardless of rotation interval:

```
lunacm:> audit config size <size>
```

For example, the commands **audit config interval daily** and **audit config size 4m** would rotate the logs every day, unless they reached a size of 4 Mb first, in which case they would be rotated automatically. The daily rotation would still occur.

See **audit config** for additional examples.

## 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 SafeNet Luna PCIe HSM using a SafeNet Luna Network HSM, and vice-versa.

### To export the Audit Logging secret from the HSM and import to the verifying HSM:

1. Export the audit logging secret to the user local directory. The file is written to the subdirectory specified by a previous **audit config path** command.

```
lunacm:> audit export file <filename>
```

2. Exit LunaCM and list the contents of the **lunalog** directory to see the filename of the wrapped log secret:

<b>Linux</b>	<pre>ls &lt;client_install_dir&gt;/lunalog 123456 7001347 123456.lws</pre>
<b>Windows</b>	<pre>dir &lt;client_install_dir&gt;\lunalog 04/12/2017 03:56 PM &lt;DIR&gt; 123456 04/05/2017 02:35 PM &lt;DIR&gt; 7001347 04/05/2017 02:35 PM 48 123456.lws</pre>

3. Transfer the logging secret to the HSM that will verify the logs. If you are verifying the logs with another locally-installed SafeNet Luna PCIe HSM, skip this step.

- If you are planning to verify logs with a SafeNet Luna PCIe HSM, use **pscp** or **scp** to transfer the logging secret to the appliance. Provide the audit user's credentials when prompted.  
`<client_install_dir>:>pscp <log_secret_file> audit@<hostname_or_IP>: .`
  - If you are planning to verify logs with a SafeNet Luna PCIe HSM installed in a different host computer, you can use **scp**, **pscp**, or other secure means to transfer the logging secret.  
`<client_install_dir>:>pscp <log_secret_file> <user>@<hostname_or_IP>: .`
4. 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 SafeNet Luna Network HSM, connect via SSH and log in to LunaSH as the **audit** user:  
`lunash:> audit login`
  - If you are using a SafeNet Luna PCIe HSM, open LunaCM and log in using the Auditor role:  
`lunacm:> role login -name au`
5. Import the audit logging secret to the HSM.
- SafeNet Luna Network HSM (LunaSH):  
`lunash:> audit secret import -serialtarget <target_HSM_SN> -serialsource <source_HSM_SN> -file <log_secret_file>`
  - SafeNet Luna PCIe HSM (LunaCM):  
`lunacm:> audit import file <log_secret_file>`
6. You can now verify audit log files from the source HSM.
- SafeNet Luna Network HSM (LunaSH):  
`lunash:> audit log verify -file <audit_log_filename>.log`
  - SafeNet Luna PCIe HSM (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.

**NOTE** Linux users, if you notice that audit log messages are going to more than one location on your file system, you can edit the `/etc/rsyslog.conf` file to prevent reporting `local3.info` messages in `/var/log/messages` as follows:

```
//Log anything (except local3 and mail) of level info or higher.
*.info;local3.none;mail.none;authpriv.none;cron.none
/var/log/messages
```

The portion highlighted in red stops the duplication of output. This change is optional.

## Reading the Audit Log Records

In general, the audit logs are self-explanatory. Due to limitations in the firmware, however, some audit log records required further explanation, as detailed in the following sections:

## Determining the serial number of a created partition from the audit log

An audit log entry similar to the following is generated when a partition is created on the HSM:

```
5,12/12/17 16:14:14,S/N 150718 session 1 Access 2147483651:2669 SO container operation LUNA_
CREATE_CONTAINER
```

```
returned RC_OK(0x00000000) container=20 (using PIN (entry=LUNA_ENTRY_DATA_AREA))
```

It is not obvious from this entry what the serial number is for the created partition. This information, however, can be derived from the log entry, since the partition serial number is simply a concatenation of the HSM serial number and the partition container number, which are specified in the log entry, as highlighted below:

```
5,12/12/17 16:14:14,S/N 150718 session 1 Access 2147483651:2669 SO container operation LUNA_
CREATE_CONTAINER
```

```
returned RC_OK(0x00000000) container=20 (using PIN (entry=LUNA_ENTRY_DATA_AREA))
```

In the example above, the HSM serial number is 150718 and the partition container number is 20. Note that the partition container number is a three-digit number with leading zeros suppressed, so that the actual partition container number is 020. To determine the partition serial number concatenate the two numbers as follows:

```
150718020
```

Use this number to identify the partition in subsequent audit log entries.

## 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 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.

## Audit Log Categories and HSM Events

This section provides a summary of the audit log categories and their associated HSM events.

### HSM Access

HSM Event	Description
LUNA_LOGIN	C_Login. 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. This event must be allowed to proceed even if the result should be logged but cannot (for example, due to a log full condition).

HSM Event	Description
LUNA_MODIFY_OBJECT	C_SetAttributeValue
LUNA_OPEN_SESSION	C_OpenSession. 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 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
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, CA_HAAnswerLoginChallenge, CA_HALogin, CA_HAAnswerMofNChallenge, HAActivateMofN

## Log External

HSM Event	Description
LUNA_LOG_EXTERNAL	CA_LogExternal

## HSM Management

HSM Event	Description
LUNA_ZEROIZE	CA_FactoryReset This event is logged unconditionally.
LUNA_INIT_TOKEN	C_InitToken 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
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

HSM Event	Description
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
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

HSM Event	Description
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
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, CA_LKMReceiverResponse, CA_LKMInitiatorComplete, 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

HSM Event	Description
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
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

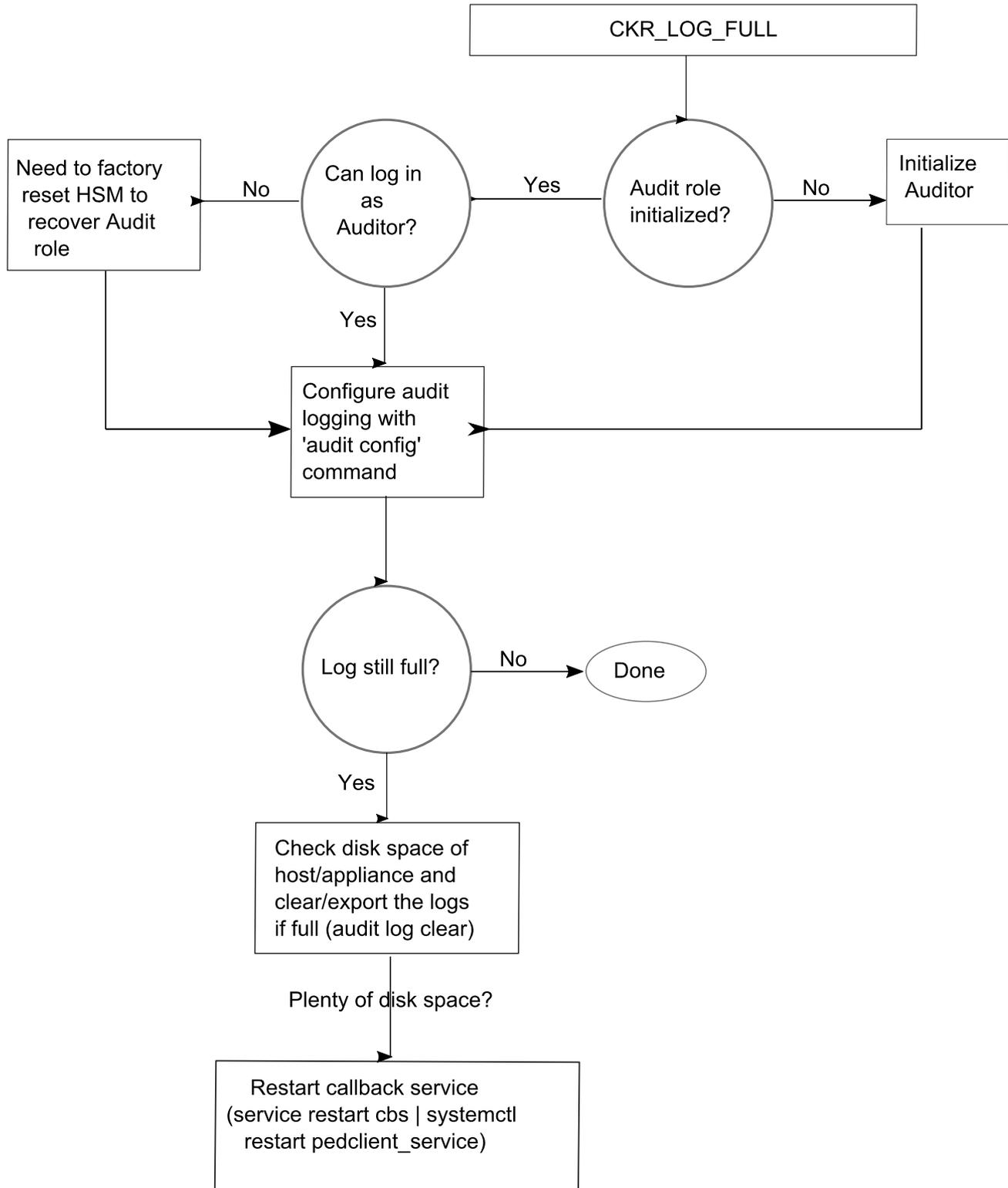
## Audit Log Management

HSM Event	Description
LUNA_LOG_SET_TIME	CA_TimeSync

HSM Event	Description
LUNA_LOG_GET_TIME	CA_GetTime
LUNA_LOG_SET_CONFIG	CA_LogSetConfig 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 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 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 7: 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 181](#).

**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 80](#) for details.

On a new, or factory-reset HSM (using **hsm factoryreset**), the following attributes are set during a hard initialization:

<p><b>HSM Label</b></p>	<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. The following characters are allowed:  <code>abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789 !@#\$%^&amp;* () - _ = + [ ] { } \   / ; : ' " , . &lt; &gt; ? ` ~</code></p> <p>Spaces are allowed; enclose the label in double quotes if it includes spaces. Including both spaces and quotation marks in a label may cause unexpected labeling behavior.</p> <p>For more information, refer to <a href="#">"Name, Label, and Password Requirements" on page 191</a>.</p>
<p><b>HSM SO credentials</b></p>	<p>For Multi-factor, or PED-authenticated HSMs, you create a new HSM SO (blue) PED key(set) or re-use an existing key(set) from an HSM you want to share credentials with. If you are using PED authentication, ensure that you have a PED key strategy before beginning. See <a href="#">"PED Authentication" on page 84</a>.</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 LunaCM, passwords and activation challenge secrets must be 7-255 characters in length (<b>NOTE:</b> If you are using firmware version 7.0.1, 7.0.2, 7.0.3, 7.3.3, or 7.4.2, activation challenge secrets must be 7-16 characters in length). The following characters are allowed:  <code>abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789 !@#\$%^&amp;* () - _ = + [ ] { } \   / ; : ' " , . &lt; &gt; ? ` ~</code></p> <p>Double quotation marks (") are problematic and should not be used in passwords.</p> <p>Spaces are allowed; to specify a password with spaces using the <b>-password</b> option, enclose the password in double quotation marks.</p>
<p><b>Cloning domain for the HSM Admin partition</b></p>	<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 Multi-factor, PED-authenticated HSMs, you create a new Domain (red) PED key(set) or re-use an existing 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:  <code>abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789 !@#\$%^&amp;* - _ = + [ ] { } / ; : ' , . ~</code></p> <p>The following characters are problematic or invalid and must not be used in a domain string: <code>" &amp; ; &lt; &gt; \ `   ( )</code></p> <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>

## To initialize a new or factory-reset HSM

1. Open a LunaCM session and set the active slot to the HSM Admin partition.

2. If Secure Transport Mode is set, you must unlock the HSM before proceeding. New SafeNet 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 80](#) for more information.

To recover your HSM from Secure Transport Mode, proceed as follows:

- a. 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

- b. Ensure that you have the Random User String and Verification String that were emailed to you for your new HSM.
  - c. Enter the following command to recover from STM, specifying the Random User String that was emailed to you for your new HSM:
- ```
lunacm:> stm recover -randomuserstring <XXXX-XXXX-XXXX-XXXX>
```
- d. 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 Group Technical Support immediately.
  - e. Enter **proceed** to recover from STM (regardless of whether the strings match or not), or enter **quit** to remain in STM.
3. If you are initializing a Multi-factor-authentication (PED-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 94](#). Alternatively, have a Remote PED instance set up, see ["About Remote PED" on page 97](#).
  4. Run the **hsm init** command, specifying a label for your SafeNet Luna PCIe HSM:

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

5. 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 Multi-factor-authenticated (PED-authenticated) HSM, you are prompted to attend to the 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 PED 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 ["PED Authentication" on page 84](#) for more information.

The prompts are self-explanatory. New users (especially those initializing a PED-authenticated HSM) may want to refer to the following examples for more information:

- ["PED-authenticated HSM Initialization Example" on the next page](#)
- ["Password-authenticated HSM Initialization Example" on page 187](#)

## 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 178](#).

**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. Open a LunaCM session and set the slot to the HSM Admin partition.
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 80](#).
4. If you are initializing a PED-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 94](#).
5. Re-initialize the HSM, specifying a label for your SafeNet Luna PCIe HSM:

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

## PED-authenticated HSM Initialization Example

This section provides detailed examples that illustrate your options when initializing a PED-authenticated HSM. It provides the following information:

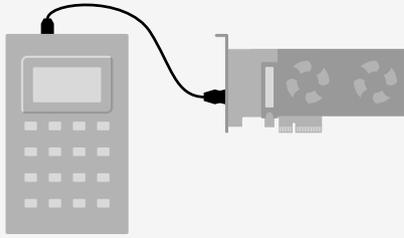
- > ["To initialize a PED-authenticated HSM" below](#)
- > ["Imprinting the Blue HSM SO PED Key" on page 183](#)
- > ["Imprinting the Red Cloning Domain PED Key" on page 185](#)
- > ["New, reuse, and overwrite options" on page 185](#)

**NOTE** Respond promptly to avoid PED timeout Error. If the PED has timed out, press the **CLR** key for five seconds to reset, or switch the PED off, and back on, to get to the "Awaiting command..." state before re-issuing a LunaSH command that invokes the PED.

### To initialize a PED-authenticated HSM

1. Your Luna PED must be connected to the HSM, either locally/directly in USB mode (see ["Changing Modes" on page 94](#)), or remotely via Remote PED connection (see ["About Remote PED" on page 97](#)).

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



2. Set the active slot to the SafeNet Luna PCIe HSM Admin partition, and issue the **hsm init** command. The HSM passes control to the Luna PED, and the command line directs you to attend to the PED prompts.
3. When you issue the **hsm init** command, the HSM passes control to the Luna PED, and the command line (lunash:>) directs you to attend to the PED prompts.
4. A "default" login is performed, just to get started (you don't need to supply any authentication for this step).
5. Luna PED asks: "Do you wish to reuse an existing keyset?". If the answer is **No**, the HSM creates a new secret which will reside on both the HSM and the key (or keys) that is (or are) about to be imprinted. If the answer is **Yes**, then the HSM does not create a new secret and instead waits for one to be presented via the PED.
6. Luna PED requests a blue PED key. It could be blank to begin with, or it could have a valid secret from another HSM (a secret that you wish to preserve), or it could have a secret that is no longer useful.
7. Luna PED checks the key you provide. If the PED key is not blank, and your answer to "...reuse an existing keyset" was **Yes**, then Luna PED proceeds to copy the secret from the PED key to the HSM.
8. If the key is not blank, and your answer to "...reuse an existing keyset" was **No**, then the PED inquires if you wish to overwrite its contents with a new HSM secret. If the current content of the key is of no value, you say **Yes**. If the current content of the key is a valid secret from another HSM (or if you did not expect the key to hold any data) you can remove it from the PED and replace it with a blank key or a key containing non-useful data, before you answer **Yes** to the 'overwrite' question.
9. Assuming that you are using a new secret, and not reusing an existing one, Luna PED asks if you wish to split the new HSM secret. It does this by asking for values of "M" and "N". You set those values to "1" and "1" respectively, unless you require MofN split-secret, multi-person quorum access control for your HSM (See ["M of N Split Secrets \(Quorum\)" on page 88](#) for details).
10. Luna PED asks if you wish to use a PED PIN (an additional secret; see ["PED Key Management" on page 111](#) for more info).
11. If you just press **Enter** (effectively saying 'no' to the PED PIN option), then the secret generated by the HSM is imprinted on the PED key, that same secret is retained as-is on the HSM, and the same secret becomes the piece needed to unlock the Security Officer/HSM Admin account on the HSM.
12. If you press some digits on the PED keypad (saying 'yes' to the PED PIN option), then the PED combines the HSM-generated secret with your PED PIN and feeds the combined data blob to the HSM. The HSM throws away the original secret and takes on the new, combined secret as its SO/HSM Admin secret.
13. The PED key contains the original HSM-generated secret, but also contains the flag that tells the PED whether to demand a PED PIN (which is either no digits, or a set of digits that you supplied, and must supply at all future uses of that PED key).

14. Luna PED gives you the option to create some duplicates of this imprinted key. You should make at least one duplicate for backup purposes. Make additional duplicates if your security policy permits, and your procedures require them.
15. Next, Luna PED requests a red Domain PED key. The HSM provides a cloning Domain secret and the PED gives you the option to imprint the secret from the HSM, or to use a domain that might already be on the key. You choose appropriately. If you are imprinting a new Domain secret, you have the same opportunities to split the secret, and to apply a PED PIN "modifier" to the secret. Again, you are given the option to create duplicates of the key.
16. At this point, the HSM is initialized and Luna PED passes control back to LunaCM.

Further actions are needed to prepare for use by your Clients, but you can now log in as SO/HSM Admin and perform HSM administrative actions.

### Imprinting the Blue HSM SO PED Key

1. Decide if you want to reuse a keyset.

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

- If you say **No** (on the PED keypad), then you are indicating there is nothing of value on your PED keys to preserve, or you are using blank keys.
- If you say **Yes**, you indicate that you have a PED key (or set of PED keys) from another HSM and you wish your current/new HSM to share the authentication with that other HSM. Authentication will be read from the PED key that you present and imprinted onto the current HSM.

2. Set MofN.

```
SLOT
SETTING SO PIN...
M value? (1-16)
>00
```

```
SLOT
SETTING SO PIN...
N value? (M-16)
>00
```

- Setting M and N to **1** means that the role authentication is not to be split, and only a single PED key will be necessary when the authentication is called for in future. Input **1** for each prompt if you do not want to use MofN.
- Setting M and N to larger than 1 sets a quorum requirement for the role, which means that the authentication is split into N different splits, of which quantity M of them (the quorum) must be presented each time you are required to authenticate. MofN allows you to enforce multi-person access control - no single person can access the HSM without cooperation of a quorum of other holders.

3. Insert your blank key or the key you wish to overwrite.

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

Insert a blue HSM Admin/SO PED key and press **Enter**.

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

- **Yes:** If the PED should overwrite the PED key with a new SO authentication. If you overwrite a PED key that contains authentication secret for another HSM, then this PED key will no longer be able to access the other HSM, only the new HSM that you are currently initializing with a new, unique authentication secret .
  - **No:** If you have changed your mind or inserted the wrong PED key.
4. For any situation other than reusing a keyset, Luna PED now prompts for you to set a PED PIN. For multi-factor authentication security, the physical PED key is "something you have." You can choose to associate that with "something you know," in the form of a multi-digit PIN code that must always be supplied along with the PED key for all future HSM access attempts.

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

Type a numeric password on the PED keypad, if you wish. Otherwise, just press **Enter** twice to indicate that no PED PIN is desired.

5. Decide if you want to duplicate your keyset.

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

- **Yes:** Present one or more blank keys, all of which will be imprinted with exact copies of the current PED key's authentication.
- **No:** Do not make any copies.

**NOTE** You should always have backups of your imprinted PED keys, to guard against loss or damage.

## Imprinting the Red Cloning Domain PED Key

To begin imprinting a Cloning Domain (red PED key), you must first log into the HSM. Insert your blue SO PED key.

1. Decide if you want to reuse a keyset.

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

- **No:** If this is your first SafeNet Luna HSM, or if this HSM will not be cloning objects with other HSMs that are already initialized
  - **Yes:** If you have another HSM and wish that HSM and the current HSM to share their cloning Domain.
2. Set MofN.
    - Setting M and N to **1** means that the domain authentication is not to be split, and only a single PED key will be necessary when the authentication is called for in future. Input **1** for each prompt if you do not want to use MofN.
    - Setting M and N to larger than 1 sets a quorum requirement for the domain, which means that the authentication is split into N different splits, of which quantity M of them (the quorum) must be presented each time you are required to provide the domain. MofN allows you to enforce multi-person access control - no single person can access the HSM without cooperation of a quorum of other holders.
  3. Insert your blank key or the key you wish to overwrite.
  4. Optionally set a PED PIN.
  5. Decide if you want to duplicate your keyset.

Once you stop duplicating the Domain key, or you indicate that you do not wish to make any duplicates, Luna PED goes back to "Awaiting command...". LunaSH says:

```
Command Result : No Error
```

## New, reuse, and overwrite options

The table below summarizes the steps involving Luna PED immediately after you invoke the command **hsm init**. The steps in the table are in the order in which they appear as PED prompts, descending down the column.

The first column is the simplest, and most like what you would encounter the very first time you initialize, using "fresh from the carton" PED keys.

The next two columns of the table show some differences if you are using previously-imprinted PED keys, choosing either to reuse what is found on the key (imprint it on your new HSM - see "[Shared PED Key Secrets](#)" on page 87) or, to overwrite what is found and generate a new secret to be imprinted on both the PED key and the HSM.

| New PED Keys                                                                                                                                                         | Existing PED Keys (Reuse)                                                                                                                                            | Existing PED Keys (Overwrite)                                                                                                                                        |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| SLOT 01<br>SETTING SO PIN...<br>Would you like to reuse an existing keyset? (Y/N)<br><b>No</b>                                                                       | SLOT 01<br>SETTING SO PIN...<br>Would you like to reuse an existing keyset? (Y/N)<br><b>Yes</b>                                                                      | SLOT 01<br>SETTING SO PIN...<br>Would you like to reuse an existing keyset? (Y/N)<br><b>No</b>                                                                       |
| SLOT 01<br>SETTING SO PIN...<br>Insert a SO / HSM Admin PED Key<br>Press ENTER.                                                                                      | SLOT 01<br>SETTING SO PIN...<br>Insert a SO / HSM Admin PED Key<br>Press ENTER.                                                                                      | Slot 01<br>SETTING SO PIN...<br>Insert a SO / HSM Admin PED Key<br>Press ENTER.                                                                                      |
| This PED Key is blank.<br>Overwrite? (YES/NO)<br><b>Yes</b>                                                                                                          | ****Warning!****<br>This PED Key is for SO / HSM Admin<br>Overwrite? (YES/NO)<br><b>No</b>                                                                           | ****Warning!****<br>This PED Key is for SO / HSM Admin<br>Overwrite? (YES/NO)<br><b>Yes</b>                                                                          |
| Enter a new PED PIN<br>Confirm new PED PIN<br>> Press <b>Enter</b> for no PED PIN<br>OR<br>> Input 4-16 digits on the PED keypad and press <b>Enter</b>              | Enter a new PED PIN<br>Confirm new PED PIN<br>> Press <b>Enter</b> for no PED PIN<br>OR<br>> Input 4-16 digits on the PED keypad and press <b>Enter</b>              | Enter a new PED PIN<br>Confirm new PED PIN<br>> Press <b>Enter</b> for no PED PIN<br>OR<br>> Input 4-16 digits on the PED keypad and press <b>Enter</b>              |
| Are you duplicating this keyset?<br>YES/NO<br>> <b>Yes:</b> duplicate. This option can be looped for as many duplicates as you need<br>> <b>No:</b> do not duplicate | Are you duplicating this keyset?<br>YES/NO<br>> <b>Yes:</b> duplicate. This option can be looped for as many duplicates as you need<br>> <b>No:</b> do not duplicate | Are you duplicating this keyset?<br>YES/NO<br>> <b>Yes:</b> duplicate. This option can be looped for as many duplicates as you need<br>> <b>No:</b> do not duplicate |
| Login SO / HSM Admin...<br>Insert a SO/ HSM Admin PED Key<br>Press ENTER                                                                                             | Login SO / HSM Admin..<br>Insert a SO/ HSM Admin PED Key<br>Press ENTER                                                                                              | Login SO / HSM Admin..<br>Insert a SO/ HSM Admin PED Key<br>Press ENTER                                                                                              |

| New PED Keys                                                                                                                                | Existing PED Keys (Reuse)                                                                                                                                                           | Existing PED Keys (Overwrite)                                                                                                                                                       |
|---------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| SETTING DOMAIN...<br>Would you like to reuse an existing keyset? (Y/N)<br>> <b>Yes</b> (unless you have good reason to create a new domain) | SETTING DOMAIN...<br>Would you like to reuse an existing keyset? (Y/N)<br>> <b>Yes</b> : make this HSM part of an existing domain<br>> <b>No</b> : create a new domain for this HSM | SETTING DOMAIN...<br>Would you like to reuse an existing keyset? (Y/N)<br>> <b>Yes</b> : make this HSM part of an existing domain<br>> <b>No</b> : create a new domain for this HSM |

## Password-authenticated HSM Initialization Example

```
lunash:>hsm init -label myLunaHSM
```

```
Please enter a password for the HSM Administrator:
> *****
```

```
Please re-enter password to confirm:
> *****
```

```
Please enter a cloning domain to use for initializing this HSM:
> *****
```

```
Please re-enter cloning domain to confirm:
> *****
```

CAUTION: Are you sure you wish to initialize this HSM?

```
Type 'proceed' to initialize the HSM, or 'quit'
to quit now.
> proceed
```

'hsm init' successful.

Command Result : 0 (Success)

```
lunacm:>hsm init -label myLunaHSM
```

```
You are about to initialize the HSM.
All contents of the HSM will be destroyed.
```

Are you sure you wish to continue?

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

```
Enter password for SO: *****
```

```
Re-enter password for SO: *****
```

Option -domain was not specified. It is required.

```
Enter the domain name: *****
```

Re-enter the domain name: \*\*\*\*\*

Command Result : No Error

When activity is complete, the system displays a “success” message.

# CHAPTER 8: 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 host system, 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.

SafeNet Luna PCIe HSM 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 the HSM roles described below access HSM functions by logging in to the Admin partition on the HSM using LunaCM. They must therefore have the appropriate Administrator access to the workstation hosting the SafeNet Luna PCIe HSM.

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 178](#))
- > Setting and changing global HSM policies (see ["HSM Capabilities and Policies" on page 193](#))
- > Creating/deleting the application partition (see ["Creating or Deleting an Application Partition" on page 204](#))
- > Updating the HSM firmware (see [Updating the SafeNet Luna PCIe HSM or SafeNet Luna Backup HSM Firmware](#))

### 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 a Role Credential" on page 191](#)

## 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

### Managing the Auditor Role

Refer to ["Configuring and Using Audit Logging" on page 166](#) for procedures involving the Auditor role. See also:

- > ["Logging In as Auditor" on page 166](#)
- > ["Changing a Role Credential" on the next page](#)

### Administrator (AD)

The HSM Administrator is a deprecated role on the Admin partition whose functions are now served by the application partition roles (see [Partition Roles](#)). Initializing this role is not recommended.

## 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 to the SafeNet Luna PCIe HSM's Admin partition as HSM Security Officer (SO), or administrative commands will fail.

### To log in as HSM SO

1. Launch LunaCM on the SafeNet Luna PCIe HSM host workstation.
2. Set the active slot to the HSM Admin partition.
3. Log in as HSM SO.

```
lunacm:> slot set -slot <slotnum>
```

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

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 a 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 to fail a login attempt.

## Changing a Role Credential

From time to time, you may need to change the credential for a role. The credential might have been compromised, or your organization's security policy may mandate password changes after a specific time interval. The following procedure allows you to change the credential for a role (HSM SO, Auditor, Partition SO, Crypto Officer, Crypto User). You must first log in using the role's current credential.

**NOTE** If **partition policy 21: Force user PIN change after set/reset** is set to **1** (default), this procedure is required after initializing or resetting the CO or CU role and/or creating a challenge secret.

### To change a role credential

1. In LunaCM, log in using the role's current credential (see [Logging In to the Application Partition](#)).

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

2. Change the credential for the logged-in role. If you are using a password-authenticated partition, specify a new password. If you are using a PED-authenticated partition, ensure that you have a blank or rewritable PED key available. Refer to ["Creating PED Keys" on page 111](#) for details on creating PED keys.

In LunaCM, passwords and activation challenge secrets must be 7-255 characters in length (**NOTE:** If you are using firmware version 7.0.1, 7.0.2, 7.0.3, 7.3.3, or 7.4.2, activation challenge secrets must be 7-16 characters in length). The following characters are allowed:

```
abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789 !@#$%^&* () -_ =+ [] {} \ | / ; : ' , . < > ? ` ~
```

Double quotation marks (") are problematic and should not be used in passwords.

Spaces are allowed; to specify a password with spaces using the **-password** option, enclose the password in double quotation marks.

```
lunacm:> role changepw -name <role>
```

3. To change the CO or CU challenge secret for an activated PED-authenticated partition, specify the **-oldpw** and/or **-newpw** options.

```
lunacm:> role changepw -name <role> -oldpw <oldpassword> -newpw <newpassword>
```

## Name, Label, and Password Requirements

This page describes length and character requirements for setting labels, domains, passwords, and challenge secrets on the SafeNet Luna PCIe HSM. This information can also be found in relevant sections throughout the documentation. Refer to the applicable section below:

- > ["HSM Labels" on the next page](#)
- > ["Cloning Domains" on the next page](#)
- > ["Partition Labels" on the next page](#)
- > ["Role Passwords or Challenge Secrets" on the next page](#)

## HSM Labels

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. The following characters are allowed:

```
abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789 !@#$%^&*()_+=[]{}|\/;:'",.<>?`~
```

Spaces are allowed; enclose the label in double quotes if it includes spaces. Including both spaces and quotation marks in a label may cause unexpected labeling behavior.

## Cloning Domains

The domain string must be 1-128 characters in length. The following characters are allowed:

```
abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789 !@#$%^&*-_+=[]{}/:'',.~
```

The following characters are problematic or invalid and must not be used in a domain string: "&;<>`|()"

Spaces are allowed, as long as the leading character is not a space; to specify a domain string with spaces using the **-domain** option, enclose the string in double quotation marks.

## Partition Labels

The partition 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. The following characters are allowed:

```
abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789 !@#$%^&*()_+=[]{}|\/;:'",.<>`~
```

Question marks (?) and double quotation marks (") are not allowed.

Spaces are allowed; enclose the label in double quotation marks if it includes spaces.

## Role Passwords or Challenge Secrets

In LunaCM, passwords and activation challenge secrets must be 7-255 characters in length (**NOTE:** If you are using firmware version 7.0.1, 7.0.2, 7.0.3, 7.3.3, or 7.4.2, activation challenge secrets must be 7-16 characters in length). The following characters are allowed:

```
abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789 !@#$%^&*()_+=[]{}|\/;:'",.<>?`~
```

Double quotation marks (") are problematic and should not be used in passwords.

Spaces are allowed; to specify a password with spaces using the **-password** option, enclose the password in double quotation marks.

# CHAPTER 9: 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 Group (see ["Upgrading HSM Capabilities" on page 270](#)). 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 SafeNet Luna PCIe HSM capabilities, their corresponding policies, and the results of changing their settings. This section contains the following procedures:

- > ["Setting HSM Policies Manually" on page 200](#)
- > ["Setting HSM Policies Using a Template" on page 201](#)

To zeroize the HSM and revert policies to their default values, see ["Resetting the SafeNet Luna PCIe HSM to Factory Condition" on page 287](#).

To zeroize the HSM and keep the existing policy settings, use `lunacm:> hsm zeroize`

## Destructive Policies

Some policies affect the security of the HSM. As a security measure, changing these policies results in application partitions or the entire HSM being zeroized. These policies are listed below as **destructive**.

| # | HSM Capability                                                                                                                                                                                                                                                                                                                                                    | HSM Policy |
|---|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|
| 0 | <b>Enable PIN-based authentication</b> <ul style="list-style-type: none"><li>&gt; 1: The HSM authenticates all users with keyboard-entered passwords.</li><li>&gt; 0: See HSM capability 1 below.</li></ul>                                                                                                                                                       | N/A        |
| 1 | <b>Enable PED-based authentication</b> <ul style="list-style-type: none"><li>&gt; 1: The HSM authenticates users with secrets stored on physical PED keys, read by a SafeNet Luna PED. The Crypto Officer and Crypto User roles may also be configured with a secondary, keyboard-entered challenge secret.</li><li>&gt; 0: See HSM capability 0 above.</li></ul> | N/A        |

| #  | HSM Capability                                                                                                                                                                                                                                                                                                                            | HSM Policy                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|----|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 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>1</b>. All SafeNet Luna PCIe HSMs are capable of full-strength cryptography with no US export restrictions.</p>                                                                                                                                                     | N/A                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| 6  | <p><b>Enable masking</b></p> <p>Always <b>0</b>. SIM has been deprecated on all current SafeNet Luna PCIe HSMs.</p>                                                                                                                                                                                                                       | N/A                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| 7  | <p><b>Enable cloning</b></p> <p>Always <b>1</b>. All current SafeNet Luna PCIe HSMs can clone cryptographic objects from one partition to another.</p>                                                                                                                                                                                    | <p><b>Allow cloning (Destructive)</b></p> <ul style="list-style-type: none"> <li>&gt; <b>1</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>0</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>1</b>: The HSM is capable of full cryptographic functions.</li> <li>&gt; <b>0</b>: The HSM is capable of backup functions only (disallowed on SafeNet Luna Backup HSMs only).</li> </ul>                                              | N/A                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| 12 | <p><b>Enable non-FIPS algorithms</b></p> <p>Always <b>1</b>. The HSM can use all cryptographic algorithms described in <a href="#">Supported Mechanisms</a>.</p>                                                                                                                                                                          | <p><b>Allow non-FIPS algorithms (Destructive)</b></p> <ul style="list-style-type: none"> <li>&gt; <b>1</b> (default): The HSM may use all available cryptographic algorithms.</li> <li>&gt; <b>0</b>: Only algorithms sanctioned by the FIPS 140-2 standard are permitted. The following is displayed in the output from <code>lunacm:&gt; hsm showinfo</code>:<br/>The HSM is in FIPS 140-2 approved operation mode.</li> </ul>                       |

| #  | HSM Capability                                                                                                                                                                                                                                                                                                                                   | HSM Policy                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|----|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 15 | <p><b>Enable SO reset of partition PIN</b></p> <p>Always <b>1</b>. This capability enables:</p> <ul style="list-style-type: none"> <li>&gt; the Partition SO to reset the password or PED secret of the Crypto Officer.</li> <li>&gt; the Crypto Officer to reset the password or PED secret of the Crypto User.</li> </ul>                      | <p><b>SO can reset partition PIN (Destructive)</b></p> <ul style="list-style-type: none"> <li>&gt; <b>1</b>: Partition SO may reset the password or PED secret of a Crypto Officer who has been locked out after too many failed login attempts.</li> <li>&gt; <b>0</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. See <a href="#">Resetting the Crypto Officer or Crypto User Credential</a>.</li> </ul> |
| 16 | <p><b>Enable network replication</b></p> <p>Always <b>1</b>. This capability enables cloning of cryptographic objects over a network. This is required for HA groups, and for partition backup to a remote SafeNet Luna Backup HSM.</p>                                                                                                          | <p><b>Allow network replication</b></p> <ul style="list-style-type: none"> <li>&gt; <b>1</b> (default): Cloning of cryptographic objects is permitted over a network. Remote backup is allowed, and the partition may be used in an HA group.</li> <li>&gt; <b>0</b>: Cloning over a network is not permitted. Partition backup is possible to a locally-connected SafeNet Luna Backup HSM only.</li> </ul>                                                                                                                                      |
| 17 | <p><b>Enable Korean Algorithms</b></p> <ul style="list-style-type: none"> <li>&gt; <b>1</b>: if you have purchased and applied a license for the Korea-specific algorithm set. See "<a href="#">Upgrading HSM Capabilities</a>" on page 270 to purchase this capability.</li> <li>&gt; <b>0</b> if you have not applied this license.</li> </ul> | N/A                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| 18 | <p><b>FIPS evaluated</b></p> <p>Always <b>0</b> - deprecated capability. All SafeNet Luna PCIe HSMs are capable of operating in FIPS Mode.</p>                                                                                                                                                                                                   | N/A                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| 19 | <p><b>Manufacturing Token</b></p> <p>Always <b>0</b>. For Thales Group internal use only.</p>                                                                                                                                                                                                                                                    | N/A                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |

| #  | HSM Capability                                                                                                                                                                                             | HSM Policy                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|----|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 21 | <p><b>Enable forcing user PIN change</b></p> <p>Always <b>1</b>. This capability forces the Crypto Officer or Crypto User to change the initial role credential created by the Partition SO.</p>           | <p><b>Force user PIN change after set/reset</b></p> <ul style="list-style-type: none"> <li>&gt; <b>1</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>0</b>: The CO/CU may continue to use the credential assigned by the Partition SO.</li> </ul> <p>See <a href="#">"Changing a Role Credential" on page 191</a>.</p> |
| 22 | <p><b>Enable offboard storage</b></p> <p>Always <b>1</b>, but SIM is not supported on this version of SafeNet Luna PCIe HSM.</p>                                                                           | <p><b>Allow offboard storage (Destructive)</b></p> <p>Deprecated policy. On previous HSMs, this policy allowed or disallowed the use of the portable SIM key.</p> <p>Default: <b>1</b></p>                                                                                                                                                                                                                                                                                                                                                                                                                       |
| 23 | <p><b>Enable partition groups</b></p> <p>Always <b>0</b> - deprecated capability.</p>                                                                                                                      | N/A                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| 25 | <p><b>Enable Remote PED usage</b></p> <p>Always <b>1</b> on PED-authenticated HSMs.<br/>Always <b>0</b> on password-authenticated HSMs.</p>                                                                | <p><b>Allow Remote PED usage</b></p> <ul style="list-style-type: none"> <li>&gt; <b>1</b> (default): The HSM may authenticate roles using a remotely-located PED server or a locally-installed PED.</li> <li>&gt; <b>0</b>: The HSM must use a locally-installed PED to authenticate roles.</li> </ul>                                                                                                                                                                                                                                                                                                           |
| 27 | <p><b>HSM non-volatile storage space</b></p> <p>Displays the maximum non-volatile storage space (in bytes) on the HSM, determined by the SafeNet Luna PCIe HSM model you selected at time of purchase.</p> | N/A                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| 30 | <p><b>Enable Unmasking</b></p> <p>Always <b>1</b>. This capability enables migration from legacy SafeNet HSMs that used SIM.</p>                                                                           | <p><b>Allow unmasking</b></p> <ul style="list-style-type: none"> <li>&gt; <b>1</b> (default): Cryptographic objects may be migrated from legacy SafeNet HSMs that used SIM.</li> <li>&gt; <b>0</b>: Migration from legacy HSMs using SIM is not possible.</li> </ul>                                                                                                                                                                                                                                                                                                                                             |
| 33 | <p><b>Maximum number of partitions</b></p> <p>Displays the maximum number of application partitions that can be created on the HSM.</p>                                                                    | <p><b>Current maximum number of partitions</b></p> <p>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>                                                                                                                                                                                                                                                                                                                               |

| #  | HSM Capability                                                                                                                                                                                                                                                                                     | HSM Policy                                                                                                                                                                                                                                                                                                                                                                                                                      |
|----|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 35 | <b>Enable Single Domain</b><br>Always <b>0</b> . Not applicable to SafeNet Luna PCIe HSM.                                                                                                                                                                                                          | N/A                                                                                                                                                                                                                                                                                                                                                                                                                             |
| 36 | <b>Enable Unified PED Key</b><br>Always <b>0</b> . Not applicable to SafeNet Luna PCIe HSM.                                                                                                                                                                                                        | N/A                                                                                                                                                                                                                                                                                                                                                                                                                             |
| 37 | <b>Enable MofN</b><br>Always <b>1</b> on PED-authenticated HSMs.<br>Always <b>0</b> on password-authenticated HSMs.                                                                                                                                                                                | <b>Allow MofN</b><br><ul style="list-style-type: none"> <li>&gt; <b>1</b> (default): During PED key creation, you have the option to require a quorum to authenticate the role, by splitting the PED secret among multiple PED keys (see "<a href="#">M of N Split Secrets (Quorum)</a>" on page 88)</li> <li>&gt; <b>0</b>: Users do not have the option to split PED secrets (M and N are automatically set to 1).</li> </ul> |
| 38 | <b>Enable small form factor backup/restore</b><br>Always <b>0</b> . Not available in this release.                                                                                                                                                                                                 | N/A                                                                                                                                                                                                                                                                                                                                                                                                                             |
| 39 | <b>Enable Secure Trusted Channel</b><br>Always <b>1</b> .                                                                                                                                                                                                                                          | <b>Allow Secure Trusted Channel</b><br>Secure Trusted Channel is a Network HSM feature, and has no function on SafeNet Luna PCIe HSM. Thales Group does not recommend turning this policy on at any time.                                                                                                                                                                                                                       |
| 40 | <b>Enable decommission on tamper</b><br>Always <b>1</b> . This enables the HSM to be automatically decommissioned if a tamper event occurs (see " <a href="#">Comparing Zeroize, Decommission, and Factory Reset</a> " on page 288).                                                               | <b>Decommission on tamper (Destructive)</b><br><ul style="list-style-type: none"> <li>&gt; <b>1</b>: The HSM is decommissioned if a tamper event occurs (see "<a href="#">Tamper Events</a>" on page 211).</li> <li>&gt; <b>0</b> (default): The contents of the HSM are not affected by a tamper event.</li> </ul>                                                                                                             |
| 42 | <b>Enable partition re-initialize</b><br>Always <b>0</b> . Not applicable to SafeNet Luna PCIe HSM. This capability and any associated feature and command(s) are applicable only to the Luna IS product, which shares some common code. No such feature has been tested on SafeNet Luna PCIe HSM. | N/A                                                                                                                                                                                                                                                                                                                                                                                                                             |
| 43 | <b>Enable low level math acceleration</b><br>Always <b>1</b> . This capability enables acceleration of cryptographic functionality for maximum HSM performance.                                                                                                                                    | <b>Allow low-level math acceleration</b><br><ul style="list-style-type: none"> <li>&gt; <b>1</b> (default): Provides maximum HSM performance.</li> <li>&gt; <b>0</b>: Do not turn this policy off unless instructed by Thales Group Technical Support.</li> </ul>                                                                                                                                                               |

| #  | HSM Capability                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               | HSM Policy                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|----|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 46 | <p><b>Allow Disabling Decommission</b></p> <p>Always <b>1</b>. This capability enables the HSM SO to disable the decommission jumper header on the HSM.</p>                                                                                                                                                                                                                                                                                                                                                  | <p><b>Disable Decommission (Destructive)</b></p> <ul style="list-style-type: none"> <li>&gt; <b>1</b>: The decommission jumper header is disabled, preventing decommissioning of the HSM.</li> <li>&gt; <b>0</b> (default): Decommission works as described in <a href="#">"Decommissioning the HSM Card" on page 286</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></p> <p>Always <b>0</b>. Not available in this release.</p>                                                                                                                                                                                                                                                                                                                                                                                                                      | N/A                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| 48 | <p><b>Enable Controlled Tamper Recovery</b></p> <p>Always <b>1</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>1</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>0</b>: The HSM must be restarted before it can resume normal operations.</li> </ul> <p>See <a href="#">"Tamper Events" on page 211</a> for more information.</p>                                                                                                                                                                                                                                                                                                       |
| 49 | <p><b>Enable Partition Utilization Metrics</b></p> <p>Always <b>1</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>1</b>: The HSM SO can view Partition Utilization Metrics.</li> <li>&gt; <b>0</b> (default): Partition Utilization Metrics are not available.</li> </ul> <p>See <a href="#">"Partition Utilization Metrics" on page 227</a> 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 272</a>).</p> <ul style="list-style-type: none"> <li>&gt; <b>1</b> on FM-ready HSMs running firmware 7.4 or higher, with the FM capability license installed (see <a href="#">"Preparing the SafeNet Luna PCIe HSM to Use FMs" on page 275</a>).</li> <li>&gt; <b>0</b> on FM-ready HSMs running firmware 7.4 or higher without the FM capability license.</li> </ul> <p>Does not appear on HSMs that are not FM-ready or are running firmware older than 7.4.</p> | <p><b>Allow Functionality Modules (Destructive)</b></p> <ul style="list-style-type: none"> <li>&gt; <b>1</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> <li>&gt; <b>0</b> (default): FMs may not be loaded to the HSM.</li> </ul> <div style="border: 1px solid orange; padding: 5px; margin-top: 10px;"> <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 272</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> |
| 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>1</b> on FM-ready HSMs running firmware 7.4 or higher, with the FM capability license installed (see <a href="#">"Preparing the SafeNet Luna PCIe HSM to Use FMs" on page 275</a>).</li> <li>&gt; <b>0</b> on FM-ready HSMs running firmware 7.4 or higher without the FM capability license.</li> </ul> <p>Does not appear on HSMs that are not FM-ready or are running firmware older than 7.4.</p>                                  | <p><b>Allow SMFS Auto Activation (Destructive)</b></p> <ul style="list-style-type: none"> <li>&gt; <b>1</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 PED-authenticated partitions in general, persists through a power outage of up to 2 hours duration.</li> <li>&gt; <b>0</b> (default): If disabled, the HSM SO must manually activate the SMFS each time the HSM reboots or loses power.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                |

| #  | HSM Capability                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       | HSM Policy                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|----|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 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>1</b> on FM-ready HSMs running firmware 7.4 or higher, with the FM capability license installed (see <a href="#">"Preparing the SafeNet Luna PCIe HSM to Use FMs" on page 275</a>).</li> <li>&gt; <b>0</b> on FM-ready HSMs running firmware 7.4 or higher without the FM capability license.</li> </ul> <p>Does not appear on HSMs that are not FM-ready or are running firmware older than 7.4.</p>            | <p><b>Restrict FM Privilege Level (Destructive)</b></p> <ul style="list-style-type: none"> <li>&gt; <b>1</b>: FM privilege is restricted.</li> <li>&gt; <b>0</b> (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).</li> </ul> |
| 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>1</b> on FM-ready HSMs running firmware 7.4 or higher, with the FM capability license installed (see <a href="#">"Preparing the SafeNet Luna PCIe HSM to Use FMs" on page 275</a>).</li> <li>&gt; <b>0</b> on FM-ready HSMs running firmware 7.4 or higher without the FM capability license.</li> </ul> <p>Does not appear on HSMs that are not FM-ready or are running firmware older than 7.4.</p> | <p><b>Encrypt Keys Passing from FM to HSM (Destructive)</b></p> <ul style="list-style-type: none"> <li>&gt; <b>1</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>0</b> (default): Keys are not encrypted before crossing to the FMCE.</li> </ul>                                                                                                                                  |

## 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 193](#) 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 178](#)).

- > If you are changing a destructive policy and you have partitions existing on the HSM, back up any important cryptographic objects (see [Backup and Restore Using a G5-Based Backup HSM](#) or [Backup and Restore Using a G7-Based Backup HSM](#)).

### To manually set or change an HSM policy

1. Launch LunaCM and set the active slot to the HSM Admin partition.  
lunacm:> **slot set -slot** <slotnum>
2. [Optional] Display the existing HSM policy settings.  
lunacm:> **hsm showpolicies**
3. Log in as HSM SO (see "Logging In as HSM Security Officer" on page 190).  
lunacm:> **role login -name so**
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).

lunacm:> **hsm changehsmpolicy -policy** <policy\_ID> **-value** <value>

If you are changing a destructive policy, you are prompted to enter **proceed** to continue the operation.

## 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 firmware version 7.1.0. See [Version Dependencies by Feature](#) for more information.

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 SafeNet Luna PCIe HSM to Factory Condition](#)" on page 287.

To zeroize the HSM and keep the existing policy settings, use lunacm:> **hsm zeroize**

This section provides instructions for the following procedures, and some general guidelines and restrictions:

- > "[Creating an HSM Policy Template](#)" on the next page
- > "[Editing an HSM Policy Template](#)" on the next page
- > "[Applying an HSM Policy Template](#)" on page 203

## 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. Launch LunaCM and set the active slot to the Admin partition. If you are creating a template from an initialized HSM, you must log in as HSM SO.

```
lunacm:> slot set slot <admin_slotnum>
```

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

2. Create the HSM policy template file with an original filename. Specify the path to the location where you wish to save the template. No file extension is required. If a template file with the same name exists in the specified directory, it is overwritten.

```
lunacm:> hsm showpolicies -exporttemplate <filepath/filename>
```

```
lunacm:>hsm showpolicies -templatefile /usr/safenet/lunaclient/templates/HSMPT
```

```
HSM policies for HSM: myPCIeHSM written to /usr/safenet/lunaclient/templates/HSMPT
```

```
Command Result : No Error
```

3. 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 193](#) 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

```

### 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. Ensure that the template file is saved on the workstation hosting the destination HSM.
2. Launch LunaCM and initialize the destination HSM using the policy template file. If the template file is not in the same directory as LunaCM, include the correct filepath.

```
lunacm:> hsm init -label <label> -applytemplate <filepath/filename>
```

3. Verify that the template has been applied correctly by checking the partition's policy settings.

```
lunacm:> hsm showpolicies
```

# CHAPTER 10: Application Partitions

The SafeNet Luna PCIe HSM has two partitions:

- > 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.
- > 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. 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.

This chapter contains the following procedures for managing application partitions:

- > ["Creating or Deleting an Application Partition" below](#)

## Creating or Deleting an Application Partition

The HSM Security Officer (SO) is responsible for creating the application partition. 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 178](#)).
- > You require the HSM SO credential (blue PED key).

### To create an application partition

1. Log in as HSM SO (see ["Logging In as HSM Security Officer" on page 190](#)).  
lunacm:> **role login -name so**
2. Create the application partition.  
lunacm:> **partition create**
3. [Optional] Confirm that the partition was created.  
lunacm:> **slot list**

### To delete an application partition

1. Log in as HSM SO (see ["Logging In as HSM Security Officer" on page 190](#)).  
lunacm:> **role login -name so**

2. Delete the application partition by specifying the slot number.

lunacm:> **partition delete -slot** <slot>

# CHAPTER 11: Security in Operation

This section addresses actions and settings with security-related implications.

- > ["Security Effects of Administrative Actions" below](#)
- > ["Tamper Events" on page 211](#)

Refer also to [Security of Your Partition Challenge](#).

## Security Effects of Administrative Actions

---

Actions that you take, in the course of administering your SafeNet 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> <p>(1) This is a destructive operation.<br/> (2) You will lose all your partitions.<br/> (3) You may lose some capabilities.<br/> (4) You must re-initialize the HSM.<br/> (5) If the PED use is remote, you must re-connect it.</p> |

### 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.

## Tamper Events

SafeNet Luna PCIe HSMs detect hardware anomalies (such as card over-temperature) and physical events (such as card removal or chassis intrusion), and register 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 193). While the HSM is in the tamper condition, only the subset of LunaCM commands required to view the HSM status or clear the tamper condition are available. For PED-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 type of tamper event is indicated by the **HSM Status** field in the output of `lunacm:> slot list`. The status also indicates whether the tamper event 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 (requires chassis connector to card tamper header) | 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. |

| Tamper event              | Response                                                                                                                                                                                                                                           |
|---------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 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 193 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 PED-authenticated partitions, it is disabled when a tamper is detected, or if any uncleared tamper conditions are detected on reboot. See [Activation and Auto-activation on Multi-factor- \(PED-\) Authenticated Partitions](#) and [Partition Capabilities and Policies](#) for more information.

### To recover from a tamper

1. View the output of `lunacm:> slot list` (displayed by default on login). The reason for the tamper is indicated by the **HSM Status** field. You can also use `lunacm:> hsm tampershow` to display the last tamper event.

**NOTE** The `slot list` and `hsm tampershow` commands only show 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 the `lunadiag` utility.

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:

`lunacm:> hsm tamperclear`

4. If the tamper message indicates that a reset is required, exit LunaCM and use the **lunareset** utility to reset the HSM.

```
lunareset <device>
```

5. Verify that all tampers have been cleared:

```
lunacm:> hsm tampershow
```

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 204.
  - b. Re-initialize the partition roles. See [Initializing an Application Partition](#).
  - c. To restore the partition contents from backup, see [Backup and Restore Using a G5-Based Backup HSM](#) or [Backup and Restore Using a G7-Based Backup HSM](#).
7. If the **Policy 22: Allow Activation** and/or **Policy 23: Allow AutoActivation** are enabled on your PED-authenticated partitions, the CO and CU (if enabled) must log in to reactivate those roles:

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

# CHAPTER 12: Monitoring the HSM

Thales Group 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](#)
- > [SNMP Monitoring](#)
- > ["Performance Monitoring" on page 226](#)
- > ["Partition Utilization Metrics" on page 227](#)
- > ["Keycard and Token Return Codes" on page 229](#)
- > ["Library Codes" on page 247](#)
- > ["Vendor-Defined Return Codes" on page 251](#)
- > ["HSM Alarm Codes" on page 257](#)

## 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.

| 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.                                                                                                   |
| 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.                                                          |

| Indicated Status of HSM        | Meaning                                                                                                                                                            | Recovery                                                                                                                                                                                                                                                                    |
|--------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 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 (vreset for SafeNet Luna PCIe HSM, or ureset for SafeNet Luna USB 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 (vreset for SafeNet Luna PCIe HSM, or ureset for SafeNet Luna USB HSM). The event is logged.<br><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 (vreset for SafeNet Luna PCIe HSM, or ureset for SafeNet Luna USB HSM). The event is logged.<br><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 178](#) for more information.

For a comparison of various destruction or denial actions on the HSM, see ["Comparison of Destruction/Denial Actions" on page 288](#).

## 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 SafeNet Luna USB HSM or a SafeNet Luna Backup HSM.

In the `Chrystoki.conf` file (or the Windows `crystoki.ini` file), for SafeNet Luna USB HSM, you can remove the empty slots by modifying the `CardReader` entry, like this:

```
CardReader = {
  LunaG5Slots=0;
}
```

For SafeNet Luna Network HSM, 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.

## 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 SafeNet Luna HSM problem.

## 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 K7 HSM card, used in the SafeNet Luna Network HSM and SafeNet Luna PCIe HSM 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.

## SNMP Monitoring

This chapter describes Simple Network Management Protocol (SNMP v3) support for remote monitoring of conditions on a local HSM that might require administrative attention. It contains the following sections:

- > ["Installing the SafeNet SNMP Subagent" below](#)
- > ["The SafeNet Chrysalis-UTSP MIB" on page 219](#)
- > ["The SafeNet Luna HSM MIB" on page 220](#)
- > ["Frequently Asked Questions" on page 226](#)

## MIB

Thales Group provides the following MIBs (management information base) in the Luna HSM Client installation package:

| MIB Name               | Description                                                        |
|------------------------|--------------------------------------------------------------------|
| CHRYSLIS-UTSP-MIB.txt  | Defines SNMP access to information about the SafeNet appliance.    |
| SAFENET-HSM-MIB.txt    | Defines SNMP access to information about the SafeNet Luna HSM.     |
| SAFENET-GLOBAL-MIB.txt | Must be found in your system path so that symbols can be resolved. |

Copy all MIBs in `<Luna_HSM_Client_install_dir>/snmp` to the MIB directory on your system. Only the MIBs necessary for SafeNet Luna PCIe HSM and SafeNet Luna USB HSM are included in a client installation.

**NOTE** Your SNMP application also requires the following standard SNMP MIBs:

- > **SNMPv2-SMI.txt** -- defined in RFC 2578, Section 2
- > **SNMPv2-TC.txt** -- defined in RFC 2579, Section 2

## Installing the SafeNet SNMP Subagent

We find that most customers choosing to use SNMP already have an SNMP infrastructure in place. Therefore, we provide a subagent that you can install on your managed workstations, and which can point to your agent via the socket created by the agent. This applies to SafeNet Luna USB HSM and SafeNet Luna PCIe HSM - for SafeNet Luna Network HSM, the subagent is already on the appliance.

The SNMP subagent (luna-snmp) is an AgentX SNMP module that extends an existing SNMP agent with support for SafeNet Luna HSM monitoring. It is an optional component of the Luna HSM Client installation. The subagent has been tested against net-snmp, but should work with any SNMP agent that supports the AgentX protocol.

### To install the SNMP subagent

After selecting one or more products from the main Luna HSM Client installation menu, you are presented with a list of optional components, including the SNMP subagent. It is not selected by default, but can be installed with any product except the SafeNet Luna Network HSM client installed in isolation.

1. In the installation media, go to the appropriate folder for your operating system.
2. Run the installer (install.sh for Linux and UNIX, LunaHSMClient.exe for Windows).
3. Choose the SafeNet products that you wish to install, and include SNMP among your selections. The subagent is installed for any SafeNet product except SafeNet Luna Network HSM in isolation.
4. Proceed to Post-installation configuration.

### Post-installation configuration

After the Luna HSM Client is installed, complete the following steps to configure the SNMP subagent:

1. Copy the SafeNet MIBs from **<install dir>/snmp** to the main SNMP agent's MIB directory. Or copy to another computer (your SNMP computer) if you are not running SNMP from the same computer where Luna HSM Client software is installed.
2. If running on Windows, configure the subagent via the file **<install dir>/snmp/luna-snmp.conf** to point to the AgentX port where the main SNMP agent is listening. The file must then be copied to the same directory as **snmpd.conf**. (This assumes net-snmp is installed; the setup might differ if you have another agent.)  
  
If running on a UNIX-based platform, the subagent should work without extra configuration assuming that the primary SNMP agent is listening on the default local socket (**/var/agentx/master**). You still have the option of editing and using **luna-snmp.conf**.
3. After configuration is complete, start the agent. Then start the subagent via the service tool applicable to your platform (for example, **service luna-snmp start** on Linux, or start SafeNet SNMP Subagent Service from the services in Windows).

Normally the agent is started first. However, the subagent periodically attempts to connect to the agent until it is successful. The defaults controlling this behavior are listed below. They can be overridden by changing the appropriate entries in **luna-snmp.conf**.

### Troubleshooting

If you encounter the following warning:

#### **Warning: Failed to connect to the agentx master agent ([NIL]):**

you must enable AgentX support by adding **master agentx** to your SNMPD configuration file. Refer to the man page for **snmpd.conf** for more information.

## Configuration Options In the luna-snmp.conf File

| Option                                                            | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                         | Default                                                                                                                                                                                |
|-------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| agentXSocket<br>[<transport-specifier>:]<transport-address>[,...] | Defines the address to which the subagent should connect. The default on UNIX-based systems is the Unix Domain socket <code>"/var/agentx/master"</code> .<br>Another common alternative is <code>tcp:localhost:705</code> .<br>See the section LISTENING ADDRESSES in the <code>snmpd</code> man page for more information about the format of addresses ( <a href="http://www.net-snmp.org/docs/man/snmpd.html">http://www.net-snmp.org/docs/man/snmpd.html</a> ). | The default, for Linux, is <code>"/var/agentx/master"</code> .<br>In the file, you can choose to un-comment <code>"tcp:localhost:705"</code> which is most commonly used with Windows. |
| agentXPingInterval<br><NUM>                                       | Makes the subagent try to reconnect every <NUM> seconds to the master if it ever becomes (or starts) disconnected.                                                                                                                                                                                                                                                                                                                                                  | 15                                                                                                                                                                                     |
| agentXTimeout <NUM>                                               | Defines the timeout period (NUM seconds) for an AgentX request.                                                                                                                                                                                                                                                                                                                                                                                                     | 1                                                                                                                                                                                      |
| agentXRetries <NUM>                                               | Defines the number of retries for an AgentX request.                                                                                                                                                                                                                                                                                                                                                                                                                | 5                                                                                                                                                                                      |

## The SafeNet Chrysalis-UTSP MIB

**NOTE** The Chrysalis MIB is the SafeNet MIB for all SafeNet Luna HSM products - the Chrysalis name is retained for historical continuity.

To illustrate accessing data, the command `"snmpwalk -v 3 -u admin -l authPriv -a SHA1 -A 12345678 -x AES -X 87654321 myLuna19 private"` produced this output:

- > CHRYSALIS-UTSP-MIB::hsmOperationRequests.0 = Counter64: 3858380
- > CHRYSALIS-UTSP-MIB::hsmOperationErrors.0 = Counter64: 385838
- > CHRYSALIS-UTSP-MIB::hsmCriticalEvents.0 = Counter64: 0
- > CHRYSALIS-UTSP-MIB::hsmNonCriticalEvents.0 = Counter64: 5
- > CHRYSALIS-UTSP-MIB::ntIsOperStatus.0 = INTEGER: up(1)
- > CHRYSALIS-UTSP-MIB::ntIsConnectedClients.0 = Gauge32: 0
- > CHRYSALIS-UTSP-MIB::ntIsLinks.0 = Gauge32: 0
- > CHRYSALIS-UTSP-MIB::ntIsSuccessfulClientConnections.0 = Counter64: 16571615927115620
- > CHRYSALIS-UTSP-MIB::ntIsFailedClientConnections.0 = Counter64: 1657161592711562

The various counts are recorded since the last restart.

| Item                            | Description                                                                                                                                                                                                                       |
|---------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| hsmOperationRequests            | The total number of HSM operations that have been requested.                                                                                                                                                                      |
| hsmOperationErrors              | The total number of HSM operations that have been requested, that have resulted in errors.                                                                                                                                        |
| hsmCriticalEvents               | The total number of critical HSM events that have been detected (Tamper, Decommission, Zeroization, SO creation, or Audit role creation).<br><br><b>NOTE</b> Not implemented in this release. hsmCriticalEvents always reports 0. |
| hsmNonCriticalEvents            | The total number of NON-critical HSM events that have been detected (any that are not among the critical list, above).<br><br><b>NOTE</b> Not implemented in this release. hsmNonCriticalEvents always reports 0.                 |
| ntlsOperStatus                  | The current operational status of the NTL service, where the options are:<br>1 = up,<br>2 = not running, and<br>3 = status cannot be determined.                                                                                  |
| ntlsConnectedClients            | The current number of connected clients using NTLS.                                                                                                                                                                               |
| ntlsLinks                       | The current number of links in NTLS - can be multiple per client, depending on processes.                                                                                                                                         |
| ntlsSuccessfulClientConnections | The total number of successful client connections.                                                                                                                                                                                |
| ntlsFailedClientConnections     | The total number of UNSuccessful client connections.                                                                                                                                                                              |

## The SafeNet Luna HSM MIB

The SAFENET-HSM-MIB defines HSM status information and HSM Partition information that can be viewed via SNMP.

To access tables, use a command like:

```
snmptable -a SHA -A snmppass -u snmpuser -x AES -X snmppass -l authPriv -v 3 192.20.11.59
SAFENET-HSM-MIB:hsmTable
```

The information is defined in tables, as detailed in the following sections.

### SNMP Table Updates

The SNMP tables are updated and cached every 60 seconds. Any changes made on the HSM may therefore take up to 60 seconds to be included in the tables. When a query is received to view the tables, the most recent cached version is displayed. If a change you were expecting is not displayed, wait 60 seconds and try again.

**NOTE** Some values may not get updated automatically, such as the HSM firmware version (hsmFirmwareVersion) following a firmware upgrade. To force an update, restart the SNMP agent.

## hsmTable

This table provides a list of all the HSM information on the managed element.

| Item                     | Type          | Description                                                  | Values                                                                                                                 |
|--------------------------|---------------|--------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------|
| hsmSerialNumber          | DisplayString | Serial number of the HSM - used as an index into the tables. | From factory                                                                                                           |
| hsmFirmwareVersion       | DisplayString | Version of firmware executing on the HSM.                    | As found                                                                                                               |
| hsmLabel                 | DisplayString | Label associated with the HSM.                               | Provided by SO at init time                                                                                            |
| hsmModel                 | DisplayString | Model identifier for the HSM.                                | From factory                                                                                                           |
| hsmAuthenticationMethod  | INTEGER       | Authentication mode of the HSM.                              | unknown(1), -- not known<br>password(2), -- requires passwords<br>pedKeys(3) -- requires PED                           |
| hsmRpvInitialized        | INTEGER       | Remote ped vector initialized flag of the HSM.               | notSupported(1), -- rpv not supported<br>uninitialized(2), -- rpv not initialized<br>initialized(3) -- rpv initialized |
| hsmFipsMode              | TruthValue    | FIPS 140-2 operation mode enabled flag of the HSM.           | Factory set                                                                                                            |
| hsmPerformance           | INTEGER       | Performance level of the HSM.                                |                                                                                                                        |
| hsmStorageTotalBytes     | Unsigned32    | Total storage capacity in bytes of the HSM                   | Factory set                                                                                                            |
| hsmStorageAllocatedBytes | Unsigned32    | Number of allocated bytes on the HSM                         | Calculated                                                                                                             |
| hsmStorageAvailableBytes | Unsigned32    | Number of available bytes on the HSM                         | Calculated                                                                                                             |

| Item                    | Type       | Description                                                            | Values                                        |
|-------------------------|------------|------------------------------------------------------------------------|-----------------------------------------------|
| hsmMaximumPartitions    | Unsigned32 | Maximum number of partitions allowed on the HSM                        | 2, 5, 10, 15, or 20, per license              |
| hsmPartitionsCreated    | Unsigned32 | Number of partitions created on the HSM                                | As found                                      |
| hsmPartitionsFree       | Unsigned32 | Number of partitions that can still be created on the HSM              | Calculated                                    |
| hsmBackupProtocol       | INTEGER    | Backup protocol used on the HSM                                        | unknown(1), none(2), cloning(3), keyExport(4) |
| hsmAdminLoginAttempts   | Counter32  | Number of failed Administrator login attempts left before HSM zeroized | As found, calculated                          |
| hsmAuditRoleInitialized | INTEGER    | Audit role is initialized flag                                         | notSupported(0), yes(1), no(2)                |
| hsmManuallyZeroized     | TruthValue | Was HSM manually zeroized flag                                         | As found                                      |
| hsmUpTime               | Counter64  | Up time in seconds since last HSM reset                                | Counted                                       |
| hsmBusyTime             | Counter64  | Busy time in seconds since the last HSM reset                          | Calculated                                    |
| hsmCommandCount         | Counter64  | HSM commands processed since last HSM reset                            | Counted                                       |

### The hsmPartitionTable

This table provides a list of all the partition information on the managed element.

| Item                          | Type          | Description                                      | Values                                             |
|-------------------------------|---------------|--------------------------------------------------|----------------------------------------------------|
| hsmPartitionSerialNumber      | DisplayString | Serial number for the partition                  | Generated                                          |
| hsmPartitionLabel             | DisplayString | Label assigned to the partition                  | Provided at partition creation                     |
| hsmPartitionActivated         | TruthValue    | Partition activation flag                        | Set by policy                                      |
| hsmPartitionStorageTotalBytes | Unsigned32    | Total storage capacity in bytes of the partition | Set or calculated at partition creation or re-size |

| Item                              | Type       | Description                                         | Values     |
|-----------------------------------|------------|-----------------------------------------------------|------------|
| hsmPartitionStorageAllocatedBytes | Unsigned32 | Number of allocated (in use) bytes on the partition | Calculated |
| hsmPartitionStorageAvailableBytes | Unsigned32 | Number of available (unused) bytes on the partition | Calculated |
| hsmPartitionObjectCount           | Unsigned32 | Number of objects in the partition                  | Counted    |

## hsmLicenseTable

This table provides a list of all the license information on the managed element. More than one HSM might be connected to a Host, so they are accessed with two indices; the first index identifies the HSM for which the license entry corresponds (hsmSerialNumber), the second is the index for the corresponding license (hsmLicenseID).

| Item                  | Type          | Description         | Values                                 |
|-----------------------|---------------|---------------------|----------------------------------------|
| hsmLicenseID          | DisplayString | License identifier  | Set at factory or at capability update |
| hsmLicenseDescription | DisplayString | License description | Set at factory or at capability update |

## hsmPolicyTable

This table provides a list of all the HSM policy information on the managed element.

| Item                 | Type          | Description                 | Values                                                                       |
|----------------------|---------------|-----------------------------|------------------------------------------------------------------------------|
| hsmPolicyType        | INTEGER       | Type of policy              | capability(1),<br>policy(2)                                                  |
| hsmPolicyID          | Unsigned32    | Policy identifier           | Numeric value identifies policy and is used as a index into the policy table |
| hsmPolicyDescription | DisplayString | Description of the policy   | Brief text description of what the policy does                               |
| hsmPolicyValue       | DisplayString | Current value of the policy | Brief text description to show current state/value of policy                 |

## hsmPartitionPolicyTable

This table provides a list of all the partition policy information on the managed element.

| Item                          | Type          | Description                 | Values                                                                       |
|-------------------------------|---------------|-----------------------------|------------------------------------------------------------------------------|
| hsmPartitionPolicyType        | INTEGER       | Capability or policy        | capability(1), policy(2)                                                     |
| hsmPartitionPolicyID          | Unsigned32    | Policy identifier           | Numeric value identifies policy and is used as a index into the policy table |
| hsmPartitionPolicyDescription | DisplayString | Description of the policy   | Brief text description of what the policy does                               |
| hsmPartitionPolicyValue       | DisplayString | Current value of the policy | Brief text description to show current state/value of policy                 |

### hsmClientRegistrationTable

This table provides a list of registered clients.

| Item                 | Type          | Description                                    | Values                                                                                                                                                                                                                          |
|----------------------|---------------|------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| hsmClientName        | DisplayString | Name of the client                             | Name provided on client cert                                                                                                                                                                                                    |
| hsmClientAddress     | DisplayString | Address of the client                          | IP address of the client                                                                                                                                                                                                        |
| hsmClientRequiresHTL | TruthValue    | Flag specifying if HTL required for the client | Flag set at HSM host side to control client access<br><b>Note:</b> HTL is not available in release 7.x. This value will always return <b>false</b> for 7.x HSMs.                                                                |
| hsmClientOTTEpiry    | INTEGER       | OTT expiry time (-1 if not provisioned)        | Expiry time, in seconds, for HTL OneTimeToken (range is 0-3600); -1 indicates not provisioned, 0 means never expires<br><b>Note:</b> HTL is not available in release 7.x. This value will always return <b>-1</b> for 7.x HSMs. |

### hsmClientPartitionAssignmentTable

This table provides a list of assigned partitions for a given client.

| Item                           | Type          | Description                    | Values |
|--------------------------------|---------------|--------------------------------|--------|
| hsmClientHsmSerialNumber       | DisplayString | Index into the HSM table       | --     |
| hsmClientPartitionSerialNumber | DisplayString | Index into the Partition Table | --     |

## SNMP output compared to SafeNet tools output

For comparison, the following shows LunaCM or LunaSH command outputs that provide HSM information equivalent to the SNMP information depicted in the tables above (from the HSM MIB).

### HSM Information

At the HSM level the information in the outputs of **hsm show** and **hsm showpolicies** and **hsm displaylicenses** includes the following:

- > SW Version
- > FW Version
- > HSM label
- > Serial #
- > HW Model
- > Authentication Method
- > RPV state
- > FIPS mode
- > HSM total storage space (bytes)
- > HSM used storage space (bytes)
- > HSM free storage space (bytes)
- > Performance level
- > Max # of partitions
- > # of partitions created
- > # of free partitions
- > HSM policies and their settings

### Partition Information

At the application partition level, the information in the outputs of **partition show** and **partition showpolicies** includes the following:

- > Partition Name
- > Partition Serial #
- > Activation State
- > AutoActivation State
- > Partition total storage space (bytes)
- > Partition used storage space (bytes)
- > Partition free storage space (bytes)
- > Partition Object Count
- > Partition policies and their settings

---

## Frequently Asked Questions

---

This section provides additional information by answering questions that are frequently asked by our customers.

### **We want to use SNMP to remotely monitor and manage our installation – why do you not support such standard SNMP traps as CPU and Memory exhaustion?**

Those sorts of traps were specifically excluded because they can be used to establish a covert channel (an illicit signaling channel that can be used to communicate from a high assurance “area” to a lower assurance one in an effort to circumvent the security policy). Resource exhaustion events/alerts are the oldest known form of covert channel signaling. Exercise care with any HSM product that does allow such traps - what other basic security holes might be present?

---

## 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 lunacm:> [hsm monitor](#).

## 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 Network HSM 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 firmware version 7.3.0 and client 7.3. See [Version Dependencies by Feature](#) for more information.

## 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 firmware 7.3 (and newer) which implements 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 showUtilization** command allows you to view the current utilization counter values for all partitions, and overall counts for the entire HSM, without resetting the counters.

The **hsm resetUtilization** command allows you to reset to zero the current utilization counter values for all partitions.

### To access the Partition Utilization Metrics feature

1. Ensure that your HSM is at firmware version 7.3 or newer (if needed, upgrade to a suitable version; see [Updating the SafeNet Luna PCIe HSM or SafeNet Luna Backup HSM Firmware](#)).
2. Log in as HSM SO (see "[Logging In as HSM Security Officer](#)" on page 190).  
lunacm:> **role login -name so**
3. Enable HSM policy 49: Allow Partition Utilization Metrics.  
lunacm:> **hsm changehsmpolicy -policy 49 -value 1**

### To view or save Partition Utilization Metrics without resetting

lunacm:> **hsm showUtilization -serial** <partition\_SN>

### 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 display the metrics since the last reset (making them available to be captured manually or by script) and then immediately reset the metrics:

lunacm:> **hsm resetUtilization**

## Keycard 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_CRYPTO_PROTOCOL | 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_ERROR                  |
| LUNA_RET_MM_INVALID_HANDLE                  | 0x00310001 | CKR_DEVICE_ERROR                  |
| LUNA_RET_MM_USAGE_ALREADY_SET               | 0x00310002 | CKR_DEVICE_ERROR                  |
| LUNA_RET_MM_ACCESS_OUTSIDE_ALLOCATION_RANGE | 0x00310003 | CKR_DEVICE_ERROR                  |
| LUNA_RET_MM_INVALID_USAGE                   | 0x00310004 | CKR_DEVICE_ERROR                  |
| LUNA_RET_MM_ITERATOR_PAST_END               | 0x00310005 | CKR_DEVICE_ERROR                  |
| LUNA_RET_MM_FATAL_ERROR                     | 0x00310006 | CKR_DEVICE_ERROR                  |
| 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         |
| LUNA_RET_SECRET_KEY_MUST_BE_SENSITIVE       | 0x00130013 | CKR_ATTRIBUTE_VALUE_INVALID       |

| HSM Error                                          | Hex Code   | PKCS#11 or SFNT Defined CKR Error |
|----------------------------------------------------|------------|-----------------------------------|
| 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                  |
| LUNA_RET_SM_DATA_INVALID                           | 0x00200002 | CKR_DATA_INVALID                  |
| LUNA_RET_NO_RNG_SEED                               | 0x00200015 | CKR_DATA_INVALID                  |

| HSM Error                        | Hex Code   | PKCS#11 or SFNT Defined CKR Error |
|----------------------------------|------------|-----------------------------------|
| 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                  |
| LUNA_RET_RC2_SELF_TEST_FAILURE   | 0x0030000c | CKR_DEVICE_ERROR                  |
| LUNA_RET_RC4_SELF_TEST_FAILURE   | 0x0030000d | CKR_DEVICE_ERROR                  |

| HSM Error                                   | Hex Code   | PKCS#11 or SFNT Defined CKR 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                  |
| LUNA_RET_RETRY                              | 0x00300021 | CKR_DEVICE_ERROR                  |
| LUNA_RET_SHA1_RSA_SELF_TEST_FAILURE         | 0x00300022 | CKR_DEVICE_ERROR                  |

| HSM Error                            | Hex Code   | PKCS#11 or SFNT Defined CKR 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            |
| LUNA_RET_MECHANISM_INVALID           | 0x00700000 | CKR_MECHANISM_INVALID             |

| HSM Error                                    | Hex Code   | PKCS#11 or SFNT Defined CKR Error    |
|----------------------------------------------|------------|--------------------------------------|
| 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           |
| LUNA_RET_SM_OTHER_USER_LOGGED_IN             | 0x01000001 | CKR_USER_ALREADY_LOGGED_IN           |

| HSM Error                                 | Hex Code   | PKCS#11 or SFNT Defined CKR Error  |
|-------------------------------------------|------------|------------------------------------|
| 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                   |
| LUNA_RET_ISES_INIT_FAILED                 | 0x00300881 | CKR_DEVICE_ERROR                   |
| LUNA_RET_ISES_LNAU_TEST_FAILED            | 0x00300882 | CKR_DEVICE_ERROR                   |

| HSM Error                                    | Hex Code   | PKCS#11 or SFNT Defined CKR 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                        |
| LUNA_RET_BAD_PPID                            | 0x00200a0d | CKR_DATA_INVALID                  |
| LUNA_RET_BAD_FW_VERSION                      | 0x00200a0e | CKR_DATA_INVALID                  |

| HSM Error                                | Hex Code   | PKCS#11 or SFNT Defined CKR Error |
|------------------------------------------|------------|-----------------------------------|
| 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                  |
| LUNA_RET_NOT_FOUND                       | 0x80000007 | CKR_FUNCTION_FAILED               |
| LUNA_RET_TOO_MANY_CONTAINERS             | 0x80000008 | CKR_TOO_MANY_CONTAINERS           |

| HSM Error                                 | Hex Code   | PKCS#11 or SFNT Defined CKR Error    |
|-------------------------------------------|------------|--------------------------------------|
| 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                     |
| LUNA_RET_TSN_MISMATCH                     | 0x8000010a | CKR_DATA_INVALID                     |
| LUNA_RET_KCV_PARAMETER_MISSING            | 0x8000010b | CKR_CLONING_PARAMETER_MISSING        |

| HSM Error                         | Hex Code   | PKCS#11 or SFNT Defined CKR Error |
|-----------------------------------|------------|-----------------------------------|
| 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      |
| LUNA_RET_SIM_VERSION_UNSUPPORTED  | 0x8000011c | CKR_SIM_VERSION_UNSUPPORTED       |
| LUNA_RET_SIM_CORRUPT_DATA         | 0x8000011d | CKR_SIM_CORRUPT_DATA              |

| HSM Error                             | Hex Code   | PKCS#11 or SFNT Defined CKR Error |
|---------------------------------------|------------|-----------------------------------|
| 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                 |
| LUNA_RET_SPLIT_DATA_INVALID           | 0x80000208 | CKR_ARGUMENTS_BAD                 |
| LUNA_RET_SPLIT_ID_INVALID             | 0x80000209 | CKR_ARGUMENTS_BAD                 |

| HSM Error                               | Hex Code   | PKCS#11 or SFNT Defined CKR Error |
|-----------------------------------------|------------|-----------------------------------|
| 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        |
| LUNA_RET_M_OF_N_IS_NOT_REQUIRED         | 0x8000021f | CKR_OPERATION_NOT_INITIALIZED     |

| HSM Error                             | Hex Code   | PKCS#11 or SFNT Defined CKR Error |
|---------------------------------------|------------|-----------------------------------|
| 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                 |
| LUNA_RET_SM_CONTEXT_BUFFER_OVERFLOW   | 0x80000409 | CKR_DEVICE_MEMORY                 |
| LUNA_RET_SM_TOSM_DOES_NOT_VALIDATE    | 0x8000040A | CKR_USER_NOT_LOGGED_IN            |

| HSM Error                              | Hex Code   | PKCS#11 or SFNT Defined CKR Error |
|----------------------------------------|------------|-----------------------------------|
| 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              | 0x8000a01  | CKR_FUNCTION_NOT_SUPPORTED        |
| LUNA_RET_CB_PARAM_INVALID              | 0x8000a02  | CKR_CALLBACK_ERROR                |
| LUNA_RET_CB_NO_MEMORY                  | 0x8000a03  | CKR_DEVICE_MEMORY                 |
| LUNA_RET_CB_TIMEOUT                    | 0x8000a04  | CKR_CALLBACK_ERROR                |

| HSM Error                                | Hex Code   | PKCS#11 or SFNT Defined CKR 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                |
| LUNA_RET_CB_MUST_WRITE                   | 0x80000a26 | CKR_CALLBACK_ERROR                |
| LUNA_RET_CB_INVALID_CALL_FOR_THE_STATE   | 0x80000a27 | CKR_CALLBACK_ERROR                |

| HSM Error                                | Hex Code   | PKCS#11 or SFNT Defined CKR Error   |
|------------------------------------------|------------|-------------------------------------|
| LUNA_RET_CB_SYNC_ERROR                   | 0x8000a28  | CKR_CALLBACK_ERROR                  |
| LUNA_RET_CB_PROT_DATA_INVALID            | 0x8000a29  | CKR_CALLBACK_ERROR                  |
| LUNA_RET_LOG_FILE_NOT_OPEN               | 0x8000d00  | CKR_LOG_FILE_NOT_OPEN               |
| LUNA_RET_LOG_FILE_WRITE_ERROR            | 0x8000d01  | CKR_LOG_FILE_WRITE_ERROR            |
| LUNA_RET_LOG_BAD_FILE_NAME               | 0x8000d02  | CKR_LOG_BAD_FILE_NAME               |
| LUNA_RET_LOG_FULL                        | 0x8000d03  | CKR_LOG_FULL                        |
| LUNA_RET_LOG_NO_KCV                      | 0x8000d04  | CKR_LOG_NO_KCV                      |
| LUNA_RET_LOG_BAD_RECORD_HMAC             | 0x8000d05  | CKR_LOG_BAD_RECORD_HMAC             |
| LUNA_RET_LOG_BAD_TIME                    | 0x8000d06  | CKR_LOG_BAD_TIME                    |
| LUNA_RET_LOG_AUDIT_NOT_INITIALIZED       | 0x8000d07  | CKR_LOG_AUDIT_NOT_INITIALIZED       |
| LUNA_RET_LOG_RESYNC_NEEDED               | 0x8000d08  | CKR_LOG_RESYNC_NEEDED               |
| LUNA_RET_AUDIT_LOGIN_TIMEOUT_IN_PROGRESS | 0x8000d09  | CKR_AUDIT_LOGIN_TIMEOUT_IN_PROGRESS |
| LUNA_RET_AUDIT_LOGIN_FAILURE_THRESHOLD   | 0x8000d0a  | 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 SafeNet's CKDemo utility.

## 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                           |
| 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 |

| Hex value  | Decimal value | Return code/error description |
|------------|---------------|-------------------------------|
| 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         |
| 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                  |

| Hex value  | Decimal value | Return code/error description         |
|------------|---------------|---------------------------------------|
| 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              |
| 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             |

| Hex value  | Decimal value | Return code/error description     |
|------------|---------------|-----------------------------------|
| 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                      |
| 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                  |

| Hex value  | Decimal value | Return code/error description |
|------------|---------------|-------------------------------|
| 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                      |

| Code       | Name                           |
|------------|--------------------------------|
| 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    |
| 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               |

| Code       | Name                                |
|------------|-------------------------------------|
| 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               |
| 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              |

| Code       | Name                                      |
|------------|-------------------------------------------|
| 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    |
| 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                 |

| Code       | Name                                  |
|------------|---------------------------------------|
| 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       |
| 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          |

| Code       | Name                                          |
|------------|-----------------------------------------------|
| 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_REKEY_KEY                                 |
| 0x80000074 | CKR_KEY_RETRY_FAILURE                         |
| 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                                      |

---

## HSM Alarm Codes

---

The SafeNet Luna PCIe HSM alarm messages indicate error conditions on the HSM card that might require user intervention. The alarms apply to a SafeNet 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" below](#)
- > ["List of HSM Alarm Codes" on the next page](#)
- > ["HSM Alarm Code Samples" on page 263](#)
- > ["HSM Alarm Codes" above](#)

### 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 the [lunadiag](#) utility to output the FRAM Log in order to determine the tamper information, or to pass on to Thales Group 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 K7 card is still present on the PCIe bus (i.e. chassis open causes a cold reset of the K7) 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 Group 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:<br>VST      |

| ALM ID             | Alarm Message                     | Description                                                                                                                          | Info               |
|--------------------|-----------------------------------|--------------------------------------------------------------------------------------------------------------------------------------|--------------------|
| 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:<br>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,<br>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              |
| 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                                                                                                         |                    |
| <b>Boot Loader</b> |                                   |                                                                                                                                      | <b>Tamper Flag</b> |

| ALM ID | Alarm Message                              | Description                                                                                                                                  | Info              |
|--------|--------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------|-------------------|
| 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). |                   |
| 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             |

| ALM ID          | Alarm Message                        | Description                                                                                                                                                                                                                                                     | Info |
|-----------------|--------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------|
| <b>Firmware</b> |                                      |                                                                                                                                                                                                                                                                 |      |
| 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.                                                                                                            |      |
| 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 (For L3 card, the tamper monitoring settings if incorrect are corrected. ). Otherwise there was an unexpected tamper security write protection change. |      |

| ALM ID | Alarm Message                                  | Description                                                                                                                                                                               | Info           |
|--------|------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------|
| 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.                              |                |
| 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,<br>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          |

| ALM ID | Alarm Message                 | Description                                                                               | Info  |
|--------|-------------------------------|-------------------------------------------------------------------------------------------|-------|
| 2021   | HSM was removed from chassis  | HSM was removed from host chassis just before this FW execution. HSM will be deactivated. | CS    |
| 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).                                      |       |

## 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  $\geq 75\text{C}$ , firmware re-issues ALM for activation of high temperature warning.
- > Temperature  $< 75\text{C}$
- Firmware issues ALM for deactivation of high temperature warning.

## Temperature – High Hard Tamper

When the temperature starts below  $75\text{C}$  and reaches high hard tamper limit of  $88\text{C}$  and then drops back below  $75\text{C}$  the following actions occur:

- > Same as soft tamper described above up to when card is held in soft tamper reset
- > Temperature  $> 88\text{C}$
- 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  $< 80\text{C}$
- 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  $\geq 75\text{C}$ , firmware re-issues ALM for activation of high temperature warning
- > Temperature  $< 75\text{C}$
- Firmware issues ALM for deactivation of high temperature warning
- > Temperature  $< 80\text{C}$
- 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 Tamperers During Storage

When the HSM is powered off its tamper detection is powered by the on-card battery. Some hard tamperers 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 the [lunadiag](#) utility to output the FRAM Log in order to determine the tamper information, or to pass on to Thales Group 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 the [lunadiag](#) utility to output the FRAM Log in order to determine the tamper information, or to pass on to Thales Group 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 the [lunadiag](#) utility to output the FRAM Log in order to determine the tamper information, or to pass on to Thales Group 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 the [lunadiag](#) utility to output the FRAM Log in order to determine the tamper information, or to pass on to Thales Group Technical Support.

# CHAPTER 13: HSM Updates and Upgrades

Thales Group releases periodic updates to the SafeNet Luna PCIe HSM firmware, as well as updated versions of the Luna HSM Client software. If you have recently purchased a new SafeNet Luna PCIe HSM 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 Group Customer Support Portal: <https://supportportal.thalesgroup.com>.

Depending on the model of SafeNet Luna PCIe HSM you selected at time of purchase, you may also be able to purchase upgrades to the HSM's capabilities.

The Customer Release Notes (CRN) contain important information on updates:

## > Update Considerations

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 SafeNet Luna PCIe HSM Firmware" below
- > "Updating the Luna HSM Client Software" on page 79
- > Updating the SafeNet Luna G5 Backup HSM Firmware
- > "Rolling Back the SafeNet Luna HSM Firmware" on the next page
- > "Upgrading HSM Capabilities" on page 270

## Updating the SafeNet Luna PCIe HSM Firmware

To update the firmware on a SafeNet Luna PCIe HSM, download the desired firmware version from the Thales Group Support Portal. Use LunaCM on the host workstation to apply the update. You require:

- > SafeNet Luna HSM firmware update file (<filename>.fuf) and/or
- > the firmware update authentication code file(s) (<filename>.txt)

**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.

### To update the SafeNet Luna PCIe HSM firmware

1. Copy the firmware file (<filename>.fuf) and the authentication code file (<filename>.txt) to the Luna HSM Client root directory.
  - Windows: C:\Program Files\SafeNet\LunaClient
  - Linux: /usr/safenet/lunaclient/bin
  - Solaris: /opt/safenet/lunaclient/bin

**NOTE** On some Windows configurations, you might not have authority to copy or unzip files directly into **C:\Program Files\...** If this is the case, put the files in a known location that you can reference in a LunaCM command.

2. Launch LunaCM.
3. If more than one HSM is installed, set the active slot to the Admin partition of the HSM you wish to update.  
lunacm:> **slot set -slot** <slot\_number>
4. Log in as HSM SO.  
lunacm:> **role login -name so**
5. Apply the new firmware update by specifying the update file and the authentication code file. If the files are not located in the Luna HSM Client root directory, specify the filepaths.  
lunacm:> **hsm updatefw -fuf** <filename>.fuf **-authcode** <filename>.txt

## Changing the Firmware Upgrade Permissions (Linux only)

By default, the root user and any user who is part of the **hsmusers** group can perform a firmware update. You can use this procedure to restrict firmware update operations to root only (that is, disable firmware update for members of the **hsmusers** group).

### To restrict firmware update operations to the root user only

1. Open the the **/etc/modprobe.d/k7.conf** file for editing:  
**sudoedit /etc/modprobe.d/k7.conf**
2. Change the **k7\_rootonly\_reset** option from **0** to **1**. Save the file and exit the editor.
3. Stop any processes that are using the K7 driver. Typically this means stopping the **pedclient** service, and the **luna-snmp** service, if you are using SNMP.  
**sudo systemctl stop pedclient\_service**  
**sudo systemctl stop luna-snmp**
4. Reload the driver:  
**sudo systemctl reload k7**

## Rolling Back the SafeNet Luna HSM Firmware

When updating the HSM firmware, the SafeNet Luna PCIe HSM 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!** 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 zeroizes 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 272 for details.

### To roll back the SafeNet Luna HSM firmware to the previous version

1. Check the previous firmware version that is available on the HSM.

```
lunacm:> hsm showinfo
```

2. Back up any important cryptographic objects currently stored on the HSM (see [Backup and Restore Using a G5-Based Backup HSM](#) or [Backup and Restore Using a G7-Based Backup HSM](#)).

3. At the LunaCM prompt, login as HSM SO.

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

4. Roll back the HSM firmware.

```
lunacm:> hsm rollbackfw
```

LunaCM performs an automatic restart following the rollback procedure.

5. Re-initialize the HSM and restore your partition from backup.

## Upgrading HSM Capabilities

A Secure Capability Upgrade for SafeNet Luna PCIe HSM is delivered to you as a downloaded file set. Follow the FTP instructions in the email you received from Thales Group Technical Support and unzip the files to the host workstation. The update procedure is similar to the procedure for firmware updates.

**NOTE** On some Windows configurations, you might not have authority to copy or unzip files directly into **C:\Program Files\...** If this is the case, put the files in a known location that you can reference in a LunaCM command.

You require:

- > the SafeNet Luna PCIe HSM capability upgrade file (<filename>.**cu**f)
- > the capability update authentication code file (<filename>.**tx**t)

### Installing the Capability Upgrade

Once the files are unpacked and available on the host workstation, open a command-prompt session.

#### To install the upgrade package

1. Navigate to the Luna HSM Client directory and launch LunaCM.

2. Log in as HSM SO.

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

3. Apply the new capability by specifying the upgrade file and the file containing the authorization code. If the files are not located in the SafeNet Luna Network HSM Client directory, specify the filepaths.

```
lunacm:> hsm updatecap -cuf <upgrade_file> -authcode <authcode_file>
```

4. Check that the new capability is in place.

```
lunacm:> hsm showpolicies
```

# CHAPTER 14: Functionality Modules

Functionality Modules (FMs) consist of your own custom-developed code, loaded and operating within the logical and physical security of a SafeNet Luna PCIe HSM as part of the HSM firmware. FMs allow you to customize your SafeNet Luna PCIe HSM'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 SafeNet Luna PCIe HSM 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 HSM firmware version 7.4.0 and client 7.4. See [Version Dependencies by Feature](#) for more information.

This feature has hardware dependencies described in "[Preparing the SafeNet Luna PCIe HSM to Use FMs](#)" on page 275.

This chapter contains the following sections:

- > ["FM Deployment Constraints" below](#)
- > ["Preparing the SafeNet Luna PCIe HSM to Use FMs" on page 275](#)
- > ["Building and Signing an FM" on page 278](#)
- > ["Loading an FM Into the HSM Firmware" on page 280](#)
- > ["Deleting an FM From the HSM Firmware" on page 282](#)
- > ["Recovering the HSM After FM Failure" on page 283](#)

## FM Deployment Constraints

This section describes important considerations and constraints associated with deploying your Functionality Modules (FMs). Your SafeNet Luna PCIe HSM must meet all the criteria described in "[Preparing the SafeNet Luna PCIe HSM to Use FMs](#)" on page 275.

Introducing FMs into your SafeNet Luna PCIe HSM deployment will change the functionality of certain HSM features. Please take the following constraints into consideration before using FMs:

- > ["FMs and High-Availability \(HA\)" on the next page](#)

- > ["FMs and Backup/Restore/Cloning" below](#)
- > ["FMs and HSM Firmware Rollback" on the next page](#)
- > ["FM Configuration and Remote PED" on the next page](#)
- > ["FM-Enabled HSM Cannot be Verified With CMU" on the next page](#)
- > ["Key Attributes" on the next page](#)
- > ["No EDDSA or EC\\_MONTGOMERY Private Keys with C\\_CreateObject" on the next page](#)
- > ["FM Sample Applications Dependent on General Cryptoki Samples" on the next page](#)
- > ["Memory for FMs" on page 275](#)

**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 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, 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 SafeNet Luna PCIe HSM to Use FMs" on page 275](#)), 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

It is currently not possible to back up cryptographic material from an FM-enabled SafeNet Luna PCIe HSM to a SafeNet Luna Backup HSM, or to clone those objects to a partition on a non-FM-enabled Luna HSM. To back up your important keys, you must clone key material to another FM-ready or FM-enabled Luna HSM partition, either manually using `lunacm:> partition clone` or by setting up an HA group.

Similarly, material that has been backed-up from non-FM-enabled HSMs cannot be restored onto an FM-enabled HSM 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 HSM Firmware Rollback

Enabling **HSM Policy 50** permanently disables the ability to roll back the HSM firmware to a version lower than 7.4.0. Attempting to roll back the firmware once **HSM policy 50** has been enabled will return the following error:

```
Error in execution: CKR_OPERATION_NOT_ALLOWED.
```

```
Command Result : 0x80000030 (CKR_OPERATION_NOT_ALLOWED)
```

## 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 `lunacm:>ped disconnect` and then open it again with `lunacm:>ped connect` before you can resume remote configuration.

This might be required several times during SafeNet Luna PCIe HSM setup for FMs. To prevent this, enable **HSM Policy 51: Allow SMFS Auto Activation**. 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 Group 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 SafeNet Luna PCIe HSM 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 SafeNet Luna PCIe HSM 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 SafeNet Luna PCIe HSM to Use FMs

This section provides information on how to prepare your SafeNet Luna PCIe HSM 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 to Luna HSM Firmware 7.4.0 or Higher" 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 272](#) 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 SafeNet Luna PCIe HSM hardware configuration that must be created by Thales Group at the factory. SafeNet Luna PCIe HSMs that have this configuration are "FM-ready". If your SafeNet Luna PCIe HSM is not FM-ready, contact your Thales Group representative or Thales Group Customer Support for further guidance.

#### Determining Whether the HSM is FM-Ready

Starting with release 7.4, all SafeNet Luna PCIe HSMs are FM-ready from the factory. HSMs shipped prior to 7.4 are not. To determine if your HSM is FM-ready, check the Product Part # on the PCIe card label:



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 Group representative or Thales Group Customer Support for guidance on how to obtain FM-ready hardware.

## Step 2: Update to Luna HSM Firmware 7.4.0 or Higher

To use FMs, you require HSM firmware version 7.4.0 or higher. You can download the latest software/firmware packages from the Thales Group Support Portal (see ["Updating the SafeNet Luna PCIe HSM or SafeNet Luna Backup HSM Firmware" on page 1](#)).

When you have completed the upgrade, you can check the output from `lunacm:>hsm showinfo` to ensure that the HSM is FM-ready:

```
FM HW Status ->          FM Ready
Firmware Version -> 7.4.0
```

## Step 3: Purchase and Apply the FM Capability License

To use FMs, contact your Thales Group sales representative to purchase the FM capability license. The FM license is delivered as a `.cuf` file that is specific to your HSM serial number. Refer to ["Upgrading HSM Capabilities" on page 270](#) for the procedure.

When you have activated your license on the HSM, you can use `lunacm:>hsm showinfo` to check that it is installed:

```
License Count -> 8
  1. 621000068-000 K7 Base
  2. 621010185-003 Key backup via cloning protocol
  3. 621000134-002 Enable 32 megabytes of object storage
  4. 621000135-002 Enable allow decommissioning
  5. 621000021-002 Maximum performance
  6. 621000138-001 Controlled tamper recovery
  7. 621000154-001 Enable decommission on tamper with policy off
  8. 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 SafeNet Luna PCIe HSM (see ["HSM Capabilities and Policies" on page 193](#)). Use `lunacm:>hsm showpolicies` to list HSM policies.

```
50: Allow Functionality Modules : 0
51: Allow SMFS Auto Activation : 0
52: Restrict FM Privilege Level : 0
53: Encrypt keys passing from FM to HSM : 0
```

### 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 SafeNet Luna PCIe HSM. 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 272](#) 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.

**NOTE** After setting HSM policy 50, you must add the following entry to the **Chrystoki.conf/crystoki.ini** configuration file before you can re-initialize the HSM:

```
[Misc]
LoginAllowedOnFMEnabledHSMs=1
```

### 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 PED-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 Group 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 Group 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 Group 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.
- > **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 HSM, skip this procedure.

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" on page 1 -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) : Gemalto
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 host 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](#)" below.

## 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 the **ctfm** tool provided with the Luna HSM Client software and the following procedure.

## Prerequisites

- > Your HSM must meet the criteria described in ["Preparing the SafeNet Luna PCIe HSM to Use FMs" on page 275](#).
- > **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 278](#), using the Luna HSM Client 7.4 or higher. 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 HSM Admin partition.

**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 **ctfm** on the SafeNet Luna PCIe HSM host workstation to load the FM, specifying filepaths for the FM and the signing certificate. If you have previously loaded an FM signed by the same private key, the certificate is already stored on the HSM Admin partition, and you only need to specify the certificate label. If you have more than one SafeNet Luna PCIe HSM installed, specify the Admin partition slot number for the desired HSM. You are prompted for the HSM SO credential.

```
ctfm i -f <filepath/fm_filename>.fm {-c <filepath/cert_filename>.cert | -l <stored_cert_label>} [-s <slot_number>]
```

2. Reset the HSM.

```
lunareset <dev_path>
```

```
lunacm:> 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 (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 `lunacm:> hsm restart` or the `lunareset` utility.

3. Activate the Secure Memory File System (SMFS). You are prompted for the HSM SO credential.

```
ctfm a
```

4. [Optional] Confirm the FM status.

```
ctfm q
```

## Deleting an FM From the HSM Firmware

This procedure allows the HSM SO to delete a specified FM from the HSM firmware using the **ctfm** tool provided with the Luna HSM Client software.

**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 page 280).

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 284.

### Prerequisites

- > You require the FM ID of the FM you wish to delete.

### To delete an FM from the HSM firmware

1. [Optional] Use **ctfm** to list the FMs currently loaded on the HSM and see the desired FM ID.

```
ctfm q
```

2. Delete the FM by specifying its FM ID. You are prompted for the HSM SO credential.

```
ctfm d -i <FM_ID>
```

3. [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.

```
ctfm q
```

```
[user@myLunaClient bin]# ./ctfm
Luna Functionality Module Management Utility (64-bit) v7.4.0-208. Copyright (c) 2018 SafeNet.
All rights reserved.
```

```
Getting status of the FM on all available devices
```

```
Current Functionality Module Configuration for device 0:
```

```
Serial # : 67842
```

```
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
```

4. Launch LunaCM, change the active slot to the Admin partition, and restart the HSM.

```
lunacm:> slot set -slot <Admin_slot_number>
```

```
lunacm:> 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 278), and attempt to load it onto the HSM ("[Loading an FM Into the HSM Firmware](#)" on page 280). 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.

The Luna HSM Client FM Tools include **fmrecover**, 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. Erase all FMs currently loaded on the HSM. This will leave the SMFS intact and preserve any key material you may have stored there. You must specify the SafeNet Luna PCIe HSM device node:

```
fmrecover --fm <K7_node>
```

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 2.

2. Erase the SMFS.

**CAUTION!** This will erase any cryptographic objects you have stored in the SMFS. If this is important key material, erasing the SMFS is a last resort to restore HSM functions.

```
fmrecover --smfs <K7_node>
```

3. Load your patched FM and restart the SMFS (see "[Loading an FM Into the HSM Firmware](#)" on page 280).

## 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 15: Zeroizing or Resetting the HSM to Factory Conditions

During the lifetime of a SafeNet 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 SafeNet Luna PCIe HSM to Factory Condition" on page 287](#)
- > ["Decommissioning the HSM Card" on the next page](#)
- > ["Comparing Zeroize, Decommission, and Factory Reset" on page 288](#)
- > ["Comparison of Destruction/Denial Actions" on page 288](#)
- > ["Effects of Administrative Actions on Functionality Modules" on page 284](#)
- > ["RMA and Shipping Back to Thales Group" on page 290](#)
- > ["End of Service and Disposal" on page 290](#)

## 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. SafeNet Luna HSMs do not.

In the context of SafeNet Luna HSMs, keys at rest (keys or objects that are stored in the HSM) 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
- > short the pins of the decommission header
- > 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.

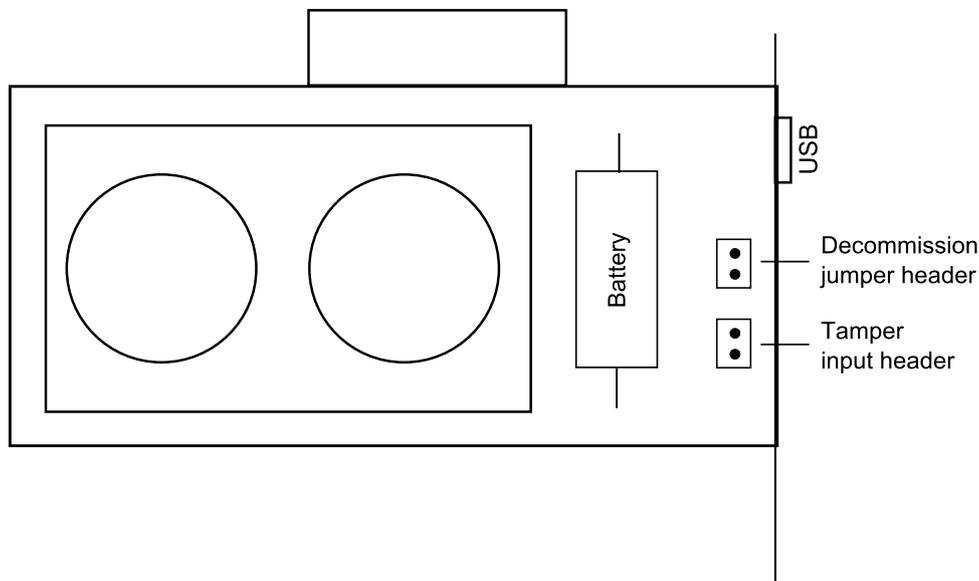
The HSM must now be re-initialized in order to use it again, and initialization overwrites the HSM with new user parameters. Everything is further encrypted with a new KEK unique to that HSM.

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 Group

## Decommissioning the HSM Card

The SafeNet Luna PCIe HSM is equipped with a two-pin decommission jumper header, as illustrated below.



By default, short-circuiting the decommission jumper header decommissions the HSM. You can use the blade of a screwdriver, or other conductive tool to short-circuit the two pins of the decommission header, or you can connect a switch to the decommission header if desired. Power is not required to decommission the HSM, that is, you can decommission the HSM after removing it from the chassis.

When you decommission a SafeNet Luna PCIe HSM, the HSM is zeroized, all user accounts are deleted, and the HSM is returned to its factory state. Any firmware or partition upgrade packs installed on the HSM are retained.

You can also set **HSM Policy 40: Decommission on Tamper** to automatically decommission the HSM for selected tamper events. See ["Tamper Events" on page 211](#) for details.

## Disabling Decommissioning

You can disable the decommissioning feature if desired, by enabling **HSM Policy 46: Disable Decommission** (see ["HSM Capabilities and Policies" on page 193](#)). The primary reason for disabling decommissioning is to prevent the HSM from being automatically decommissioned due to loss of battery (see ["Tamper Events" on page 211](#)). If decommissioning is disabled, the SafeNet Luna PCIe HSM has an indefinite shelf life, as far as the battery is concerned.

### To disable decommissioning

1. Launch LunaCM and log in as HSM SO.  
lunacm:>**role login -name so**
2. Enable **HSM Policy 46: Disable Decommission**:  
lunacm:> **hsm changehsmpolicy -policy 46 -value 1**

## Resetting the SafeNet Luna PCIe HSM to Factory Condition

These instructions will allow you to restore your SafeNet Luna PCIe HSM 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 updates, those remain in place, and are not affected by this procedure.

To roll back the HSM firmware to the previous version, see ["Rolling Back the SafeNet Luna HSM Firmware" on page 269](#).

### Prerequisites

- > Only the HSM SO can perform factory reset.

### To reset the HSM to factory condition

1. Set the active slot to the admin partition and log in as HSM SO.  
lunacm:> **slot set -slot <slotnum>**  
lunacm:> **role login -name so**
2. Reset the HSM to factory settings.  
lunacm:> **hsm factoryreset**

## Comparing Zeroize, Decommission, and Factory Reset

You can clear the contents of your HSM on demand, 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, 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>                                                                                                         | 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: <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; lunacm:&gt; <b>hsm zeroize</b></li> </ul>      | 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: <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> | 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: <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> |
| Factory Reset         | lunacm:> <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 SafeNet Luna PCIe HSM 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)

| Event                                                                                                                                                                                                                                                                                                                                                                                             | Scen. 1 | Scen. 2 | How to discover (See Note 3)                                                                                                                                                                                                                                                                                                                             | How to recover                  |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------|---------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------|
| <ul style="list-style-type: none"> <li>&gt; Three bad SO login attempts</li> <li>&gt; lunacm:&gt; <b>hsm zeroize</b></li> <li>&gt; lunacm:&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     | <ul style="list-style-type: none"> <li>&gt; Log entry</li> <li>&gt; "Partition Status -&gt; Zeroized" in HSM info (from <b>hsm showinfo</b> on admin partition)</li> </ul>                                                                                                                                                                               | Restore HSM objects from Backup |
| <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; lunacm:&gt; <b>stm transport</b></li> </ul> | YES     | NO      | <p>Parse logs for text like "tamper", "TVK was corrupted", or "Generating new TVK", indicating that a tamper event was logged. 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> | Reboot [See Note 1]             |
| <p>Decommission</p> <ul style="list-style-type: none"> <li>&gt; Short-circuiting the tamper header pins</li> </ul>                                                                                                                                                                                                                                                                                | NO      | YES     | <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.<br>1 | Scen.<br>2 | 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 178](#).

## RMA and Shipping Back to Thales Group

Although rare, it could happen that you need to ship a SafeNet appliance back to Thales Group.

Contact your Thales representative to obtain the Return Material Authorization (RMA) and instructions for packing and shipping.

You might wish (or your security policy might require you) to take maximum precaution with any contents in your HSM before it leaves your possession.

If so, there are two options available to secure the contents of the SafeNet Luna PCIe HSM before returning it to Thales Group:

- > Decommission the HSM, forcibly clearing all HSM contents (see ["Decommissioning the HSM Card" on page 286](#) for instructions).
- > Set Secure Transport Mode on the HSM (see ["Secure Transport Mode" on page 80](#) for instructions) and provide the verification string and random user string to your Thales Group representative by secure means. This will allow Thales Group to know if the HSM is tampered while in transit.

## End of Service and Disposal

SafeNet Luna HSMs and appliances are deployed into a wide variety of markets and environments. Arranging for the eventual disposal of a SafeNet Luna HSM or appliance that is no longer needed can be a simple accounting task and a call to your local computer recycling service, or it can be a complex and rigorous set of procedures intended to protect very sensitive information.

### Needs Can Differ

Some users of SafeNet Luna HSMs employ cryptographic keys and material that have a very short "shelf life". A relatively short time after the HSM is taken out of service, any objects that it contains are no longer relevant. The HSM could be disposed of, with no concern about any material that might remain in it.

The majority of our customers are concerned with their keys and objects that are stored on the HSM. It is important to them that those items never be exposed. The fact is that they are never exposed, but see below for explanations and actions that address the concerns of auditors who might be more accustomed to other ways of safeguarding HSM contents.

## SafeNet Luna HSM Protects Your Keys and Objects

The design philosophy of our SafeNet Luna HSMs ensures that contents are safe from attackers. Unlike other HSM products on the market, SafeNet Luna HSMs never store sensitive objects, like cryptographic keys, unencrypted. Therefore, SafeNet Luna HSMs have no real need - other than perception or "optics" - to perform active erasure of HSM contents, in case of an attack or tamper event.

Instead, the basic state of a SafeNet Luna HSM is that any stored keys and objects are strongly encrypted. They are decrypted only for current use, and only into volatile memory within the HSM.

If power is removed from the HSM, or if the current session closes, the temporarily-decrypted objects instantly evaporate. The encrypted originals remain, but they are unusable by anyone who does not have the correct HSM keys to decrypt them.

### How the HSM encryption keys protect your sensitive objects

In addition to encryption with the user specific access keys or passwords, all objects on the HSM are encrypted by the HSM's global key encryption key (KEK) and the HSM's unique Master Tamper Key (MTK).

If the HSM experiences a Decommission event (pressing of the small red button on back of SafeNet Luna Network HSM, or shorting of the pins of the decommission header on the HSM card, or removal of the battery while main power is not connected to a SafeNet Luna USB HSM) then the KEK is deleted.

If the HSM experiences a tamper event (physical intrusion, environmental excursion), then the MTK is destroyed.

Destruction of either of those keys instantly renders any objects in the HSM unusable by anyone. In the case of a Decommission event, when the HSM is next powered on, it requires initialization, which wipes even the encrypted remains of your former keys and objects.

We recognize that some organizations build their protocols around assumptions that apply to other suppliers' HSMs - where keys are stored unencrypted and must be actively erased in the event of an attack or removal from service. If your policies include that assumption, then you can re-initialize after Decommission - which actively erases the encrypted objects for which no decrypting key existed. For purposes of security, such an action is not required, but it can satisfy pre-existing protocols that presume a weakness not present in SafeNet Luna HSMs.