

Thales Luna Network HSM 7.7.0

HSM ADMINISTRATION GUIDE



Document Information

Product Version	7.7.0
Document Part Number	007-000553-003
Release Date	24 March 2021

Revision History

Revision	Date	Reason
Rev. A	24 March 2021	Initial release

Trademarks, Copyrights, and Third-Party Software

Copyright 2001-2021 Thales Group. All rights reserved. Thales and the Thales logo are trademarks and service marks of Thales and/or its subsidiaries and are registered in certain countries. All other trademarks and service marks, whether registered or not in specific countries, are the property of their respective owners.

Disclaimer

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

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

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

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

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

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

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

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

Thales Group does not and shall not warrant that this product will be resistant to all possible attacks and shall not incur, and disclaims, any liability in this respect. Even if each product is compliant with current security standards in force on the date of their design, security mechanisms' resistance necessarily evolves according to the state of the art in security and notably under the emergence of new attacks. Under no circumstances, shall Thales Group be held liable for any third party actions and in particular in case of any successful attack against systems or equipment incorporating Thales products. Thales Group disclaims any liability with respect to security for direct, indirect, incidental or consequential damages that result from any use of its products. It is further stressed that independent testing and verification by the person using the product is particularly encouraged, especially in any application in which defective, incorrect or insecure functioning could result in damage to persons or property, denial of service, or loss of privacy.

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

Regulatory Compliance

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

USA, FCC

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

Canada

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

Europe

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

CONTENTS

Preface: About the HSM Administration Guide	9
Customer Release Notes	9
Audience	10
Document Conventions	10
Support Contacts	12
Chapter 1: Secure Transport Mode	13
Recovering an HSM From Secure Transport Mode	15
Placing an HSM Into Secure Transport Mode	16
Chapter 2: PED Authentication	17
PED Authentication Architecture	17
Comparing Password and PED Authentication	18
PED Keys	19
PED Key Types and Roles	19
Shared PED Key Secrets	21
M of N Split Secrets (Quorum)	23
PED-Authenticated HSMs with Firmware 7.7.0 (and newer)	24
New-series PED Behavior Notes	24
Updating or Rolling-back PED-auth HSM Firmware	25
Luna PED Received Items	25
Luna PED Hardware Functions	27
Physical Features	27
Keypad Functions	28
Modes of Operation	29
PED with Newer CPU (AC Power Block Now Optional)	30
Local PED Setup	31
Secure Local PED	32
About Remote PED	32
Remote PED Architecture	33
PEDserver-PEDclient Communications	37
Initializing the Remote PED Vector and Creating an Orange Remote PED Key	38
Installing PEDserver and Setting Up the Remote Luna PED	41
Opening a Remote PED Connection	43
Ending or Switching the Remote PED Connection	51
Remote PED Troubleshooting	52
Migrating the Orange Remote PED Key For Luna 7.7.0 or Newer	56
Migrating the Orange RPK(s) Using a Local PED Connection	58
Updating Luna PED Firmware (for older-version PED that requires a power-block)	59
Updating Luna PED Firmware (for USB-powered PED)	62

Preparing for the Upgrade	63
Upgrading the Luna PED Firmware to Version 2.9.0 (or newer)	64
PED Key Management	65
Creating PED Keys	65
Performing PED Authentication	70
Consequences of Losing PED Keys	72
Identifying a PED Key Secret	74
Duplicating Existing PED Keys	75
Changing a PED Key Secret	76
PEDserver and PEDclient	79
The PEDserver Utility	79
The PEDclient Utility	79
pedserver	80
pedserver appliance	81
pedserver appliance delete	82
pedserver appliance list	83
pedserver appliance register	84
pedserver mode	85
pedserver mode config	86
pedserver mode connect	88
pedserver mode disconnect	89
pedserver mode show	90
pedserver mode start	92
pedserver mode stop	94
pedserver regen	96
pedclient	96
pedclient mode assignid	98
pedclient mode config	99
pedclient mode deleteid	101
pedclient mode releaseid	102
pedclient mode setid	103
pedclient mode show	104
pedclient mode start	105
pedclient mode stop	107
pedclient mode testid	108
Chapter 3: Audit Logging	109
Audit limitations and Controlled tamper recovery state	112
The Audit Role	112
Audit Log Records	115
Audit Log Message Format	116
Audit Logging General Advice and Recommendations	119
Logging In as Auditor	120
Configuring and Using Audit Logging	121
Configuring Audit Logging	121
Copying Log Files Off the Appliance	124
Exporting the Audit Logging Secret and Importing to a Verifying HSM	124

Reading the Audit Log Records	126
Audit Role Authentication Considerations	126
Remote Audit Logging	126
Changing the Auditor Credential	127
Audit Log Categories and HSM Events	128
Audit Log Troubleshooting	135
Chapter 4: Initializing the HSM	136
Initializing a New or Factory-reset HSM	136
Re-initializing the HSM	139
PED-authenticated HSM Initialization Example	139
Password-authenticated HSM Initialization Example	145
Chapter 5: HSM Roles	147
Logging In as HSM Security Officer	148
Changing the HSM SO Credential	148
Chapter 6: HSM Capabilities and Policies	150
Setting HSM Policies Manually	160
Setting HSM Policies Using a Template	160
Creating an HSM Policy Template	161
Editing an HSM Policy Template	161
Applying an HSM Policy Template	162
Chapter 7: Application Partitions	163
Creating or Deleting an Application Partition	163
Customizing Partition Sizes	164
Re-sizing an Existing Partition	165
Chapter 8: Security in Operation	167
Security Effects of Administrative Actions	167
Tamper Events	172
Recovering from a Tamper Event	173
Chapter 9: Monitoring the HSM	175
HSM Status Values	175
System Operational and Error Messages	176
Performance Monitoring	178
Partition Utilization Metrics	179
Rules of acquisition	179
Availability of Partition Utilization Metrics	180
Keycard and Token Return Codes	181
Library Codes	199
Vendor-Defined Return Codes	203
HSM Alarm Codes	209
Alarm Generation and Handling	210
FRAM LOG	211

List of HSM Alarm Codes	211
HSM Alarm Code Samples	215
Temperature - High Warning	216
Temperature – High Soft Tamper	216
Temperature – High Hard Tamper	216
Hard Tamperers During Storage	217
Decommission with power on	218
Stored Data Integrity	219
Chapter 10: HSM Updates and Upgrades	221
Updating the Luna HSM Firmware	221
Rolling Back the Luna HSM Firmware	223
Upgrading HSM Capabilities and Partition Licenses	224
Upgrade Options	225
Purchasing an Upgrade License	226
Activating a License on the Thales Licensing Portal	228
Managing Your Thales Licensing Portal Account	232
Applying an Upgrade License on the HSM	236
Upgrade Troubleshooting	237
Chapter 11: Functionality Modules	238
FM Deployment Constraints	238
FMs and FIPS Mode	239
FMs and High-Availability (HA)	239
FMs and Backup/Restore/Cloning	240
FMs and Secure Trusted Channel (STC)	240
FMs and Appliance Re-imaging	240
FMs and HSM Firmware Rollback	241
FM Configuration and Remote PED	241
FM-Enabled HSM Cannot be Verified With CMU	241
Key Attributes	241
No EDDSA or EC_MONTGOMERY Private Keys with C_CreateObject	241
FM Sample Applications Dependent on General Cryptoki Samples	241
Memory for FMs	242
Preparing the Luna Network HSM to Use FMs	242
Step 1: Ensure You Have FM-Ready Hardware	242
Step 2: Update to Luna Appliance Software and HSM Firmware 7.4.0 or Higher	243
Step 3: Purchase and Apply the FM Capability License	243
Step 4: Apply HSM Policy Settings	243
Building and Signing an FM	244
Loading an FM Into the HSM Firmware	248
Deleting an FM From the HSM Firmware	249
Recovering the HSM After FM Failure	250
Effects of Administrative Actions on Functionality Modules	251
Chapter 12: Zeroizing or Resetting the HSM to Factory Conditions	253
HSM Zeroization	253

Resetting the Luna Network HSM to Factory Condition 254
Comparing Zeroize, Decommission, Re-image, and Factory Reset 255
Comparison of Destruction/Denial Actions 256
Stored Data Integrity 257

PREFACE: About the HSM Administration Guide

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

- > ["Secure Transport Mode" on page 13](#)
- > ["PED Authentication" on page 17](#)
- > ["Audit Logging" on page 109](#)
- > ["Initializing the HSM" on page 136](#)
- > ["HSM Roles" on page 147](#)
- > ["HSM Capabilities and Policies" on page 150](#)
- > ["Application Partitions" on page 163](#)
- > ["Security in Operation" on page 167](#)
- > ["Monitoring the HSM" on page 175](#)
- > ["HSM Updates and Upgrades" on page 221](#)
- > ["Functionality Modules" on page 238](#)
- > ["Zeroizing or Resetting the HSM to Factory Conditions" on page 253](#)

The preface includes the following information about this document:

- > [Customer Release Notes](#)
- > ["Audience" on the next page](#)
- > ["Document Conventions" on the next page](#)
- > ["Support Contacts" on page 12](#)

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 Luna HSM users and security officers, key manager administrators, and network administrators.

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

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

Document Conventions

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

Notes

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

NOTE Take note. Contains important or helpful information.

Cautions

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

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

Warnings

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

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

Command syntax and typeface conventions

Format	Convention
bold	<p>The bold attribute is used to indicate the following:</p> <ul style="list-style-type: none"> > Command-line commands and options (Type dir /p.) > Button names (Click Save As.) > Check box and radio button names (Select the Print Duplex check box.) > Dialog box titles (On the Protect Document dialog box, click Yes.) > Field names (User Name: Enter the name of the user.) > Menu names (On the File menu, click Save.) (Click Menu > Go To > Folders.) > User input (In the Date box, type April 1.)
<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 keywords 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> <c>}	Represent required alternate keywords 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> <c>]	Represent optional alternate keywords or variables in a command line description. Choose one command line argument enclosed within the braces, if desired. Choices are separated by vertical (OR) bars.

Support Contacts

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

Customer Support Portal

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

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

Telephone

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

CHAPTER 1: Secure Transport Mode

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

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

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

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

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

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

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. This information applies to the HSM card only; STM does not affect appliance functions.
- > 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 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 HSMor, 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 172](#).

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 148). 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:

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

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

4. You are presented with a verification string:

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 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 148).
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:

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

4. After confirming the action, you are presented with:
 - **Verification String:** <XXXX-XXXX-XXXX-XXXX>
 - **Random User String:** <XXXX-XXXX-XXXX-XXXX>

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

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

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 2: PED Authentication

The Luna PIN Entry Device (Luna PED) provides PIN entry and secret authentication to a 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 Luna Network HSM 7.x requires Luna PED firmware version 2.7.1 or higher. This firmware is backward-compatible with Luna Network 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 19](#)
 - ["PED Key Types and Roles" on page 19](#)
 - ["Shared PED Key Secrets" on page 21](#)
 - ["Domain PED Keys" on page 22](#)
 - ["PED PINs" on page 22](#)
 - ["M of N Split Secrets \(Quorum\)" on page 23](#)
- > ["Luna PED Received Items" on page 25](#)
- > ["Luna PED Hardware Functions" on page 27](#)
- > ["Updating Luna PED Firmware \(for older-version PED that requires a power-block\)" on page 59](#)
- > ["Local PED Setup" on page 31](#)
- > ["About Remote PED" on page 32](#)
- > [Remote PED Setup](#)
- > ["PED Key Management" on page 65](#)
- > ["PEDserver and PEDclient" on page 79](#)

PED Authentication Architecture

The PED Authentication architecture consists of the following components:

- > **Luna PED:** a PIN Entry Device with a local or remote connection to the HSM. The PED reads authentication secrets from PED keys on behalf of an HSM or partition (see ["Luna PED Hardware Functions" on page 27](#)).
- > **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 21](#).
 - **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 22](#).
 - **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 23](#).

Comparing Password and PED Authentication

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

	Password-authentication	PED-authentication
Ability to restrict access to cryptographic keys	<ul style="list-style-type: none"> > Knowledge of role password is sufficient > For backup/restore, knowledge of partition domain password is sufficient 	<ul style="list-style-type: none"> > Ownership of the black Crypto Officer PED key is mandatory > For backup/restore, ownership of both black CO and red domain PED keys is mandatory > The Crypto User role is available to restrict access to read-only, with no key management authority > Option to associate a PED PIN with any PED key, imposing a two-factor authentication requirement on any role
Dual Control	<ul style="list-style-type: none"> > Not available 	<ul style="list-style-type: none"> > 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
Key-custodian responsibility	<ul style="list-style-type: none"> > Password knowledge only 	<ul style="list-style-type: none"> > Linked to partition password knowledge > Linked to black PED key(s) ownership and optional PED PIN knowledge

	Password-authentication	PED-authentication
Two-factor authentication for remote access	> Not available	> Remote PED and orange (Remote PED Vector) PED key deliver highly secure remote management of HSM, including remote backup

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 65.




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

Lifecycle	PED Key	PED Secret	Function
HSM Administration	Blue	HSM Security Officer (HSM SO) secret	Authenticates the HSM SO role. The HSM SO manages provisioning functions and security policies for the HSM. Mandatory
	Red 	HSM Domain or Key Cloning Vector	Cryptographically defines the set of HSMs that can participate in cloning for backup. See " Domain PED Keys " on page 22. Mandatory
	Orange 	Remote PED Vector	Establishes a connection to a Remote PED server. See * below table. Optional
HSM Auditing	White 	Auditor (AU) secret	Authenticates the Auditor role, responsible for audit log management. This role has no access to other HSM services. Optional
Partition Administration	Blue	Partition Security Officer (PO) secret	Authenticates the Partition SO role. The PO manages provisioning activities and security policies for the partition. NOTE: If you want the HSM SO to also perform Partition SO duties, you can use the same blue key to initialize both roles. Mandatory
	Red 	Partition Domain or Key Cloning Vector	Cryptographically defines the set of partitions that can participate in cloning for backup or high-availability. See " Domain PED Keys " on page 22. Mandatory

Lifecycle	PED Key	PED Secret	Function
Partition Operation	Black 	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. Mandatory
	Gray 	Limited Crypto Officer (LCO) secret **	Authenticates the Limited Crypto Officer role. The LCO can perform a subset of the actions available to the Crypto Officer. Optional (used in eIDAS-compliant schemes)
	Gray 	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. NOTE: 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. Optional

*

NOTE Orange PED Keys (RPK) for use with HSMs at firmware 7.7 or newer, with enhanced security to address modern threat environments and to comply with updated standards, have increased infrastructure onboard the key. If such an initialized RPK is overwritten to become a different role PED Key (example SO), this process that formerly would take about six seconds now takes about 36 seconds.

**

NOTE

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

Shared PED Key Secrets

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

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

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

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

Domain PED Keys

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

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

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

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

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 65). Copies made later are true copies with the same PED PIN, intended as backups for one person (see "[Duplicating Existing PED Keys](#)" on page 75). 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 72.

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 (any three in this 3 of 5 scenario, but cannot be the same key presented more than once during an authentication attempt).

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 - Partition Policy 22), 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. A further measure called Auto-Activation (Partition Policy 23) can cache the authenticated state as long as two hours, allowing automatic, hands-off resumption of operation.

PED-Authenticated HSMs with Firmware 7.7.0 (and newer)

HSM 7.7.0 and associated PEDs introduce new communications security protocols for compliance with evolving standards.

Updated HSMs need updated PEDs

An HSM at firmware 7.7.0 or newer requires connection with a PED that has f/w 2.7.4 (old PED series with power block) or f/w 2.9.0 (newer PED series with USB power).

Two PED-firmware update packages are available. Old-series PEDs (f/w 2.6.x through 2.7.2) have an upgrade path to PED f/w version 2.7.4.

New-series PEDs (f/w 2.8.x) have an upgrade path to PED f/w version 2.9.0.

When an HSM is at f/w version 7.7.0 or newer, it verifies that any connecting PED is at PED f/w 2.7.4 or 2.9.0, respectively, or the HSM refuses the connection and issues an error (LUNA_RET_PED_UNSUPPORTED_PROTOCOL).

Earlier version HSMs function with updated PEDs

A PED at f/w version 2.7.4 (older-series powered by power-block) or 2.9.0 (newer-series USB-powered) is able to work with updated HSMs *and* with older HSMs.

The result is that an updated PED can function with older HSMs (HSM f/w 5.x and 6.x) that will not be updated with the new PED communication protocols, or with earlier f/w 7.x HSMs that have yet to be updated for compliance with current eIDAS/Common Criteria and NIST standards.

This means that, if you have PED-Authenticated version pre-7.7.0 HSMs that are to be updated to f/w 7.7.0 (or newer), then you must update at least one PED first, so that you can continue to authenticate to roles on the HSM while updating.

Orange PED Keys have changed

The RPV of an orange PED Key, created with PED firmware 2.7.4 or 2.9.0 against a firmware 7.7.0 HSM has additional features compared to previous RPVs, necessary for current authentication standards. An older PED can use a newer RPV without issue (unaware of the additional crypto components). An older PED can duplicate a newer RPV onto another orange key, but only imprinting the older components - the newer security components are lost. The duplicated RPV can then be used with pre-firmware-7.7.0 HSMs, but since the newer security components are missing, the 'duplicate' orange key (and any copy of it) cannot be used with HSMs at version 7.7.0 or newer.

However, when updating PEDs and HSM firmware, existing orange PED Keys can be migrated to the new format. The same is true for a newer-style RPV that had the newer security components stripped by copying with a non-updated PED.

A blank orange PED Key receiving a new Remote PED Vector (RPV) must have the operation performed over a local connection between PED and HSM.

New-series PED Behavior Notes

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

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

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

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

Updating or Rolling-back PED-auth HSM Firmware


After a version 7.x HSM is updated to f/w version 7.7.0, or rolled back to an earlier f/w version, a USB-connected PED should be power cycled. Without this action, attempted operations against the HSM can result in "device error".

Luna PED Received Items

This chapter describes the items you received with your Luna PED device. For instructions on setting up the PED, see ["PED Authentication" on page 17](#).

Required Items

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

Qty	Item
1	Luna PED (with firmware 2.7.1 or newer) 

Qty	Item
1	<p data-bbox="212 268 1474 331">PED Power Supply 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">NOTE: 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 1008">Cable, USB 2.0, Type A to Mini B connectors (for Remote PED operation).</p> 

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

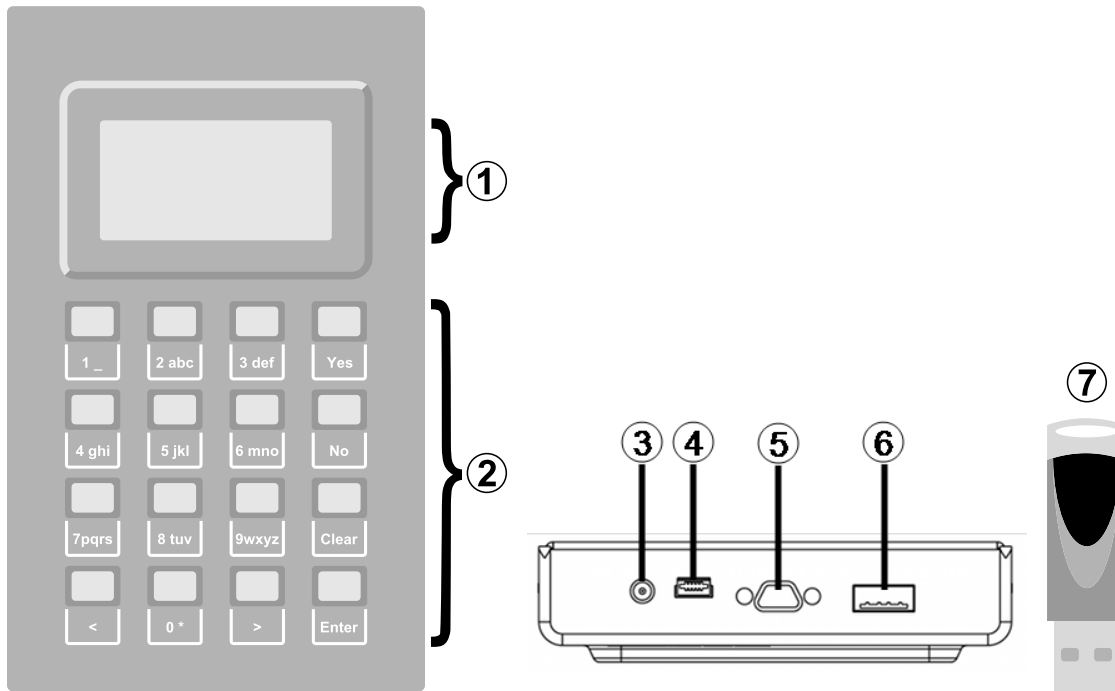
Luna PED Hardware Functions

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

- > ["Physical Features" below](#)
- > ["Keypad Functions" on the next page](#)
- > ["Modes of Operation" on page 29](#)
- > ["Admin Mode Functions" on page 30](#)
- > ["PED with Newer CPU \(AC Power Block Now Optional\)" on page 30](#)

Physical Features

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



1	Liquid Crystal Display (LCD), 8 lines.
2	Keypad for command and data entry. See "Keypad Functions" below .
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
Clear	<ul style="list-style-type: none"> > Clear the current entry, such as when entering a PED PIN > 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
<	<ul style="list-style-type: none"> > Backspace: clear the most recent digit you typed on the PED > Exit: return to the previous PED menu
>	<ul style="list-style-type: none"> > Log: displays the most recent PED actions (since entering Local or Remote Mode)
Numeric keys	<ul style="list-style-type: none"> > Select numbered menu items > Input PED PINs
Yes and No	<ul style="list-style-type: none"> > Respond to Yes or No questions from the PED
Enter	<ul style="list-style-type: none"> > Confirm an action or entry

Modes of Operation

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

- > **Local PED-SCP:** This mode is reserved for legacy Luna 6.x HSMs that use an MDSM connector between the PED and the HSM. It does not apply to Luna 7.x. Initial HSM configuration must be done in Local PED mode. See "[Local PED Setup](#)" on page 31 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 Luna Network HSM to be located in a data center or other location restricting physical access. See "[About Remote PED](#)" on page 32 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 Luna Network HSM card, or LunaSH/LunaCM will return an error (CKR_DEVICE_ERROR) when you attempt authentication.

Admin Mode Functions

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

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

< EXIT
```

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

PED with Newer CPU (AC Power Block Now Optional)

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

The older PED was shipped with an AC adapter.

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

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

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

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

Local PED Setup

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

Setting Up a Local PED Connection

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

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



2. 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 29](#).

The Luna PED is now ready to perform authentication for the HSM. You may proceed with setting up or deploying your Luna Network 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 LunaSH or LunaCM command (see ["Performing PED Authentication" on page 70](#))
- > Create copies of your PED keys (see ["Duplicating Existing PED Keys" on page 75](#))
- > Change to the Admin Mode to run tests or update PED software (see ["Changing Modes" on page 29](#))
- > Prepare to set up a Remote PED server (see ["About Remote PED" below](#))

Secure Local PED

PED firmware can be updated to version 2.7.4 in the PED with older CPU, and to version 2.9.0 in the PED with new CPU.

- > The firmware update
 - is optional and continues to work just fine, with older PED-auth HSMs, and with 7.x HSMs with firmware versions less than 7.7.0,
 - while also being *required* to work with HSMs at firmware 7.7.0 and newer.
- > The PED firmware update is mandatory before updating or using any HSM with firmware 7.7.0 or newer. This combination complies an eIDAS-related requirement for an updated secure channel.
- > The updated secure channel for Remote PED operation is now also replicated in the local channel, but because it is local it does not need to be mediated via an orange PED Key. The PED, however, sees both local and remote connections as equivalent.

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

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 37](#)

Remote PED Architecture

The Remote PED architecture consists of the following components:

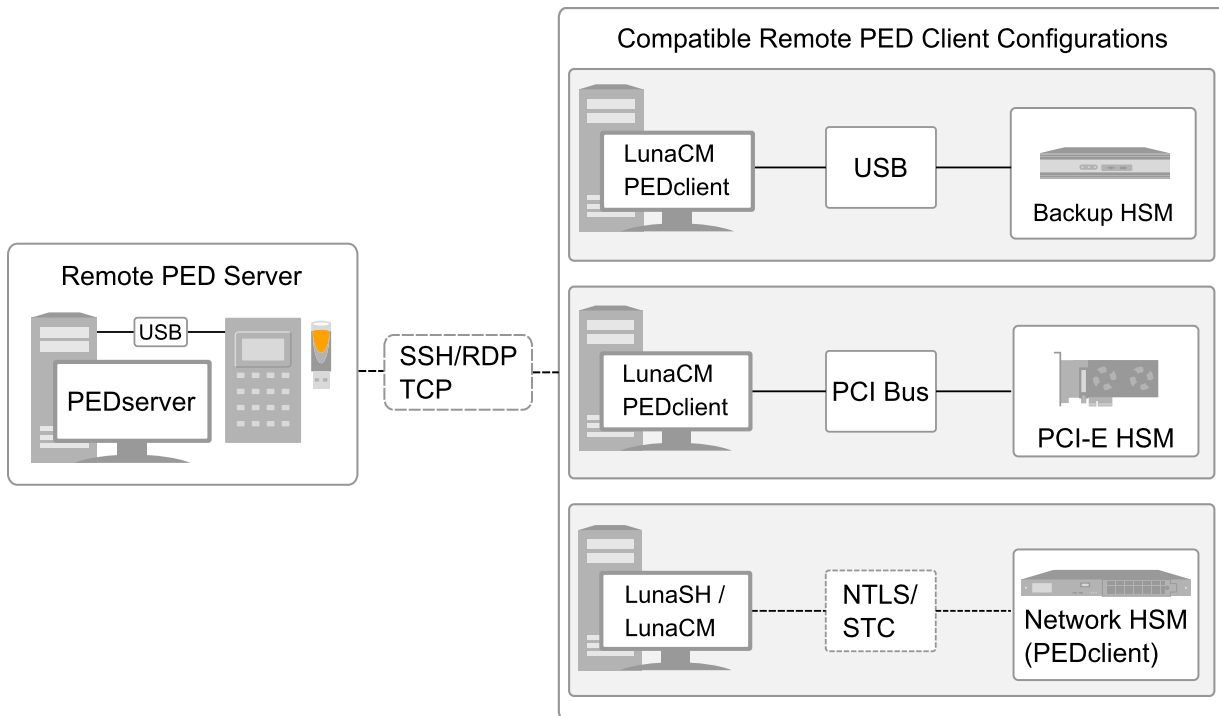
- > **Remote PED:** a Luna PED with firmware 2.7.1 or newer, connected to a network-connected workstation, powered on, and set to Remote PED mode.

NOTE Luna PED firmware versions

- 2.7.4 for PEDs that require the external power block, and
- 2.9.0 for USB-powered PEDs

are required for the enhanced connection security and NIST SP 800-131A Rev.1 compliance implemented with Luna HSM 7.7.0 and newer.

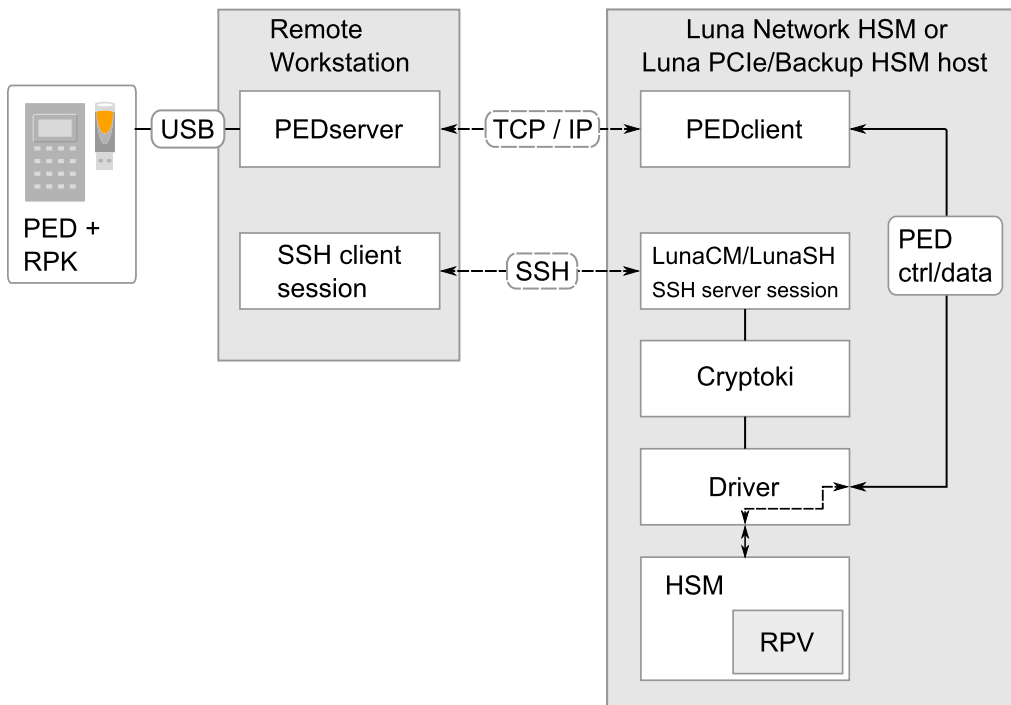
- > **Remote PED Vector (RPV):** a randomly generated, encrypted value used to authenticate between a Remote PED (via PEDserver) and a Luna HSM (via PEDclient).
- > **Remote PED Key (RPK):** an orange PED key containing an RPV (or multiple PED keys with a split RPV in an M of N quorum implementation).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



Remote PED Connections

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

- > PEDServer is running
- > a 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



Bi-directionality

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

- > **HSM-initiated:** When the HSM requires authentication, it sends (via PEDclient) a request for PED services to the Remote PED host (which receives the request via PEDserver). This requires that the Luna Network HSM be allowed to initiate external connections, and that the PEDserver IP port remains open. If the Luna Network HSM resides behind a firewall with rules prohibiting these connections, or if your IT policy prohibits opening a port on the Remote PED host, use a PED-initiated connection. See "[HSM-Initiated Remote PED](#)" on page 43.
- > **PED-initiated:** The HSM and Remote PED host exchange and register certificates, creating a trusted connection. This allows the Remote PED host (via PEDserver) to initiate the connection to the Luna Network HSM. If you have firewall or other constraints that prevent your HSM from initiating a connection to a Remote PED in the external network, use this connection method. See "[PED-Initiated Remote PED](#)" on page 47.

The following constraints apply to PED-initiated connections:

- > A maximum of 20 Remote PED servers can be registered in PEDclient.
- > A maximum of 80 Network HSM appliances can be registered in PEDserver.
- > If the connection is terminated abnormally (for example, a router switch died), there is no auto-reconnection. PEDserver automatically restarts and runs in HSM-initiated connection mode.
- > When running in PED-initiated connection mode, PEDserver does not listen for new HSM-initiated connections, for security and to simplify usability.

Priority and Lockout

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

When a Remote PED connection is active, the Local PED connection is ignored, and all authentication requests are routed to the Remote PED. Attempts to connect to a different Remote PED server are refused until the current connection times out or is deliberately ended. See ["Ending or Switching the Remote PED Connection" on page 51](#).

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 51](#).

Timeout

PEDserver and PEDclient both have configurable timeout settings (default: 1800 seconds). See ["pedserver mode config" on page 86](#) or ["hsm ped timeout" on page 1](#). The utilities are not aware of each other's timeout values, so the briefer value determines the actual timeout duration. Timeout does not apply to PED-initiated Remote PED connections.

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

Broken Connections

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

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

```

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

```

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

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.

PEDServer Configuration File

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

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

```
[Appliances]
ServerCAFile=C:\Program Files\SafeNet\LunaClient\cert\PedServerCAFile.pem
SSLConfigFile=C:\Program Files\SafeNet\LunaClient\openssl.cnf
```

```

ServerName00=myHSM
ServerIP00=192.20.11.78
ServerPort00=9697
CommonCertName00=66331
[RemotePed]
AdminPort=1502
BGProcessShutdownTimeoutSeconds=25
BGProcessStartupTimeoutSeconds=10
ExternalAdminIF=0
ExternalServerIF=1
IdleConnectionTimeoutSeconds=1800
InternalShutdownTimeoutSeconds=10
LogFileError=1
LogFileInfo=1
LogFileName=C:\Program Files\SafeNet\LunaClient\remotePedServerLog.log
LogFileTrace=0
LogFileWarning=1
MaxLogFileSize=4194304
PingInterval=1
PongTimeout=5
RpkSerialNumberQueryTimeout=15
ServerPortValue=1503
SocketReadRspTimeoutSeconds=60
SocketReadTimeoutSeconds=60
SocketWriteTimeoutSeconds=15

```

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

```

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

```

Initializing the Remote PED Vector and Creating an Orange Remote PED Key

The Remote PED (via PEDserver) authenticates itself to the Luna Network HSM 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 Luna Network HSM administrator can create this key using one of the following two methods:

- > **Local RPV Initialization:** The RPV is initialized using a Luna PED connected to the USB port on the HSM card. This is the standard method of initializing the RPV.

See "[Local RPV Initialization](#)" on the next page.

- > **Remote RPV Initialization:** The RPV is initialized using a Luna PED connected to a remote workstation running PEDserver. A one-time numeric password is used to authenticate the Remote PED to the HSM before initializing the RPV. This optional method is useful if the HSM SO has only remote SSH access to the appliance. It is available only if the HSM is in a zeroized state (uninitialized) and your firewall settings allow an HSM-initiated Remote PED connection. If you choose this method, you will set up Remote PED before initializing the RPV ("[Remote RPV Initialization](#)" on page 40).

Continue to "[Installing PEDserver and Setting Up the Remote Luna PED](#)" on page 41.

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

Local RPV Initialization

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

- > Luna PED with 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 65](#) for more information.

NOTE Orange PED Keys (RPK) for use with HSMs at firmware 7.7 or newer, with enhanced security to address modern threat environments and to comply with updated standards, have increased infrastructure onboard the key. If such an initialized RPK is overwritten to become a different role PED Key (example SO), this process that formerly would take about six seconds now takes about 36 seconds.

To initialize the RPV and create the orange PED key locally

1. If you have not already done so, set up a Local PED connection (see ["Local PED Setup" on page 31](#)).
2. Using a serial or SSH connection, log in to the Luna Network HSM appliance as **admin**.
3. If the HSM is initialized, login as HSM SO (see ["Logging In as HSM Security Officer" on page 148](#)). If not, skip to the next step.

```
lunash:> hsm login
```

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

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

5. Attend to the Luna PED and respond to the on-screen prompts. See ["Creating PED Keys" on page 65](#) 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" on the next page](#).

Remote RPV Initialization

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

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

NOTE This feature requires minimum Luna Network HSM appliance software version 7.2.0 and Luna HSM Client 7.2.0. See [Version Dependencies by Feature](#) for more information.

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

- > A blank or reusable orange PED key (or multiple keys, if you plan to make extra copies or use an M of N security scheme). See ["Creating PED Keys" on page 65](#) for more information.
- > The HSM must be in a zeroized state and the RPV uninitialized.

To initialize the RPV and create the orange key remotely

1. Open an HSM-initiated Remote PED connection.

```
lunash:> hsm ped connect
```

The Remote PED connection command prepares to secure the connection and LunaSH returns the following message:

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

```
Enter PED Password:
```

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

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

```
SLOT
COMPUTE SESSION KEY.

Enter PED Password.

*****█
```


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

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

4. Attend to the Luna PED and respond to the on-screen prompts. See "[Creating PED Keys](#)" on page 65 for a full description of the key-creation process.

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

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

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

You may now initialize the HSM. See "[Initializing the HSM](#)" on page 136 for more information.

NOTE After creating the orange (Remote PED Vector) key for an HSM using the single-session, one-time password authenticated PED connection that is used to create the key, the PED prompts for the one-time password when you end the session using **ped disconnect**. You can ignore the prompt. The PED session is disconnected properly by pressing the Enter key on the PED, without entering the password.

Installing PEDserver and Setting Up the Remote Luna PED

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

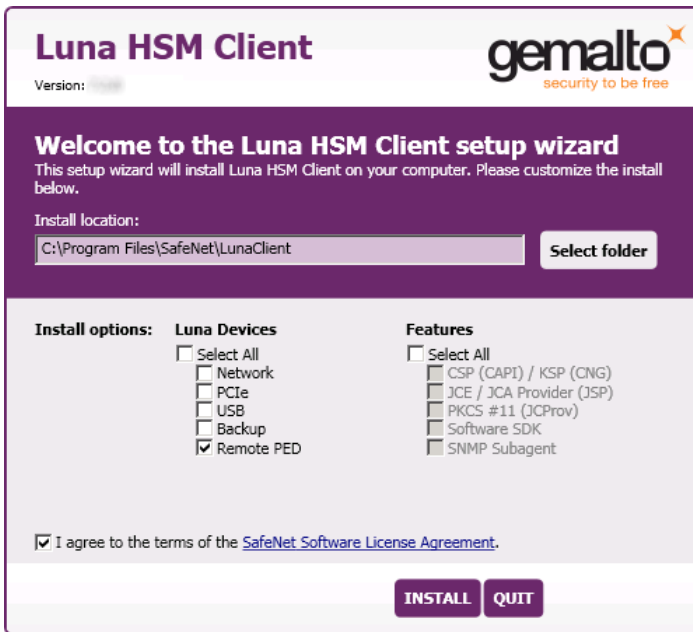
- > Network-connected workstation with compatible operating system (refer to the release notes)
- > Luna HSM Client installer
- > Luna PED with firmware 2.7.1 or higher
- > USB mini-B to USB-A connector cable
- > Luna PED DC power supply (PED 2.7.1 only; PED 2.8 and higher is powered by the USB connection)

NOTE To set up a Remote PED Server on Linux, you require Luna HSM Client 10.1.0 or newer.

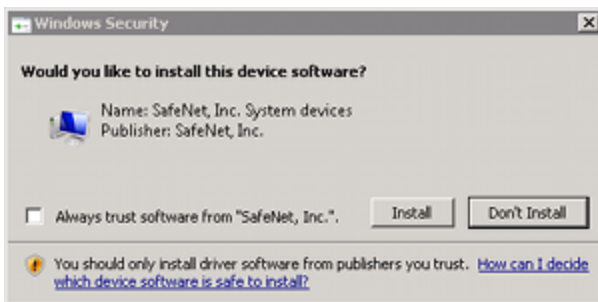
To install PEDserver and the PED driver, and set up the Luna PED

1. Run the Luna HSM Client installer and follow the on-screen instructions, as detailed in [Luna HSM Client Software Installation](#), and select the **Luna Remote PED** option. Any additional installation choices are

optional, for the purpose of this procedure.



2. On Windows, 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 29.

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

- c. Reconnect the Luna PED.

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

Opening a Remote PED Connection

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

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

See ["HSM-Initiated Remote PED" below](#).

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

See ["PED-Initiated Remote PED" on page 47](#).

NOTE For the 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 52](#).

HSM-Initiated Remote PED

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

- > Administrative access to a network-connected workstation with PEDserver installed and Luna PED connected (see ["Installing PEDserver and Setting Up the Remote Luna PED" on page 41](#))
- > Administrative access to the Luna Network HSM via SSH (if using Remote PED for HSM-level authentication)
- > Administrative access to a Luna HSM Client workstation with an assigned user partition (if using Remote PED for partition-level authentication)
- > One of the following:
 - Orange PED key with the HSM's RPV (see ["Initializing the Remote PED Vector and Creating an Orange Remote PED Key" on page 38](#))
 - Blank orange PED key (or multiple keys, if you plan to use an M of N scheme)

To launch PEDserver

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

2. Navigate to the Luna HSM Client install directory.

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

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

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

> **"pedserver mode start" on page 92 [-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 90**

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

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

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

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

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

Client Information:        Not Available

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

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

```

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

```

Show command passed.

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

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

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

To open a Remote PED connection from the Luna Network HSM appliance (LunaSH)

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

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

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

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

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

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

```
Enter PED Password:
```

See ["Remote RPV Initialization" on page 40](#) for this procedure.

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

```

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

```

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

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

The HSM-initiated Remote PED connection is now open.

3. Verify the Remote PED connection by entering a command that requires PED authentication.

- If the HSM is already initialized and you have the blue HSM SO key, you can use `lunash:> hsm login`.
- If the HSM is uninitialized, you can initialize it now with `lunash:> hsm init -label <label>`. Have blank or reusable blue and red PED keys ready (or multiple blue and red keys for M of N or to make multiple copies). See "[Creating PED Keys](#)" on page 65 for more information.

NOTE The HSM-initiated Remote PED connection eventually times out (default: 1800 seconds), and must be re-initiated each time authentication is required. To simplify this process, you can set a default IP address and/or port for LunaSH to use each time you connect. To drop the Remote PED connection manually, see "[Ending or Switching the Remote PED Connection](#)" on page 51.

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

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

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

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

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

NOTE If you want to use the Remote PED to authenticate a different HSM, you must first drop the current connection. See "[Ending or Switching the Remote PED Connection](#)" on page 51.

To open a Remote PED connection from a client workstation (LunaCM)

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

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

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

```
Command Result : No Error
```

3. Issue the first command that requires authentication.

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

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

- If the partition is uninitialized, you can initialize it now. Have blank or reusable blue and red PED keys ready (or multiple blue and red keys for MofN or for multiple copies). See "[Creating PED Keys](#)" on page 65 for more information on creating PED keys.

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

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

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

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

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

NOTE The HSM-initiated Remote PED connection eventually times out (default: 1800 seconds), and must be re-initiated each time authentication is required. To simplify this process, you can set a default IP address and/or port for LunaCM to use each time you connect. To drop the Remote PED connection manually, see ["Ending or Switching the Remote PED Connection" on page 51](#).

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

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

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

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

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

NOTE If you want to use the Remote PED to authenticate a different HSM, you must first drop the current connection. See ["Ending or Switching the Remote PED Connection" on page 51](#).

PED-Initiated Remote PED

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

- > Administrative access to a network-connected workstation with PEDserver installed and Luna PED connected (see ["Installing PEDserver and Setting Up the Remote Luna PED" on page 41](#))

- > Orange PED key with the HSM's RPV (see ["Initializing the Remote PED Vector and Creating an Orange Remote PED Key" on page 38](#))
- > Administrative access to the Luna Network HSM via SSH

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

To open a PED-initiated Remote PED connection

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

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

> **"pedserver regen" on page 96 -commonname <name>**

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

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

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

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

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

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

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

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

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

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


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

```
>pscp .\cert\client\

```

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

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

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

```
>"pedserver appliance register" on page 84 -name <appliance_name> -certificate <cert_filename> -
ip <appliance_IP> -port <port>
```

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

8. Register the PEDserver host certificate.

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

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

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

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

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

```
>"pedserver mode connect" on page 88 -name <appliance_name>
```

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

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

```
Successfully connected to myLunaHSM.
```

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

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

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

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

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

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

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

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

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

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

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

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

Workaround when you need PED-initiated Remote PED for Client

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

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

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

- > On the HSM appliance, use the **hsm ped** commands, as described earlier, to prepare the HSM for Remote PED.
 - Register a PedServer's certificate with **hsm ped server register**.
 - Make a connection with the desired PedServer with **hsm ped connect**, specifying the IP of the Remote PED Server and a port number that you know is accessible through the firewall.
- > On the Remote PED host, use the **lunacm ped** commands to set the identity of the PedServer to match what you have told the HSM to expect
 - Use **ped set** to provide the IP address and the port number that you determined (or that your colleague determined) in the lunash session.
- > On the HSM appliance, use the **hsm ped select** command to select the Remote PED server that you just configured, as the PED that will be requested by any upcoming HSM operations that need PED authentication.
- > On the Client (which could also be the Remote PED host, or could be a separate computer/application server), run a command that invokes PED operation, like the **role login** command.
- > The HSM receives the command and looks to the PED (in this case the Remote PED) that has been previously specified in lunash.

Example:

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

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

```
Default Remote PED Server Port: 1503
```

```
<snip>
```

```
Callback Server is running..
```

```
Callback Server Information:
```

```
  Hostname:          sa7-78
  IP:                192.168.0.78
  Software Version:  2.0.1 (20001)
```

```
Operating Information:
```

```
  Admin Port:       1501
```

```
:
```

```
<snip>
```

```
:
```

```
Show command passed.
```

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

```
lunash:>
```

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

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

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

```
lunacm:> ped connect
```

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

```
lunacm:> partition init -label 550097_par1 -f
```

```
lunacm:> ped connect
```

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

```
lunacm:> ped connect
```

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

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

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

Ending or Switching the Remote PED Connection

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

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

1. End the Remote PED connection.

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

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

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

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

To end or switch an HSM-initiated connection using LunaCM

1. End the Remote PED connection.

```
lunacm:> ped disconnect
```

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

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

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

To end or switch a PED-initiated Remote PED connection

1. End the Remote PED connection with the current host ().

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

2. Check the available list of Remote PED servers.

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

If the Remote PED you want to use is not in the list, see ["PED-Initiated Remote PED" on page 47](#).

3. The new Remote PED server must initiate the connection to the appliance.

> ["pedserver mode connect" on page 88](#) -name <appliance_name>

4. In LunaSH, you are now able to select the new Remote PED server from the available list.

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

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" on the next page](#)
- > ["RC_SOCKET_ERROR: PEDserver Requires Administrator Privileges" on the next page](#)

- > ["LUNA_RET_PED_UNPLUGGED: Reconnect HSM-initiated Remote PED Before Issuing Commands" below](#)
- > ["Remote PED Firewall Blocking" on the next page](#)
- > ["Remote PED Blocked Port Access" on page 55](#)
- > ["ped connect Fails if IP is Not Accessible" on page 56](#)
- > ["PEDserver on VPN fails" on page 56](#)

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 41](#).

RC_SOCKET_ERROR: PEDserver Requires Administrator Privileges

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

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

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

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

LUNA_RET_PED_UNPLUGGED: Reconnect HSM-initiated Remote PED Before Issuing Commands

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

```
lunash:>hsm login
```

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

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

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

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

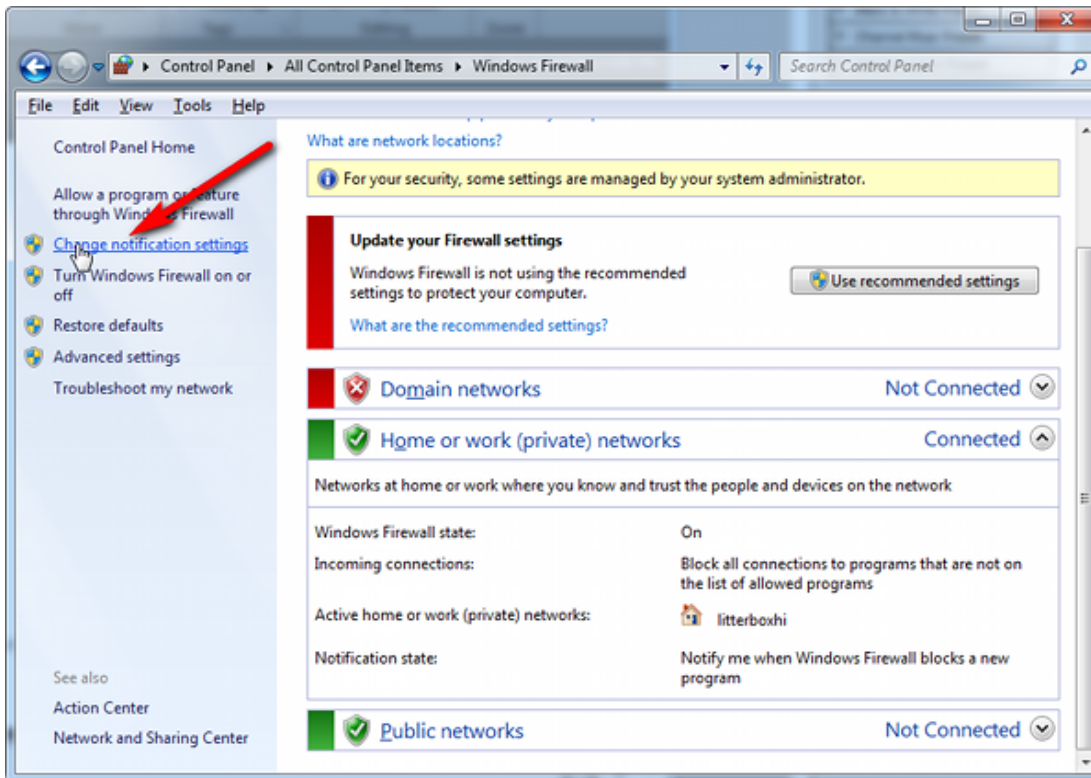
```
lunash:> hsm ped connect -ip <PEDserver_IP> -port <PEDserver_port>
```

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

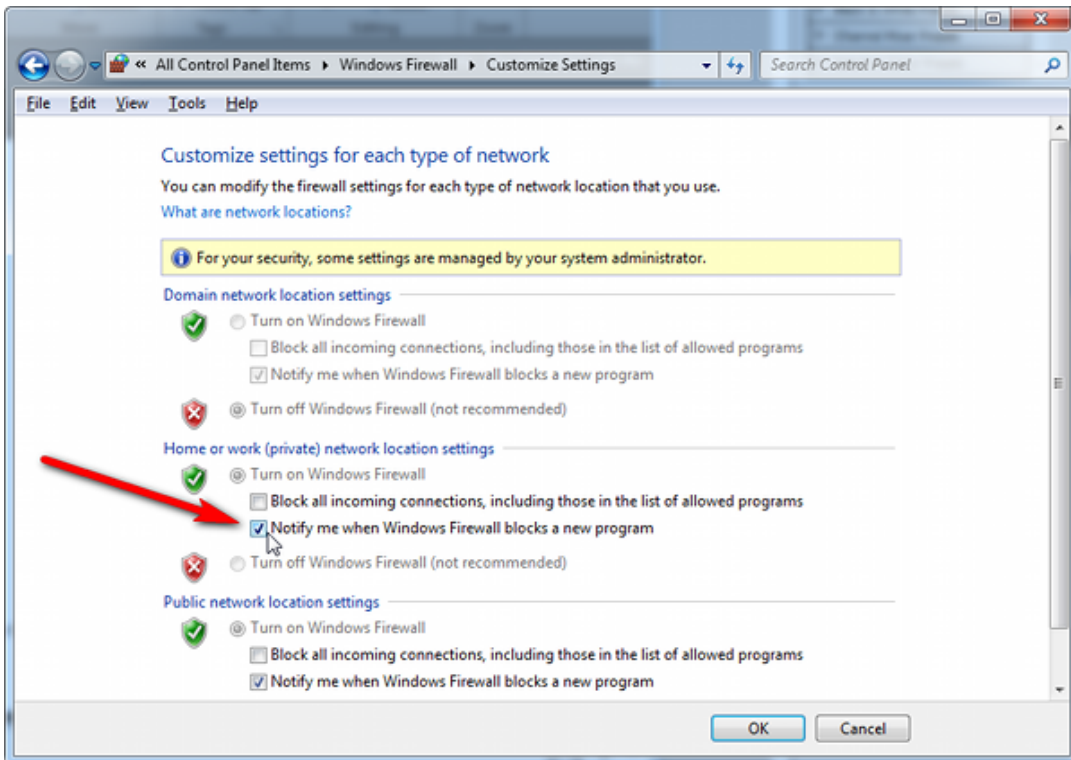
Remote PED Firewall Blocking

If you experience problems while attempting to configure a SafeNet Remote PED session over VPN, you might need to adjust Windows Firewall settings. If your security policy prohibits changes to Windows Firewall, you can use a PED-initiated connection for HSM SO-level operations. See "[PED-Initiated Remote PED](#)" on page 47.

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



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



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

Remote PED Blocked Port Access

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

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

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

1. Connect the Luna PED to a Windows host with Luna HSM Client installed and PEDserver running.
2. Open an Administrator command prompt on the Remote PED host and start the port-forwarding service.
`>plink -ssh -N -T -R 1600:localhost:1503 <user>@<Ubuntu_server_IP>.`
3. Login to the appliance as **admin** and open the HSM-initiated connection.
`lunash:> hsm ped connect -ip <Ubuntu_server_IP> -port 1600`

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

A variant of this arrangement also routes port 22 through the jump server, which allows administrative access to the Luna Network HSM 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 92 -ip <new_IP> -port <port>

PED connection Fails with Error: pedClient is not currently running

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

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

The callback service also restarts when the appliance is rebooted.

Migrating the Orange Remote PED Key For Luna 7.7.0 or Newer

Luna HSM firmware 7.7.0 introduces a new PED protocol for securing local and remote PED connections. In addition to the Luna PED firmware upgrade, any existing orange keys must be migrated to use the new protocol, or you must create a new orange key using a local PED connection after updating the HSM to firmware 7.7.0+ (see "[Initializing the Remote PED Vector and Creating an Orange Remote PED Key](#)" on page 38). If you choose to migrate existing orange key(s), use one of the following procedures:

- > "[Prerequisites](#)" on the next page

- > ["Migrating the Orange RPK\(s\) Using a Remote PED Connection" below](#)
- > ["Migrating the Orange RPK\(s\) Using a Local PED Connection" on the next page](#)

Prerequisites

- > Ensure that you have a backup orange PED key (or M of N set). If you do not have backups, see ["Duplicating Existing PED Keys" on page 75](#) for the procedure.
- > Thales recommends migrating the full M of N set of orange keys at the same time. You must have the full set, and any existing duplicate sets, present at the time of migration. If you do not have all duplicate keysets present, they can be migrated at a later time using this same procedure, or you can create new duplicates from an already-migrated keyset.
- > Depending on your Luna PED hardware, you require the following minimum firmware versions to authenticate with Luna 7.7.0 (see ["Updating Luna PED Firmware \(for older-version PED that requires a power-block\)" on page 59](#)):
 - Luna PED firmware 2.7.4 or newer for older PED
 - Luna PED firmware 2.9.0 or newer for refreshed PED
- > The Luna Network HSM firmware must be at minimum firmware version 7.7.0 (see ["Updating the Luna HSM Firmware" on page 221](#)).
- > The migration process takes about one minute per key. If you are migrating many keys (multiple duplicate copies of M of N splits, for example) you may need to adjust the PED timeouts on your appliance or client to ensure that you can complete the procedure.

For example, if you are migrating an M of N split of 3 keys, with one set of backups, Thales recommends using the following minimum timeout settings under the **Luna** section of the Luna HSM Client configuration file (see [Configuration File Summary](#)). Estimate your actual settings based on the number of keys you are migrating:

- PEDTimeout2 = **600000** (PED key interaction time)
- CommandTimeOutPedSet = **1220000** (Overall PED Operation timeout)

If you are using LunaSH to initiate the key migration, use the following commands to adjust the timeout settings:

```
lunash:> hsm ped timeout set -type pedk -seconds 600
```

```
lunash:> hsm ped timeout set -type pedo -seconds 1220
```

Migrating the Orange RPK(s) Using a Remote PED Connection

You can use your existing Remote PED connections to migrate your orange PED keys (see [Remote PED Setup](#)). This is useful if you have multiple remote PED servers used by different administrators, as they can each migrate their own orange key or M of N keyset. The migration process will begin the first time you attempt remote PED connection after updating the Luna Network HSM firmware to 7.7.0+. You can use LunaSH or LunaCM to initiate the procedure.

To migrate the orange RPK(s) using a remote Luna PED

1. Choose LunaSH or LunaCM to initiate the procedure:

- Connect to the appliance via SSH or a serial connection and log in to LunaSH as **admin** or a custom user with an **admin** role (see [Logging In to LunaSH](#)).
- Launch LunaCM on the Luna HSM Client workstation and set the active slot to a partition on the updated HSM.

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

2. Ensure that you have the orange PED key(s) ready, and initiate a PED connection:

```
lunash:> hsm ped connect [-ip <ip_address>] [-port <number>]
```

```
lunacm:> ped connect [-ip <ip_address>] [-port <number>]
```

3. The remote Luna PED prompts you to insert an orange key. Insert the orange key and press **Enter**.
4. The Luna PED informs you that this PED key must be migrated, and that the existing RPK will be preserved. It prompts you to confirm that you want to migrate this key. Press **Yes**.

- **If you are migrating a single orange key** (M = 1 and N = 1), the migration process begins, and takes about a minute.

The Luna PED then asks if you wish to migrate another key in this keyset. If you have duplicate orange keys to migrate, press **Yes** and repeat steps **3-4** for each duplicate.

- **If you are migrating an M of N keyset**, you must present the required M keys to reconstruct the RPK before the migration process can begin. Repeat steps **3-4** until you reach M keys. The migration process begins on the Mth key, and takes about a minute.

The Luna PED then asks if you wish to migrate another key in this keyset. Press **Yes** and repeat steps **3-4** for each key until all N keys have been migrated, including the keys you presented to meet the M requirement.

If you have duplicate orange M of N keysets, repeat steps **3-4** for each key in each duplicate keyset.

Migrating the Orange RPK(s) Using a Local PED Connection

If it is possible to gather all your existing orange keys into one place, you can also migrate your orange keys for Luna 7.7.0 using a Luna PED connected directly to the Luna Network HSM (see ["Local PED Setup" on page 31](#)).

To migrate the orange RPK(s) using a locally-connected Luna PED

1. Connect to the appliance via SSH or a serial connection, and log in to LunaSH as **admin** or a custom user with an **admin** role (see ["Logging In To LunaSH" on page 1](#)).

2. Log in to the HSM.

```
lunash:> hsm login
```

3. Ensure that the Luna PED is in **Local-USB** mode (see ["Changing Modes" on page 29](#)).

4. Ensure that you have the orange PED key(s) ready. Proceed as if you were initializing the Remote PED vector.

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

5. The Luna PED prompts you to confirm that you want to use an existing keyset. Press **Yes**.
6. The Luna PED prompts you to insert an orange key. Insert the orange key and press **Enter**.

7. The Luna PED informs you that this PED key must be migrated, and that the existing RPV will be preserved. It prompts you to confirm that you want to migrate this key. Press **Yes**.
- **If you are migrating a single orange key** (M = 1 and N = 1), the migration process begins, and takes about a minute.
The Luna PED then asks if you wish to migrate another key in this keyset. If you have duplicate orange keys to migrate, press **Yes** and repeat steps **6-7** for each duplicate.
 - **If you are migrating an M of N keyset**, you must present the required M keys to reconstruct the RPV before the migration process can begin. Repeat steps **6-7** until you reach M keys. The migration process begins on the Mth key, and takes about a minute.
The Luna PED then asks if you wish to migrate another key in this keyset. Press **Yes** and repeat steps **6-7** for each key until all N keys have been migrated.
If you have duplicate orange M of N keysets, repeat steps **6-7** for each key in each duplicate keyset.

Updating Luna PED Firmware (for older-version PED that requires a power-block)

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

NOTE If your Luna PED is the newer model that is powered by a USB connection (and is not shipped with a power-block), see "[Updating Luna PED Firmware \(for USB-powered PED\)](#)" on page 62.

Files Included in the Upgrade Package

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

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

Preparing for the Update

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

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

To prepare your computer for the update

1. Ensure that Luna HSM Client software, including the Remote PED option, is installed on the Windows PC you will use to update the PED. To verify, ensure that the following files/directories are installed:
 - C:\Program Files\SafeNet\LunaClient\RemotePEDDriver
 - C:\Program Files\SafeNet\LunaClient\pedserver.exe
2. The update files are provided in an archive file named for the PED upgrade part number. Extract the files to the Windows Luna HSM Client workstation connected to the Luna PED you are updating.
3. On your Luna HSM Client workstation, open a command prompt window and move to the directory where you copied the files in the update package.

To prepare the Luna PED for the firmware update

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

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

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

Updating the Luna PED Firmware

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

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

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

To update the Luna PED firmware

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

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

NOTE If you have both older Luna PEDs (that are powered by a power block and addressed on "Updating Luna PED Firmware (for older-version PED that requires a power-block)" on page 59), and the newer Luna PEDs (powered by USB connection and addressed on this page), then the LunaPED_Update.exe files for each are different and not interchangeable.

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

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

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

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

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

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

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

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

```
Software update
Success
Press ENTER
```

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

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

7. Press **<** to exit to the **Select Mode** menu. If the update was successful, the new PED version is displayed at the bottom of the PED screen.
8. Your Luna PED is now updated and ready to use. Repeat the procedure for each Luna PED that you own.

Troubleshooting

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

No PED Prompts

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

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

Files Uploaded in the Wrong Order

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

```
Failure (VERIFY) (7)
```

```
Press Enter
```

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

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

Upgrade Failed Message (or Similar)

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

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

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

Updating Luna PED Firmware (for USB-powered PED)

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

To update the Luna PED Firmware from Version 2.8.0 to a newer version 2.8.x or 2.9.x, follow the steps below.

If your Luna PED is the older type, that was shipped with a power-block, then do not use these instructions; see ["Updating Luna PED Firmware \(for older-version PED that requires a power-block\)" on page 59](#) instead.

Preparing for the Upgrade

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

Prepare your computer for the upgrade

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

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

NOTE If you have both older Luna PEDs (that are powered by a power block and addressed on ["Updating Luna PED Firmware \(for older-version PED that requires a power-block\)" on page 59](#)), and the newer Luna PEDs (powered by USB connection and addressed on this page), then the LunaPED_Update.exe files for each are different and *not interchangeable*.

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

Prepare the Luna PED for the firmware upgrade

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

NOTE LUNA PED version 2.8.X (or 2.9.x) is powered by the USB port; a separate power supply to the Luna PED is not provided nor required.

3. Allow the PED to boot normally until it reaches the default "Local PED mode Awaiting command..."
4. Press the < key to display the **Mode** menu.
5. Verify the PED version – the bottom line of the PED display should say "PED V.2.8.0"

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

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

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

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

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

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

Transfer and confirm the PED FW Update

1. In a command prompt window, on your Windows PC, from the directory where you copied the files in the upgrade package, execute the following command:

Prompt > **LunaPED_Update.exe ped-2.9.x-y-z-production-itb-real.bin** (where x-y-z are numbers specific to the released build of the firmware)

2. At the Luna PED keypad, select **Yes** in response to the prompt.
3. The output of the update command in the Windows command prompt should be similar to the following:

```
LunaPED_Update v3.0.0-1 May 10 2017 22:52:25
PED operation is required (to upload image)...
(Sent xxxxxxxx bytes in xxxxxxxxxx microseconds).
PED operation is required (to save image)...
```

4. If the image has transferred correctly, Luna PED displays the following message:

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

5. Select **Yes** to save the new image.
6. Wait approximately 20 seconds. The PED displays the following message:

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

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

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

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

Done

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

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 Luna PED.

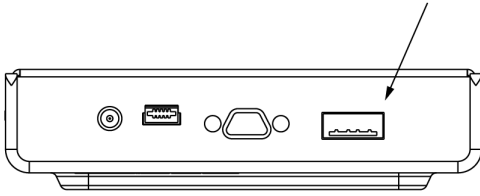
- > ["Creating PED Keys" below](#)
 - ["Stage 1: Reusing Existing PED Keys" on the next page](#)
 - ["Stage 2: Defining M of N" on page 68](#)
 - ["Stage 3: Setting a PED PIN" on page 68](#)
 - ["Stage 4: Duplicating New PED Keys" on page 70](#)
- > ["Performing PED Authentication" on page 70](#)
- > ["Consequences of Losing PED Keys" on page 72](#)
- > ["Identifying a PED Key Secret" on page 74](#)
- > ["Duplicating Existing PED Keys" on page 75](#)
- > ["Changing a PED Key Secret" on page 76](#)

Creating PED Keys

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

- > If you are reusing an existing PED key or keyset, the owners of those keys must be present with their keys and 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 LunaSH or LunaCM commands to initialize the applicable role, domain, or vector.

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

```
lunash:> hsm init
```

- **Orange Remote PED Key:**

```
lunash:> hsm 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:**

```
lunash:> audit init
```

The Luna PED responds, displaying:

```
Remote PED mode
Token found
```

NOTE The PED screen prompts for a Black PED Key for any of "User", "Crypto Officer", "Limited Crypto Officer", "Crypto User". The PED is not aware that the key you present has a black or a gray sticker on it. The colored stickers are visual identifiers for your convenience in keeping track of your PED Keys. You differentiate by how you label, and how you use, a given physical key that the PED sees as "black" (once it has been imprinted with a secret).

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

Stage 1: Reusing Existing PED Keys

If you want to use a PED key with an existing authentication secret, have the key ready to present to the 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 21 and "[Domain PED Keys](#)" on page 22 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 23 for more information. If you do not want to use M of N (authentication by one PED key), enter a value of **1** for both M and N.

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

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

>03
```

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

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

>05
```

3. Continue to "[Stage 3: Setting a 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 22 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 72.

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

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

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

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

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

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

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

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

3. The PED prompts you for a PIN.

- If you want to set a 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" on the next page.](#)

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 75](#).

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 68](#) 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 68](#) for each M of N split. Otherwise, the key creation process is complete.

Performing PED Authentication

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

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

NOTE The PED screen prompts for a Black PED Key for any of "User", "Crypto Officer", "Limited Crypto Officer", "Crypto User". The PED is not aware that the key you present has a black or a gray sticker on it. The colored stickers are visual identifiers for your convenience in keeping track of your PED Keys. You differentiate by how you label, and how you use, a given physical key that the PED sees as "black" (once it has been imprinted with a secret).

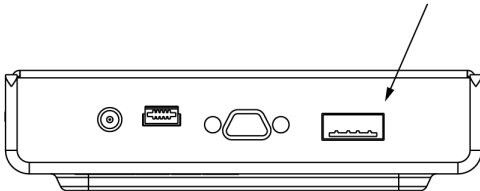
When you issue a command that requires PED interaction, the interface returns a message like the following:

```
lunash:>hsm login
```

Luna PED operation required to login as HSM Administrator - use Security Officer (blue) PED key. The PED briefly displays the following message before prompting you for the appropriate PED key:

```
Remote PED mode
Token found
```

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



CAUTION! Multiple failed authentication attempts result in zeroization of the HSM or partition, or role lockout, depending on the role. This is a security measure designed to thwart repeated, unauthorized attempts to access cryptographic material. For details, see ["Logging In as HSM Security Officer" on page 148](#) 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 RPs on the PED-authenticated Luna Network 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 page 74](#)
- > ["Gray Crypto User Key" on page 74](#)
- > ["White Audit User Key" on page 74](#)

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 SO space 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 SO space 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 SO space(s). If the HSM is factory-reset, the contents of the HSM SO space are unrecoverable. Follow the same procedure as you would if you lost the blue HSM SO key, but you cannot restore the HSM SO space from backup.

Orange Remote PED Key

If the Remote PED Vector is lost, create a new one and distribute a copy to the administrator of each Remote PED server. See ["Initializing the Remote PED Vector and Creating an Orange Remote PED Key" on page 38](#).

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:

- > Luna PED in Admin Mode (see ["Changing Modes" on page 29](#))
- > 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
```

3. 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:

- > Luna PED in Admin Mode (see ["Changing Modes" on page 29](#))
- > 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 23](#).

To duplicate an existing PED key

1. 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" on the next page](#)
- > ["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 page 78](#)
- > ["Black Crypto Officer Key" on page 78](#)
- > ["Gray Crypto User Key" on page 78](#)
- > ["White Audit User Key" on page 78](#)

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 LunaSH, log in as HSM SO.
lunash:> **hsm login**
2. Initiate the PED key change.
lunash:> **hsm changepw**
3. You are prompted to present the original blue key(s) and then to create a new HSM SO keyset. See ["Creating PED Keys" on page 65](#).

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 SO space 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 LunaSH, log in as HSM SO.
lunash:> **hsm login**
2. Initialize the RPV.
lunash:> **hsm ped vector init**
You are prompted to create a new Remote PED key.
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.

NOTE The PED screen prompts for a Black PED Key for any of "User", "Crypto Officer", "Limited Crypto Officer", "Crypto User". The PED is not aware that the key you present has a black or a gray sticker on it. The colored stickers are visual identifiers for your convenience in keeping track of your PED Keys. You differentiate by how you label, and how you use, a given physical key that the PED sees as "black" (once it has been imprinted with a secret).

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. Log into LunaSH as **audit**.
2. Log in as the Audit User.
lunash:> **audit login**
3. Initiate the PED key change.
lunash:> **audit changepwd**

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

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

See "[pedserver](#)" on the next page.

The PEDclient Utility

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

The PEDclient utility performs the following functions:

- > It mediates between the HSM where it is installed and the Luna PED where PEDserver is installed, to provide PED services to the requesting HSM(s).
- > It resides on a computer with RBS and an attached Luna Backup HSM, and it connects with another instance of PEDclient on a distant host of an HSM, to provide the link component for Remote Backup Service. See [Configuring a G5 Remote Backup HSM Server](#) for more information.
- > It acts as the logging daemon for HSM audit logs.

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

Thus, for example, in the case where an administrative workstation or laptop has both a Remote PED and a Remote Backup HSM attached, PEDclient would perform double duty. It would link with a locally-running instance of PEDserver, to convey HSM requests from the locally-connected Backup HSM to the locally-connected PED, and return the PED responses. As well, it would link a locally-running instance of RBS and a distant PEDclient instance to mediate Remote Backup function for that distant HSM's partitions. See [Configuring a G5 Remote Backup HSM Server](#) for more information.

See "[pedclient](#)" on page 96.

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
appliance	Registers or deregisters an appliance, or lists the registered appliances. Applies to server-initiated (peer-to-peer) mode only. See " pedserver appliance " on the next page.
mode	Specifies the mode that the PED Server will be executed in. See " pedserver mode " on page 85.
regen	Regenerates the client certificate. Applies to server-initiated (peer-to-peer) mode only. See " pedserver regen " on page 96.

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
delete	Deregisters an appliance. See " pedserver appliance delete " on the next page.
list	Lists the registered appliances. See " pedserver appliance list " on page 83.
register	Registers an appliance. See " pedserver appliance register " on page 84

pedserver appliance delete

Deregister an appliance certificate from PEDserver.

Syntax

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

Option	Description
-name <unique name>	Specifies the name of the appliance to be deregistered from PEDserver.
-force	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
-name <unique name>	Specifies the name of the appliance to be registered to PED Server.
-certificate <appliance certificate file>	Specifies the full path and filename of the certificate that was retrieved from the appliance.
-ip <appliance server IP address>	Specifies the IP address of the appliance server.
-port <port number>	Optional field. Specifies the port number used to connect to the appliance (directly or indirectly according to network configuration). Range: 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
config	Modifies or shows existing configuration file settings. See "pedserver mode config" on the next page .
connect	Connects to the appliance. See "pedserver mode connect" on page 88 .
disconnect	Disconnects from the appliance. See "pedserver mode disconnect" on page 89 .
show	Queries if PEDserver is currently running, and gets details about PEDserver. See "pedserver mode show" on page 90 .
start	Starts PEDserver. See "pedserver mode start" on page 92 .
stop	Shuts down PEDserver. See "pedserver mode stop" on page 94 .

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

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

Option	Description
-logtrace <0 or 1>	Optional. Specifies if the logger should log "trace" 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.
-maxlogfilesize <size>	Optional. Specifies the maximum log file size in KB.
-name <registered appliance name>	
-pinginterval <int>	Optional. Specifies the time interval between ping commands, in seconds.
-pingtimeout <int>	Optional. Specifies timeout of the ping response, in seconds.
-port <server port>	Optional. Specifies the server port number.
-socketreadtimeout <int>	Optional. Specifies the socket read timeout, in seconds.
-socketwritetimeout <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
-name <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.
-configfile <filename>	Optional. Specifies which PEDserver configuration file to use.
-socketreadtimeout <int>	Optional. Specifies the socket read timeout, in seconds.
-socketwritetimeout <int>	Optional. Specifies socket write timeout, in seconds.
-internalshutdowntimeout <int>	Optional. Specifies the shutdown timeout for internal services, in seconds.
-bgprocessstartuptimeout <int>	Optional. Specifies the startup timeout for the detached process, in seconds.
-bgprocessshutdowntimeout <int>	Optional. Specifies the shutdown timeout for the detached process, in seconds.
-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 stop -name hellohi
```

pedserver regen

Regenerates the client certificate. This command is available in server-initiated (peer-to-peer) mode only. Existing links (PEDserver, NTLS or STC) will not be affected until they are terminated. Afterward, the user is required to re-register the client certificate to NTLS and PEDserver.

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

Syntax

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

Option	Description
-commonname <commonname>	The client's common name (CN).
-force	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
assignid	Assigns a PED ID mapping to an HSM. See "pedclient mode assignid" on the next page.
config	Modifies or shows existing configuration file settings. See "pedclient mode config" on page 99.
deleteid	Deletes a PED ID mapping. See "pedclient mode deleteid" on page 101.
releaseid	Releases a PED ID mapping from an HSM. See "pedclient mode releaseid" on page 102.
setid	Creates a PED ID mapping. See "pedclient mode setid" on page 103.
show	Queries if PEDclient is currently running and gets details about PEDclient. See "pedclient mode show" on page 104.
start	Starts up PEDclient. See "pedclient mode start" on page 105.
stop	Shuts down PEDclient. See "pedclient mode stop" on page 107.
testid	Tests a PED ID mapping. See "pedclient mode testid" on page 108.

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
-id <pedid>	Specifies the ID of the PED to be assigned.
-id_serialnumber <serial>	Specifies the serial number of the HSM to be linked to the specified PED ID.
-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.
-locallogger	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
-show	Displays the contents of the configuration file.
-set	Updates the configuration file to be up to date with other supplied options.
-eadmin <0 or 1>	Optional. Specifies if the administration port is on "localhost" or on the external host name.
-idletimeout <int>	Optional. Specifies the idle connection timeout, in seconds.
-ignoreidletimeout	Optional. Specifies that the idle connection timeout should not apply to the connection established between the PED and HSM during their assignment.
-socketreadtimeout <int>	Optional. Specifies the socket read timeout, in seconds.
-socketwritetimeout <int>	Optional. Specifies the socket write timeout, in seconds.
-shutdowntimeout <int>	Optional. Specifies the shutdown timeout for internal services, in seconds.
-pstartuptimeout <int>	Optional. Specifies the startup timeout for the detached process, in seconds.
-pshutdowntimeout <int>	Optional. Specifies the shutdown timeout for the detached process, in seconds.
-logfilename <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.

Option	Description
-maxlogfilesize <size>	Optional. Specifies the maximum log file size in KB.
-locallogger	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
-id <PED_ID>	Specifies the ID of the PED to be deleted from the map.
-logfilename <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.
-locallogger	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
-id <PED_ID>	Specifies the ID of the PED to be released.
-logfilename <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.
-locallogger	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
-id <PED_ID>	Specifies the ID of the PED to be mapped.
-id_ip <hostname>	Specifies the IP address or hostname of the PED Server to be linked with the PED ID.
-id_port <port>	Specifies the PED Server port to be linked with the PED ID.
-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.
-locallogger	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
-admin <admin port number>	Optional. Specifies the administration port number to use.
-eadmin <0 or 1>	Optional. Specifies if the administration port is on "localhost" or on the external host name.
-socketreadtimeout <int>	Optional. Specifies the socket read timeout, in seconds.
-socketwritetimeout <int>	Optional. Specifies the socket write timeout, in seconds.
-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.
-locallogger	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
-winservice	Starts PEDclient for Windows service. The standard parameters used for pedclient mode start can be used for pedclient mode start -winservice as well.
-eadmin <0 or 1>	Optional. Specifies if the administration port is on "localhost" or on the external host name.
-idletimeout <int>	Optional. Specifies the idle connection timeout, in seconds.
-socketreadtimeout <int>	Optional. Specifies the socket read timeout, in seconds.
-socketwritetimeout <int>	Optional. Specifies the socket write timeout, in seconds.
-shutdowntimeout <int>	Optional. Specifies the shutdown timeout for internal services, in seconds.
-pstartuptimeout <int>	Optional. Specifies the startup timeout for the detached process, in seconds.
-pshutdowntimeout <int>	Optional. Specifies the shutdown timeout for the detached process, in seconds.
-logfilename <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.
-locallogger	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
-eadmin <0 or 1>	Optional. Specifies if the administration port is on "localhost" or on the external host name.
-socketreadtimeout <int>	Optional. Specifies the socket read timeout, in seconds.
-socketwritetimeout <int>	Optional. Specifies the socket write timeout, in seconds.
-shutdowntimeout <int>	Optional. Specifies the shutdown timeout for internal services, in seconds.
-pstartuptimeout <int>	Optional. Specifies the startup timeout for the detached process, in seconds.
-pshutdowntimeout <int>	Optional. Specifies the shutdown timeout for the detached process, in seconds.
-logfilename <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.
-locallogger	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
-id <PED_ID>	Specifies the ID of the PED to be tested.
-logfilename <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.
-locallogger	Optional. Specifies that the Remote PED logger should be used, not the IS logging system.

Example

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

CHAPTER 3: Audit Logging

Each event that occurs on the HSM can be recorded in the HSM event log, allowing you to audit your HSM usage. The HSM event log is viewable and configurable only by the **audit** user role. This **audit** role is disabled by default and must be explicitly enabled.

This chapter describes how to use audit logging to provide security audits of HSM activity. It contains the following sections:

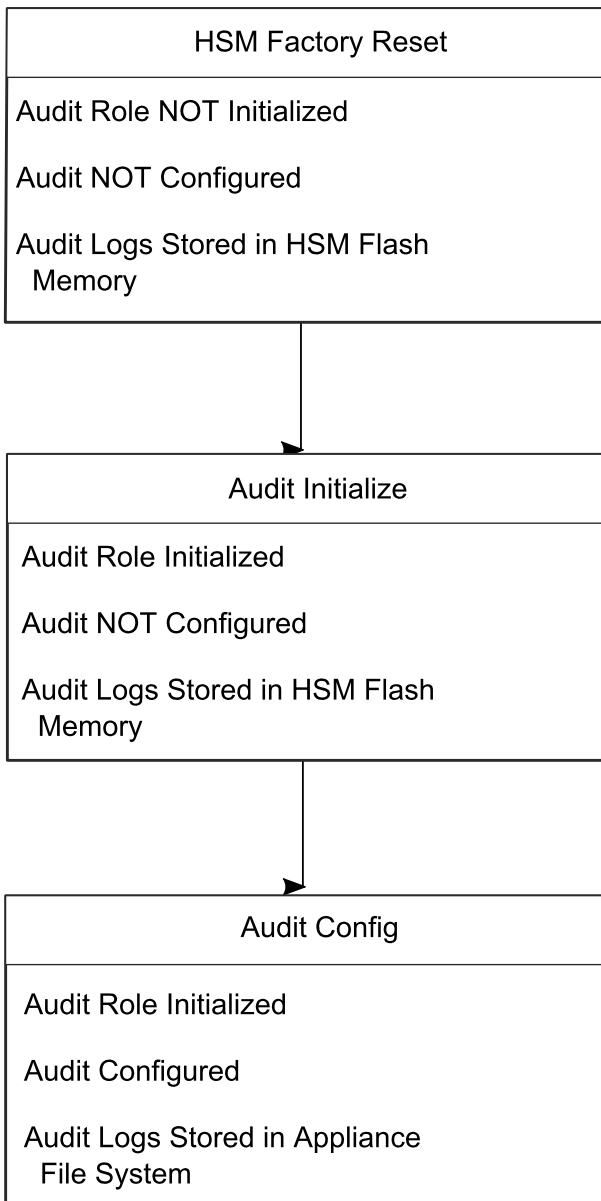
- > ["Audit Logging General Advice and Recommendations" on page 119](#)
- > ["Logging In as Auditor" on page 120](#)
- > ["Configuring and Using Audit Logging" on page 121](#)
- > ["Remote Audit Logging" on page 126](#)
- > ["Changing the Auditor Credential" on page 127](#)
- > ["Audit Log Categories and HSM Events" on page 128](#)
- > ["Audit Log Troubleshooting" on page 135](#)

Audit Logging Features

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

- > Log entries originate from the Luna Network 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 Luna Network HSM that is a member of the same domain.
- > Audit Logging can be performed on password-authenticated and PED-authenticated (both 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 Luna Network 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 HSM appliance, where they can be viewed. Log records are HMACed using an audit log secret to ensure their authenticity. The audit log secret is unique to the HSM where the log was created, and is required to view the HSM event logs. The secret can be exported, allowing you to view and verify the logs on another HSM.

Event logging impacts HSM performance

Each audit log record generated requires HSM resources. Configuring event logging to record most, or all, events may have an impact on HSM performance. You may need to adjust your logging configuration to provide adequate logging without significantly affecting performance. By default, only critical events are logged, imposing virtually no load on the HSM.

Audit limitations and Controlled tamper recovery state

The following conditions apply when HSM Policy "48: Do controlled tamper recovery" is enabled (default setting).

- > Auditor (the Audit role) cannot verify the integrity of audit logs until after recovery from tamper.
- > Auditor cannot be initialized when the HSM is in controlled tamper recovery state.
- > Existing Audit role can login when in controlled tamper recovery state.
- > Existing Audit role cannot make audit config changes when in controlled tamper recovery state.
- > Existing Audit role cannot export the audit secret when in controlled tamper recovery state.

The Audit Role

The audit logging function is controlled by two roles on Luna Network HSM, that must be used together:

- > The "audit" appliance account (use SSH or PuTTY to log in as "audit", instead of "admin", or "operator", or "monitor", etc.)
- > The "audit" HSM account (accessible only if you have logged into the appliance as "audit"; this account must be initialized)

On Luna Network HSM, the audit logging is managed by an audit user (an appliance system role), in combination with the HSM audit role, through a set of LunaSH commands. The audit user can perform only the audit-logging related tasks and self-related tasks. Other HSM appliance users, such as admin, operator, and monitor, have no access to the audit logging commands.

A default appliance (LunaSH) audit user is automatically created, but must be enabled. Upon first login, the audit user is asked to change their password. That appliance audit user would need to initialize the HSM audit role first, before being able to administer the audit logging. The Luna Network HSM admin user can create more audit users when necessary.

To simplify configuration,

- > The maximum log file size is capped at 4 MB.
- > The log path is kept internal.
- > The rotation offset is set at 0.

Audit User on the Appliance

The appliance audit user is a standard user account on Luna Network HSM, with default password "PASSWORD" (without the quotation marks). By default, the appliance audit user is disabled. Therefore, you must enable it in LunaSH before it becomes available. See ["user enable" on page 1](#) for the command syntax.

Audit Role on the HSM

A Luna Network 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 LunaSH command **audit init** to initialize the audit role, as described in ["audit init" on page 1](#).

Password-authenticated HSMs

For Luna Network 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 Luna Network 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.

Appliance Audit User Available Commands

The Audit role has a limited set of operations available to it, on the HSM, as reflected in the reduced command set available to the "audit" user when logged in to the shell (LunaSH).

```
login as: audit
audit@192.20.11.78's password:
Last login: Fri Mar 31 09:37:53 2017 from 10.124.0.31
```

Luna SA 7.0.0 Command Line Shell - Copyright (c) 2001-2017 SafeNet, Inc. All rights reserved.

```
lunash:>help
```

The following top-level commands are available:

Name	(short)	Description
help	he	Get Help
exit	e	Exit Luna Shell
hsm	hs	> Hsm
audit	a	> Audit
my	m	> My
network	n	> Network

Audit Log Secret

The HSM creates a log secret unique to the HSM, computed during the first initialization after manufacture. The log secret resides in flash memory (permanent, non-volatile memory), and is used to create log records that are sent to a log file. Later, the log secret is used to prove that a log record originated from a legitimate HSM and has not been tampered with.

Log Secret and Log Verification

The 256-bit log secret which is used to compute the HMACs is stored in the parameter area on the HSM. It is set the first time an event is logged. It can be exported from one HSM to another so that a particular sequence of log messages can be verified by the other HSM. Conversely, it can be imported from other HSMs for verification purpose.

To accomplish cross-HSM verification, the HSM generates a key-cloning vector (KCV, a.k.a. the Domain key) for the audit role when it is initialized. The KCV can then be used to encrypt the log secret for export to the HOST.

To verify a log that was generated on another HSM, assuming it is in the same domain, we simply import the wrapped secret, which the HSM subsequently decrypts; any records that are submitted to the host for verification will use this secret thereafter.

When the HSM exports the secret, it calculates a 32-bit checksum which is appended to the secret before it is encrypted with the KCV.

When the HSM imports the wrapped secret, it is decrypted, and the 32-bit checksum is calculated over the decrypted secret. If this doesn't match the decrypted checksum, then the secret that the HSM is trying to import comes from a system on a different domain, and an error is returned.

To verify a log generated on another HSM, in the same domain, the host passes to the target HSM the wrapped secret, which the target HSM subsequently decrypts; any records submitted to the target HSM for verification use this secret thereafter.

Importing a log secret from another HSM does not overwrite the target log secret because the operation writes the foreign log secret only to a separate parameter area for the wrapped log secret.

CAUTION! Once an HSM has imported a wrapped log secret from another HSM, it must export and then re-import its own log secret in order to verify its own logs again.

Audit Log Records

A log record consists of two fields – the log message and the HMAC for the previous record. When the HSM creates a log record, it uses the log secret to compute the SHA256-HMAC of all data contained in that log message, plus the HMAC of the previous log entry. The HMAC is stored in HSM flash memory. The log message is then transmitted, along with the HMAC of the previous record, to the host. The host has a logging daemon to receive and store the log data on the host hard drive.

For the first log message ever returned from the HSM to the host there is no previous record and, therefore, no HMAC in flash. In this case, the previous HMAC is set to zero and the first HMAC is computed over the first log message concatenated with 32 zero-bytes. The first record in the log file then consists of the first log message plus 32 zero-bytes. The second record consists of the second message plus HMAC1 = HMAC (message1 || 0x0000). This results in the organization shown below.

MSG 1	HMAC 0
	...
MSG n-1	HMAC n-2
MSG n	HMAC n-1
...	
MSG n+m	HMAC n+m-1
MSG n+m+1	HMAC n+m
...	
MSG end	HMAC n+m-1
Recent HMAC in NVRAM	HMAC end

To verify a sequence of m log records which is a subset of the complete log, starting at index n , the host must submit the data illustrated above. The HSM calculates the HMAC for each record the same way as it did when the record was originally generated, and compares this HMAC to the value it received. If all of the calculated HMACs match the received HMACs, then the entire sequence verifies. If an HMAC doesn't match, then the associated record and all following records can be considered suspect. Because the HMAC of each message depends on the HMAC of the previous one, inserting or altering messages would cause the calculated HMAC to be invalid.

The HSM always stores the HMAC of the most-recently generated log message in flash memory. When checking truncation, the host would send the newest record in its log to the HSM; and, the HSM would compute the HMAC and compare it to the one in flash. If it does not match, then truncation has occurred.

The HMAC of previous record is

```
"29C51014B6F131EC67CF48734101BBE301335C25F43EDF8828745C40755ABE25".
```

The remainder is the raw data for this record as ASCII-HEX.

- > The "who" is LunaSH session "session 1 Access 2147483651:22621" (identified by the lunash access ID major = 2147483651, minor = 22621).
- > The "what" is "LUNA_CREATE_CONTAINER".
- > The operation status is "LUNA_RET_SM_UNKNOWN_TOSM_STATE(0x00300014)".

Timestamping

The HSM has an internal real-time clock (RTC). The RTC does not have a relevant time value until it is synchronized with the HOST system time. Because the HSM and the host time could drift apart over time, periodic re-synchronization is necessary. Only an authenticated Auditor is allowed to synchronize the time.

Time Reported in Log

When you perform **audit show**, you might see a variance of a few seconds between the reported HSM time and the Host time. Any difference up to five seconds should be considered normal, as the HSM reads new values from its internal clock on a five-second interval. So, typically, Host time would show as slightly ahead.

Log Capacity

The log capacity of Luna Network 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 lunash:> **audit 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. If possible, use the remote logging feature to transmit log data to a Security Information and Event Management (SIEM) system to automatically analyze log data and identify anomalous events.
- > Execute lunash:> **audit log tarlogs** regularly to archive the audit logs and transfer them to a separate machine for long term storage. Also, execute **audit log clear** regularly to free up the audit log disk space on Luna Network HSM.
- > Consider installing and configuring a Luna PCIe HSM in (or connected to) the remote log server to act as a "verification engine" for the remote log server. Ensure that the log secret for the operational HSM(s) has been shared with the log server verification HSM.

NOTE This is not always possible, unless you are physically copying the logs over from the .tgz archive. Because log records do not necessarily appear on the remote log server immediately, the HMAC might be incorrect. Also, if more than one Luna Network HSM is posting log records to a remote server, this could interfere with record counts.

- > The audit log records are comma-delimited. We recommend that full use be made of the CSV formatting to import records into a database system or spreadsheet tool for analysis, if an SIEM system is not available.
- > The ASCII hex data representing the command and returned values and error code should be examined if an anomaly is detected in log review/analysis. It may be possible to match this data to the HSM's dual-port data. The dual-port, if it is available, will contain additional data that could be helpful in establishing the context surrounding the anomalous event. For example, if an unexpected error occurs it could be possible to identify the trace through the firmware subsystems associated with the error condition. This information would be needed to help in determining if the error was unexpected but legitimate or if it was forced in an attempt to exploit a potential weakness.

An important element of the security audit logging feature is the 'Log External' function. See [Audit Logging](#) for more information. For applications that cannot add this function call, it is possible to use `lunacm:> audit logmsg` within a startup script to insert a text record at the time the application is started.

NOTE Audit log and syslog entries are timestamped in UTC format.

Disk Full

In the event that all the audit disk space is used up, audit logs are written to the HSM's small persistent memory. When the HSM's persistent memory is full, normal crypto commands will fail with "disk full" error.

To resolve that situation, the audit user must:

1. Archive the audit logs on the host side.
2. Move the audit logs to some other location for safe storage.
3. Clear the audit log directory.
4. Restart the callback service.

`lunash:> service restart cbs`

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

CAUTION! If the HSM is zeroized when a "disk full" condition has occurred, HSM initialization will fail, preventing the user from clearing the logs. This will effectively lock out the appliance and RMA may be necessary.

Logging In as Auditor

Before you can change the audit logging configuration, archive audit logs, or verify audit logs from another HSM, you must log in as Auditor (AU), or relevant commands will fail.

To log in as Auditor

1. Connect to the appliance via SSH or a serial connection, and log in to LunaSH as **audit** or a custom user with an **audit** role (see ["Logging In To LunaSH" on page 1](#)).
2. Log in to the HSM.

```
lunash:> audit login
```

You are prompted for the Auditor credential.

Failed Auditor Login Attempts

If you fail three (3) consecutive Auditor login attempts, the Auditor role is locked out for ten minutes.

NOTE The system must actually receive some erroneous/false information before it logs a failed attempt; if you merely forget to insert 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](#)
- > ["Copying Log Files Off the Appliance" on page 124](#)
- > ["Exporting the Audit Logging Secret and Importing to a Verifying HSM" on page 124](#)
- > ["Reading the Audit Log Records" on page 126](#)
- > ["Audit Role Authentication Considerations" on page 126](#)

Configuring Audit Logging

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

NOTE Audit log and syslog entries are timestamped in UTC format.

TIP *Performance and Audit Logging*

Secure Audit Logging consumes HSM resources, so consider minimizing the intensity of logging that you invoke.

For example, when choosing asymmetric key usage, you have the option to specify event values to record with **-value asymmetric** or **first**.

When choosing symmetric key usage logging you can opt for the corresponding **symmetric** and **symfirst**.

An HMAC is generated for each log, so **"first"** and **"symfirst"** record the first use of a key (asymmetric sig/ver or symmetric enc/dec respectively) and are much more sparing of HSM cycles, and therefore preferred to configuring for a log entry at every individual use of a given key -- unless that level of detailed logging is mandated.

Prerequisites (HSM SO)

1. Configure the Luna Network HSM appliance to use the network time protocol (NTP). See [Timestamping – NTP and Clock Drift](#).
2. Log in to LunaSH as an admin-level user, and enable the audit user. The audit user is necessary to access and work with logs through the LunaSH interface. It is restricted from administrative functions:

```
lunash:> user enable -username audit
```

To configure audit logging (Auditor):

1. Using an SSH connection (or a local serial connection), login to LunaSH on the Luna Network HSM appliance as **audit** (not as **admin**), using the password "PASSWORD".

The first time you login as **audit**, you are prompted to change the password to something more secure. To fulfill the purpose of the Audit role, keep the **audit** user's password separate from, and unknown to, the HSM Security Officer:

The audit user sees a reduced subset of commands suitable to the audit role, only, as follows:

Name	(short)	Description
init	i	Initialize the Audit role
changePwd	ch	Change Audit User Password or PED Key
login	logi	Login as the Audit user
logout	logo	Logout the Audit user
config	co	Set Audit Parameters
sync	sy	Synchronize HSM Time to Host Time
show	sh	Display the Audit logging info
log	l	> Manage Audit Log Files
secret	se	> Export/Import Audit Logging Secret
remotehost	r	> Configure Audit Logging Remote Hosts

NOTE The audit user's commands are not available to the admin user. The audit user has no administrative control over the Luna Network HSM appliance. This is a first layer in the separation of roles. This separation allows a user with no administrative control of the appliance and HSM to have oversight of the HSM logs, while also ensuring that an administrator cannot clear those logs.

- Initialize the **audit** role on the HSM. This enables logging for all subsequent actions performed by the SO and partition user(s):

```
lunash:> audit init
```

- On password-authenticated HSMs, you are prompted for the password and cloning domain.
- On PED-authenticated HSMs, you are referred to Luna PED, which prompts you for the domain (red PED key) and Audit authentication (white PED key).

- Now that the audit role exists on the HSM, you can configure the auditing function. However, before you can configure audit logging you must log into the HSM as the **audit** role:

```
lunash:> audit login
```

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

NOTE You are now logged into the appliance as the **audit** user and into the HSM (within the appliance) as the **audit** role. Both are required. The **audit** commands, including HSM login as the **audit** role do not appear if you are logged in as any other named appliance-level user.

- Synchronize the HSM's clock with the host time (which should also be synchronized with the NTP server) so that all subsequent log records will have a valid and accurate timestamp:

```
lunash:> audit sync
```

- Configure audit logging to specify what you want to log. You can specify the level of audit appropriate for needs of the organization's policy and the nature of the application(s) using the HSM:

```
lunash:> audit config -parameter event -value <event_value>
```

NOTE The first time you configure audit logging, we suggest using only the **?** option, to see all the available options in the configuration process.

Security audits can generate a very large amount of data, which consumes HSM processing resources, host storage resources, and makes the job of the Audit Officer quite difficult when it comes time to review the logs. For this reason, ensure that you configure audit logging such that you capture only relevant data, and no more.

For example, the **First Symmetric Key Usage Only** or **First Asymmetric Key Usage Only** category is intended to assist Audit Officers to capture the relevant data in a space-efficient manner for high processing volume applications. On the other hand, a top-level Certificate Authority would likely be required, by policy, to capture all operations performed on the HSM but, since it is typically not an application that would see high volumes, configuring the HSM to audit all events would not impose a significant space and/or performance premium in that situation.

As a further example, `lunash:> audit config -parameter event -value all` will log everything the HSM does. This might be useful in some circumstances, but will quickly fill up log files.

- Configure audit logging to specify how often you want to rotate the logs:

```
lunash:> audit config -parameter rotation -value <value>
```

For example, `lunash:> audit config -parameter rotate -value hourly` would rotate the logs every hour, cutting down the size of individual log files, even in a situation of high-volume event recording, but would increase the number of files to be handled.

Log Entries

Log entries are made within the HSM, and are written to the currently active log file on the appliance file system. When a log file reaches the rotation trigger, it is closed, and a new file gets the next log entry. The number of log files on the appliance grows according to the logging settings and the rotation schedule that you configured. At any time, you can copy files to a remote computer and then clear the originals from the HSM, if you wish to free the space.

For Luna Network HSM, to simplify configuration within its closed and hardened environment, the following rules apply:

- > The maximum log file size is capped at 4 MB.
- > The log path is internal to the Luna Network HSM appliance.
- > The rotation offset is set at 0.

Copying Log Files Off the Appliance

You can copy the log files off of the appliance for viewing and verification.

To copy files off the appliance

1. Create an archive of the logs that are ready to archive:

```
lunash:> audit log list
```

```
lunash:> audit log tarlogs
```

2. View a list of the log files currently saved on the appliance:

```
lunash:> my file list
```

For this example, assume that the list includes a file named **audit.tgz**.

3. On the computer where you wish to capture and store the log files, use **pscp** or **scp** to transfer the file from the appliance:

```
/usr/safenet/lunaclient/logs :> pscp audit@myLunaHSM1:audit.tgz mylunsa1_audit_2014-02-28.tgz
```

Provide the audit user's credentials when prompted. This copies the identified file from the remote Luna Network HSM's file system (in the **audit** account) and stores the copy on your local computer file system with a useful name.

4. You can view and parse the plain-text portion of the file.
5. You can verify the authenticity of the retrieved file using a connected HSM to which you have imported the Audit logging secret from the originating Luna Network HSM.

Exporting the Audit Logging Secret and Importing to a Verifying HSM

You can export the audit log secret from one HSM and import it to another to allow the first HSM's logs to be viewed and verified on the second. The HSMs must share the same authentication method and Audit cloning domain (password string or red PED key). You can verify logs from a Luna PCIe HSM using a Luna Network

HSM, and vice-versa.

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

- On the Luna Network HSM where HSM audit log files are being created, export the audit logging secret:


```
lunash:> audit secret export
```

The filename is displayed when the secret is exported. You can check the filename with [my file list](#).
- On a computer connected to both HSMs, use **pscp** or **scp** to transfer the logging secret from the appliance.
 - If you are planning to verify logs with a Luna PCIe HSM, you can use the PCIe HSM's host computer.
 - If you are planning to verify logs with a second Luna Network HSM, you must transfer the logging secret to a client computer, and then to the second appliance.

```
<client_install_dir>:> pscp audit@ <hostname_or_IP>:<log_secret_file> .
```

Then, if transferring to a second Luna Network HSM:

```
<client_install_dir>:> pscp <log_secret_file> audit@<hostname_or_IP>:
```

This copies the identified file from the remote Luna Network HSM's file system (in the **audit** account) and stores the copy on your local computer file system in the directory from which you issued the command. Provide the audit user's credentials when prompted.
- Log in to the verifying HSM appliance as the **audit** user. For this example, we will assume that you have already initialized the HSM audit user role, using the same domain/secret as is associated with the source HSM.
 - If you are using a Luna Network HSM, connect via SSH and log in to LunaSH as the **audit** user:


```
lunash:> audit login
```
 - If you are using a Luna PCIe HSM, open LunaCM and log in using the Auditor role:


```
lunacm:> role login -name au
```
- Import the audit logging secret to the HSM.
 - Luna Network HSM (LunaSH):


```
lunash:> audit secret import -serialtarget <target_HSM_SN> -serialsource <source_HSM_SN> -file <log_secret_file>
```
 - Luna PCIe HSM (LunaCM):


```
lunacm:> audit import file <log_secret_file>
```
- You can now verify audit log files from the source HSM.
 - Luna Network HSM (LunaSH):


```
lunash:> audit log verify -file <audit_log_filename>.log
```
 - 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.

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.

Remote Audit Logging

With Luna Network HSM, the audit logs can be sent to one or more remote logging servers. Either UDP or TCP protocol can be specified. The default is UDP and port 514.

NOTE You or your network administrator will need to adjust your firewall to pass this traffic (iptables).

UDP Considerations

If you are using the UDP protocol for logging, the following statements are required in the `/etc/rsyslog.conf` file:

```
$ModLoad imudp
$InputUDPServerRun (PORT)
```

Possible approaches include the following:

> With templates:

```
$template AuditFile, "/var/log/luna/audit_remote.log"
if $syslogfacility-text == 'local3' then ?AuditFile;AuditFormat
```

> Without templates:

```
local3.* /var/log/audit.log;AuditFormat
```

> Dynamic filename:

```
$template DynFile, "/var/log/luna/%HOSTNAME%.log"
if $syslogfacility-text == 'local3' then ?DynFile;AuditFormat
```

NOTE The important thing to remember is that the incoming logs go to **local3**, and the port/protocol that is set on the Luna appliance must be the same that is set on the server running rsyslog.

Example using TCP

The following example illustrates how to setup a remote Linux system to receive the audit logs using TCP:

1. Register the remote Linux system IP address or hostname with the Luna Network HSM:

```
lunash:> audit remotehost add -host 192.20.9.160 -protocol tcp -port 1660
```

2. Modify the remote Linux system `/etc/rsyslog.conf` file to receive the audit logs:

```
$ModLoad imtcp
$InputTCPServerRun 514
$template AuditFormat, "%msg:F,94:2%\n"
#save log messages from Luna Network HSM
local3.* /var/log/luna/audit.log;AuditFormat
```

3. Modify the remote Linux system `/etc/sysconfig/rsyslog` file to receive the remote logs:

```
# Enables logging from remote machines. The listener will listen to the specified port.
SYSLOGD_OPTIONS="-r -m 0"
```

4. Restart the rsyslog daemon on the remote Linux system:

```
# service rsyslog restart
```

5. Monitor the audit logs on the remote Linux system:

```
# tail -f /var/log/luna/audit.log
```

Changing the Auditor Credential

From time to time, you may need to change the Auditor's credential. The credential might have been compromised, or your organization's security policy may mandate account credential changes after a specific time interval. The Auditor can change their own credential at any time.

To change the Auditor credential

1. Connect to the appliance via SSH or a serial connection, and log in to LunaSH as **audit** or a custom user with an **audit** role (see ["Logging In To LunaSH" on page 1](#)).
2. Log in as Auditor (see ["Logging In as Auditor" on page 120](#)).
3. Change the Auditor credential.

```
lunash:> audit changepwd
```

You are prompted for the current Auditor credential, and then to create a new one.

Audit Log Categories and HSM Events

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

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).
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

HSM Event	Description
LUNA_LOAD_CUSTOM_MODULE	CA_LoadModule
LUNA_LOAD_ENCRYPTED_CUSTOM_MODULE	CA_LoadEncryptedModule
LUNA_UNLOAD_CUSTOM_MODULE	CA_UnloadModule
LUNA_EXECUTE_CUSTOM_COMMAND	CA_PerformModuleCall
LUNA_HA_LOGIN	CA_HAGetLoginChallenge, 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

HSM Event	Description
LUNA_EXTRACT_CONTEXTS	C_GetOperationState
LUNA_INSERT_CONTEXTS	C_SetOperationState
LUNA_SELF_TEST	C_PerformSelfTest
LUNA_LOAD_CERT	CA_SetTokenCertificateSignature
LUNA_HA_INIT	CA_HAInit
LUNA_SET_HSM_POLICY	CA_SetHSMPolicy
LUNA_SET_DESTRUCTIVE_HSM_POLICY	CA_SetDestructiveHSMPolicy
LUNA_SET_CONTAINER_POLICY	CA_SetContainerPolicy
LUNA_SET_CAPABILITY	Internal, for capability update
LUNA_CREATE_LOGIN_CHALLENGE	CA_CreateLoginChallenge
LUNA_REQUEST_CHALLENGE	CA_SIMInsert, CA_SIMMultiSign
LUNA_PED_INIT_RPV	CA_InitializeRemotePEDVector
LUNA_PED_DELETE_RPV	CA_DeleteRemotePEDVector
LUNA_MTK_LOCK	Internal, for manufacturing
LUNA_MTK_UNLOCK_CHALLENGE	Internal, for manufacturing
LUNA_MTK_UNLOCK_RESPONSE	Internal, for manufacturing
LUNA_MTK_RESTORE	CA_MTKRestore
LUNA_MTK_RESPLIT	CA_MTKResplit
LUNA_MTK_ZEROIZE	CA_MTKZeroize
LUNA_FW_UPGRADE_INIT	CA_FirmwareUpdate
LUNA_FW_UPGRADE_UPDATE	CA_FirmwareUpdate
LUNA_FW_UPGRADE_FINAL	CA_FirmwareUpdate
LUNA_FW_ROLLBACK	CA_FirmwareRollback

HSM Event	Description
LUNA_MTK_SET_STORAGE	CA_MTKSetStorage
LUNA_SET_CONTAINER_SIZE	CA_SetContainerSize

Key Management

HSM Event	Description
LUNA_CREATE_OBJECT	C_CreateObject
LUNA_COPY_OBJECT	C_CopyObject
LUNA_DESTROY_OBJECT	C_DestroyObject
LUNA_DESTROY_MULTIPLE_OBJECTS	CA_DestroyMultipleObjects
LUNA_GENERATE_KEY	C_GenerateKey
LUNA_GENERATE_KEY_PAIR	C_GenerateKeyPair
LUNA_WRAP_KEY	C_WrapKey
LUNA_UNWRAP_KEY	C_UnwrapKey
LUNA_DERIVE_KEY	C_DeriveKey
LUNA_GET_RANDOM	C_GenerateRandom
LUNA_CLONE_AS_SOURCE, LUNA_REPLICATE_AS_SOURCE	CA_CloneAsSource
LUNA_CLONE_AS_TARGET_INIT, LUNA_REPLICATE_AS_TARGET_INIT	CA_CloneAsTargetInit
LUNA_CLONE_AS_TARGET, LUNA_REPLICATE_AS_TARGET	CA_CloneAsTarget
LUNA_GEN_TKN_KEYS	CA_GenerateTokenKeys
LUNA_GEN_KCV	CA_ManualKCV, C_InitPIN, C_InitToken, CA_InitAudit
LUNA_SET_LKCV	CA_SetLKCV

HSM Event	Description
LUNA_M_OF_N_GENERATE	CA_GenerateMofN_Common, CA_GenerateMofN
LUNA_M_OF_N_ACTIVATE	CA_ActivateMofN
LUNA_M_OF_N_MODIFY	CA_ActivateMofN
LUNA_EXTRACT	CA_Extract
LUNA_INSERT	CA_Insert
LUNA_LKM_COMMAND	CA_LKMInitiatorChallenge, 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
LUNA_DECRYPT_INIT	C_DecryptInit
LUNA_DECRYPT	C_Decrypt
LUNA_DECRYPT_END	C_DecryptFinal
LUNA_DIGEST_INIT	C_DigestInit
LUNA_DIGEST	C_Digest
LUNA_DIGEST_KEY	C_DigestKey
LUNA_DIGEST_END	C_DigestFinal
LUNA_SIGN_INIT	C_SignInit
LUNA_SIGN	C_Sign

HSM Event	Description
LUNA_SIGN_END	C_SignFinal
LUNA_VERIFY_INIT	C_VerifyInit
LUNA_VERIFY	C_Verify
LUNA_VERIFY_END	C_VerifyFinal
LUNA_SIGN_SINGLEPART	C_Sign
LUNA_VERIFY_SINGLEPART	C_Verify
LUNA_WRAP_CSP	CA_CloneMofN_Common
LUNA_M_OF_N_DUPLICATE	CA_DuplicateMofN
LUNA_ENCRYPT_SINGLEPART	C_Encrypt
LUNA_DECRYPT_SINGLEPART	C_Decrypt

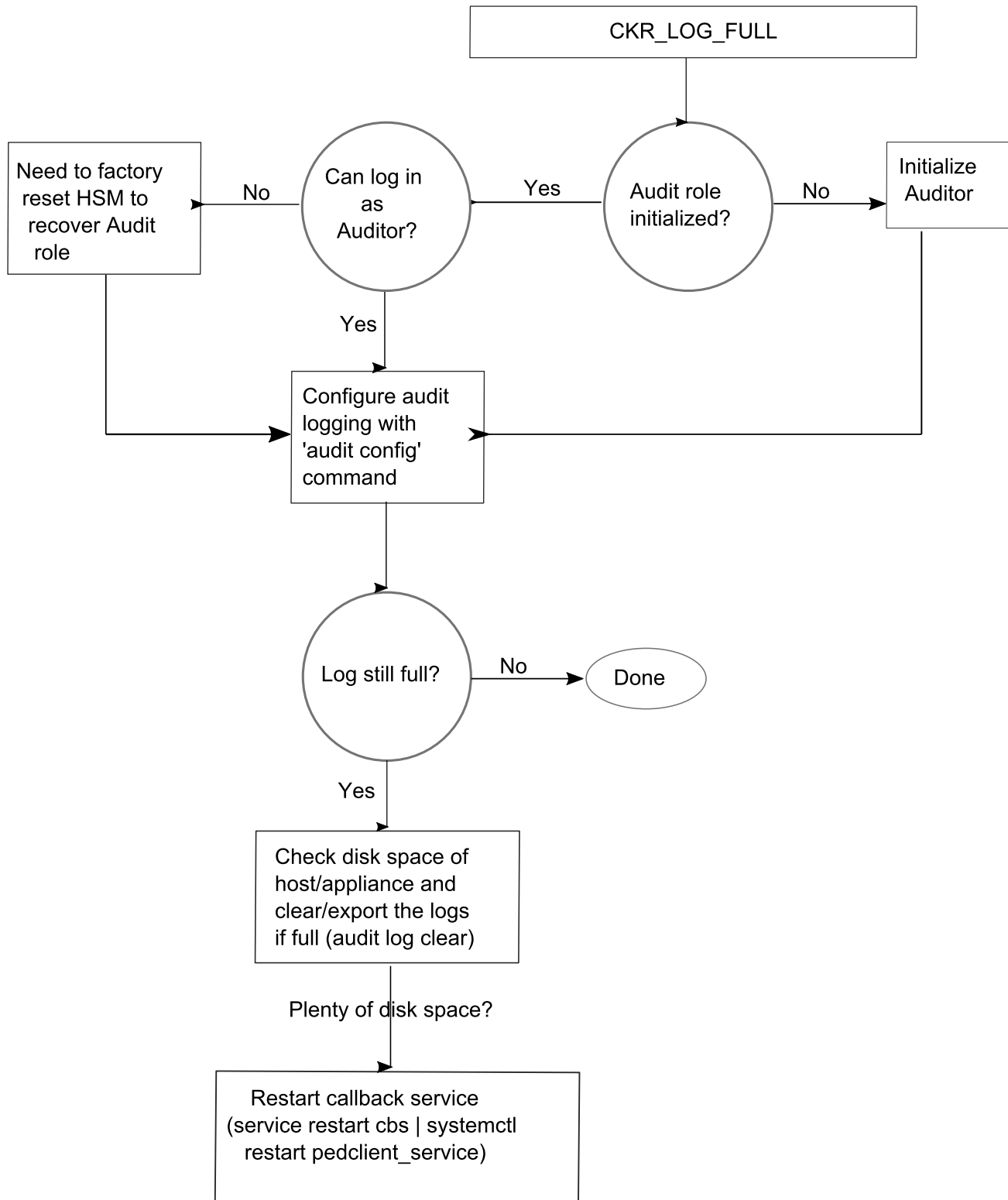
Audit Log Management

HSM Event	Description
LUNA_LOG_SET_TIME	CA_TimeSync
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

HSM Event	Description
LUNA_LOG_EXPORT_SECRET	CA_LogExportSecret

Audit Log Troubleshooting

The following sequence might help for problems with audit logging, like "log full."



CHAPTER 4: Initializing the HSM

Initialization prepares a new HSM for use, or an existing HSM for reuse. You must initialize the HSM before you can generate or store objects, allow clients to connect, or perform cryptographic operations:

- > On a new or factory-reset HSM, initialization sets the HSM SO credentials, the HSM label, and the cloning domain of the HSM Admin partition. This is often referred to as a 'hard' initialization. See ["Initializing a New or Factory-reset HSM" below](#).
- > On an initialized HSM, re-initialization destroys all existing partitions and objects, but retains the SO credentials and cloning domain. You have the option to change or retain the existing label. This is often referred to as a 'soft' initialization. See ["Re-initializing the HSM" on page 139](#).

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 13](#) for details.

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

HSM Label	<p>The label is a string that uniquely identifies this HSM.</p> <p>The HSM label created during initialization must be 1-32 characters in length. If you specify a longer label, it will automatically be truncated to 32 characters. Only alphanumeric characters and the underscore are allowed:</p> <pre>abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789_</pre> <p>For more information, refer to Name, Label, and Password Requirements.</p>
HSM SO credentials	<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 "PED Authentication" on page 17.</p> <p>For password-authenticated HSMs, you specify the HSM SO password. For proper security, it should be different from the appliance admin password, and employ standard password-security characteristics.</p> <p>In LunaSH, the SO or CO password must be 7-255 characters in length. The following characters are allowed:</p> <pre>abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789 !@#\$%^*()-_=[] { } / : ' , . ~</pre> <p>The following characters are invalid or problematic and must not be used in the HSM SO password:</p> <pre>"&;<>` \ ` </pre> <p>Spaces are allowed; to specify a password with spaces, enclose the password in double quotation marks.</p>
Cloning domain for the HSM Admin partition	<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:</p> <pre>abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789 !@#\$%^*-_=[] { } / : ' , . ~</pre> <p>The following characters are problematic or invalid and must not be used in a domain string: "&;<>` \ ` ()</p> <p>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.</p>

To initialize a new or factory-reset HSM

1. Log into LunaSH as **admin**. You can use a serial terminal window or SSH connection.

2. If Secure Transport Mode is set, you must unlock the HSM before proceeding. New Luna HSMs are shipped from the factory in Secure Transport Mode (STM). STM allows you to verify whether or not an HSM has been tampered while it is not in your possession, such as when it is shipped to another location, or placed into storage. See ["Secure Transport Mode" on page 13](#) 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:


```
lunash:> hsm 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 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 29](#). Alternatively, have a Remote PED instance set up, see ["About Remote PED" on page 32](#).

4. Run the **hsm init** command, specifying a label for your Luna Network HSM:

```
lunash:> 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 17](#) 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 145](#)

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 136.

CAUTION! Ensure you have backups for any partitions and objects you want to keep, before reinitializing the HSM.

To re-initialize the HSM (soft init)

1. Log into LunaSH as **admin**. You can use a serial terminal window or SSH connection.
2. Log in as the HSM SO.
3. If Secure Transport Mode is set, you must unlock the HSM before proceeding. See "[Secure Transport Mode](#)" on page 13.
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 29.
5. Re-initialize the HSM, specifying a label for your Luna Network HSM:

```
lunash:> 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:

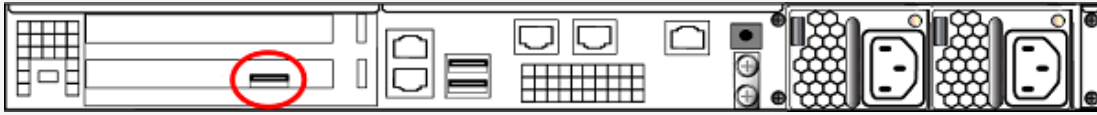
- > "[To initialize a PED-authenticated HSM](#)" below
- > "[Imprinting the Blue HSM SO PED Key](#)" on page 141
- > "[Imprinting the Red Cloning Domain PED Key](#)" on page 143
- > "[New, reuse, and overwrite options](#)" on page 143

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 29), or remotely via Remote PED connection (see "[About Remote PED](#)" on page 32).

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



2. Set the active slot to the Luna Network 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 23](#) for details).
10. Luna PED asks if you wish to use a PED PIN (an additional secret; see ["PED Key Management" on page 65](#) 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 LunaSH.

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

New PED Keys	Existing PED Keys (Reuse)	Existing PED Keys (Overwrite)
SETTING DOMAIN... Would you like to reuse an existing keyset? (Y/N) > Yes (unless you have good reason to create a new domain)	SETTING DOMAIN... Would you like to reuse an existing keyset? (Y/N) > Yes : make this HSM part of an existing domain > No : create a new domain for this HSM	SETTING DOMAIN... Would you like to reuse an existing keyset? (Y/N) > Yes : make this HSM part of an existing domain > No : 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 5: HSM Roles

The security of an HSM and its cryptographic contents depends on well-controlled access to that HSM. A controlled access policy is defined by:

- > the set of users with valid login credentials for the appliance, the HSM and the application partition
- > the actions each user is allowed to perform when logged in (the user's role)

For example, an access policy that adheres to the PKCS#11 standard requires two roles: the security officer (SO), who administers the user account(s), and the standard user, who performs cryptographic operations. When a user logs in to the HSM, they can perform only those functions that are permitted for their role.

Luna Network HSM divides roles on the HSM according to an enhanced version of the PKCS#11 standard. Configuration, administration, and auditing of the HSM itself is the responsibility of the roles described below. Cryptographic functions take place on the application partition, which has a different set of independent roles (see [Partition Roles](#)).

Personnel holding HSM-level roles access the HSM by logging in to LunaSH via SSH or a serial connection. They must therefore have the appropriate appliance user access for their respective HSM role, to ensure that they can access all LunaSH commands necessary to perform HSM administration tasks.

The HSM-level roles are as follows:

HSM Security Officer (SO)

The HSM SO handles all administrative and configuration tasks on the HSM, including:

- > Initializing the HSM and setting the SO credential (see ["Initializing the HSM" on page 136](#))
- > Setting and changing global HSM policies (see ["HSM Capabilities and Policies" on page 150](#))
- > Creating/deleting the application partition (see ["Creating or Deleting an Application Partition" on page 163](#))
- > Updating the HSM firmware (see ["Updating the Luna HSM Firmware" on page 221](#))

The HSM SO must have **admin**-level user access to the Luna Network HSM appliance (see [Appliance Users and Roles](#)).

Managing the HSM Security Officer Role

Refer also to the following procedures to manage the HSM SO role:

- > ["Logging In as HSM Security Officer" on the next page](#)
- > ["Changing the HSM SO Credential" on the next page](#)

Auditor (AU)

The Auditor is responsible for managing HSM audit logging. These responsibilities have been separated from the other roles on the HSM and application partition so that the Auditor can provide independent oversight of all HSM processes, and no other user, including the HSM SO, can clear those logs. The Auditor's tasks include:

- > Initializing the Auditor role

- > Setting up audit logging on the HSM
- > Configuring the maximum size of audit log files and the time interval for log rotation
- > Archiving the audit logs

The Auditor must have access to the **audit** account on the Luna Network HSM appliance (see [Appliance Users and Roles](#)).

Managing the Auditor Role

Refer to ["Configuring and Using Audit Logging" on page 121](#) for procedures involving the Auditor role. See also:

- > ["Logging In as Auditor" on page 120](#)
- > ["Changing the Auditor Credential" on page 127](#)

Logging In as HSM Security Officer

Before you can create an application partition or perform other administrative functions on the HSM, you must log in as HSM Security Officer (SO), or administrative commands will fail.

To log in as HSM SO

1. Connect to the appliance via SSH or a serial connection, and log in to LunaSH as **admin** or a custom user with an **admin** role (see ["Logging In To LunaSH" on page 1](#)).
2. Log in to the HSM.

```
lunash:> hsm login
```

You are prompted for the HSM SO credential.

Failed HSM SO Login Attempts

If you fail three (3) consecutive HSM SO login attempts, application partitions are destroyed, the HSM is zeroized and all of its contents are rendered unrecoverable. The number is not adjustable. As soon as you authenticate successfully, the counter is reset to zero.

NOTE The system must actually receive some erroneous/false information before it logs a failed attempt; if you merely forget to insert 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 the HSM SO Credential

From time to time, you may need to change the HSM Security Officer's credential. The credential might have been compromised, or your organization's security policy may mandate account credential changes after a specific time interval. The HSM SO can change their own credential at any time.

There is no way to reset the HSM SO credential except to re-initialize the HSM, zeroizing the contents of the HSM and its application partitions. Resetting a credential requires a higher authority. On the HSM, there is no authority higher than the HSM SO.

To change the HSM SO credential

1. Connect to the appliance via SSH or a serial connection, and log in to LunaSH as **admin** or a custom user with an **admin** role (see [Logging In to LunaSH](#)).
2. Log in as HSM SO (see ["Logging In as HSM Security Officer" on the previous page](#)).
3. Change the HSM SO credential.

```
lunash:> hsm changepw
```

You are prompted for the current HSM SO credential, and then to create a new one.

In LunaSH, the SO or CO password must be 7-255 characters in length. The following characters are allowed:

```
abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789 !@#$%^*()-_=[ ]{}/:'",.~
```

The following characters are invalid or problematic and must not be used in the HSM SO password:

```
"&;<>\'`|
```

Spaces are allowed; to specify a password with spaces, enclose the password in double quotation marks.

CHAPTER 6: HSM Capabilities and Policies

The HSM can be configured to suit the cryptographic needs of your organization. Configurable functions are governed by the following settings:

- > **HSM Capabilities** are features of HSM functionality, set at manufacture based on the HSM model you selected at time of purchase. You can add new capabilities to the HSM by purchasing and applying capability licenses from Thales (see "[Upgrading HSM Capabilities and Partition Licenses](#)" on page 224). Some capabilities have corresponding modifiable HSM policies.
- > **HSM Policies** are configurable settings that allow the HSM Security Officer to modify the function of their corresponding capabilities. Some policies affect HSM-wide functionality, and others allow further customization of individual partitions by the Partition Security Officer.

The table below describes all Luna Network HSM capabilities, their corresponding policies, and the results of changing their settings. This section contains the following procedures:

- > "[Setting HSM Policies Manually](#)" on page 160
- > "[Setting HSM Policies Using a Template](#)" on page 160

To zeroize the HSM and revert policies to their default values, see "[Resetting the Luna Network HSM to Factory Condition](#)" on page 254.

To zeroize the HSM and keep the existing policy settings, use lunash:> **hsm zeroize**

Destructive Policies

Some policies affect the security of the HSM. As a security measure, changing these policies results in application partitions or the entire HSM being zeroized. These policies are listed below as **destructive**.

#	HSM Capability	HSM Policy
0	Enable PIN-based authentication <ul style="list-style-type: none">> Allowed: The HSM authenticates all users with keyboard-entered passwords.> Disallowed: See HSM capability 1 below.	N/A

#	HSM Capability	HSM Policy
1	<p>Enable PED-based authentication</p> <ul style="list-style-type: none"> > Allowed: The HSM authenticates users with secrets stored on physical PED keys, read by a Luna PED. The Crypto Officer and Crypto User roles may also be configured with a secondary, keyboard-entered challenge secret. > Disallowed: See HSM capability 0 above. 	N/A
2	<p>Performance level</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"> > 4: Standard performance > 8: Enterprise performance > 15: Maximum performance 	N/A
4	<p>Enable domestic mechanisms & key sizes</p> <p>Always allowed. All Luna Network HSMs are capable of full-strength cryptography with no US export restrictions.</p>	N/A
6	<p>Enable masking</p> <p>Always disallowed. SIM has been deprecated on all current Luna Network HSMs.</p>	N/A
7	<p>Enable cloning</p> <p>Always allowed. All current Luna Network HSMs can clone cryptographic objects from one partition to another.</p>	<p>Allow cloning (Destructive)</p> <ul style="list-style-type: none"> > ON (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. > OFF: No partition on the HSM may clone cryptographic objects. Partition SOs cannot change this.
9	<p>Enable full (non-backup) functionality</p> <ul style="list-style-type: none"> > Allowed: The HSM is capable of full cryptographic functions. > Disallowed: The HSM is capable of backup functions only (disallowed on Luna Backup HSMs only). 	N/A

#	HSM Capability	HSM Policy
12	<p>Enable non-FIPS algorithms</p> <p>Always allowed. The HSM can use all cryptographic algorithms described in Supported Mechanisms.</p>	<p>Allow non-FIPS algorithms (Destructive) *</p> <ul style="list-style-type: none"> > ON (default): The HSM may use all available cryptographic algorithms, meaning all the FIPS-approved algorithms as well as all the non-FIPS algorithms. > OFF: Only algorithms sanctioned by the FIPS 140-2 standard are permitted. The following is displayed in the output from lunash:> hsm show: <pre>FIPS 140-2 Operation: ===== The HSM is in FIPS 140-2 approved operation mode.</pre> <div style="border: 1px solid #004a99; padding: 10px; margin-top: 10px;"> <p>NOTE When C_GetMechanismInfo is called and the HSM policy “Allow NonFIPS Algorithms” is disabled:</p> <ol style="list-style-type: none"> 1) If a mechanism has the WRAP flag set and MPE_NO_WRAP, the WRAP flag is <i>not</i> returned by the HSM as part of the mechanism info. 2) If a mechanism has the SIGN flag set and MPE_NO_SIGN, the SIGN flag is <i>not</i> returned by the HSM as part of the mechanism info. <p>When the policy is enabled, the HSM returns all the flags that are applicable to the requested mechanism.</p> </div>
15	<p>Enable SO reset of partition PIN</p> <p>Always allowed. This capability enables:</p> <ul style="list-style-type: none"> > the Partition SO to reset the password or PED secret of the Crypto Officer. > the Crypto Officer to reset the password or PED secret of the Crypto User. 	<p>SO can reset partition PIN (Destructive)</p> <ul style="list-style-type: none"> > ON: Partition SO may reset the password or PED secret of a Crypto Officer who has been locked out after too many failed login attempts. > OFF (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. <p>See Resetting the Crypto Officer or Crypto User Credential.</p>
16	<p>Enable network replication</p> <p>Always allowed. This capability enables cloning of cryptographic objects over a network. This is required for HA groups, and for partition backup to a remote or client-connected Luna Backup HSM.</p>	<p>Allow network replication</p> <ul style="list-style-type: none"> > ON (default): Cloning of cryptographic objects is permitted over a network. Remote and client-connected backup is allowed, and the partition may be used in an HA group. > OFF: Cloning over a network is not permitted. Partition backup is possible to a locally-connected Luna Backup HSM only.

#	HSM Capability	HSM Policy
17	<p>Enable Korean Algorithms</p> <ul style="list-style-type: none"> > Allowed: if you have purchased and applied a license for the Korea-specific algorithm set. See "Upgrading HSM Capabilities and Partition Licenses" on page 224 to purchase this capability. > Disallowed if you have not applied this license. 	N/A
18	<p>FIPS evaluated</p> <p>Always disallowed - deprecated capability. All Luna Network HSMs are capable of operating in FIPS Mode.</p> <div style="border: 1px solid black; padding: 5px; margin-top: 10px;"> <p>NOTE This capability is visible (not used) in previous HSM firmware versions, but is removed from version 7.7.0 onward.</p> </div>	N/A
19	<p>Manufacturing Token</p> <p>Always disallowed. For Thales internal use only.</p>	N/A
21	<p>Enable forcing user PIN change</p> <p>Always allowed. This capability forces the Crypto Officer or Crypto User to change the initial role credential created by the Partition SO.</p>	<p>Force user PIN change after set/reset</p> <ul style="list-style-type: none"> > ON (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. > OFF: The CO/CU may continue to use the credential assigned by the Partition SO. <p>See Changing a Partition Role Credential.</p>
22	<p>Enable portable masking key</p> <p>Always allowed, but SIM is not supported on this version of Luna Network HSM.</p>	<p>Allow offboard storage (Destructive)</p> <p>Deprecated policy. On previous HSMs, this policy allowed or disallowed the use of the portable SIM key.</p> <p>Default: ON</p>
23	<p>Enable partition groups</p> <p>Always disallowed - deprecated capability.</p>	N/A

#	HSM Capability	HSM Policy
25	<p>Enable Remote PED usage</p> <p>Always allowed on PED-authenticated HSMs.</p> <p>Always disallowed on password-authenticated HSMs.</p>	<p>Allow Remote PED usage</p> <ul style="list-style-type: none"> > ON (default): The HSM may authenticate roles using a remotely-located PED server or a locally-installed PED. > OFF: The HSM must use a locally-installed PED to authenticate roles.
27	<p>HSM non-volatile storage space</p> <p>Displays the maximum non-volatile storage space (in bytes) on the HSM, determined by the Luna Network HSM model you selected at time of purchase.</p>	N/A
30	<p>Enable Unmasking</p> <p>Always allowed. This capability enables migration from legacy Luna HSMs that used SIM.</p>	<p>Allow unmasking</p> <ul style="list-style-type: none"> > ON (default): Cryptographic objects may be migrated from legacy Luna HSMs that used SIM. > OFF: Migration from legacy HSMs using SIM is not possible.
33	<p>Maximum number of partitions</p> <p>Displays the maximum number of application partitions that can be created on the HSM. The default maximum is determined by the Luna Network HSM model you selected at time of purchase. On some models, you can upgrade the number of allowable partitions by purchasing additional partition licenses (see "Upgrading HSM Capabilities and Partition Licenses" on page 224).</p>	<p>Current maximum number of partitions</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>
35	<p>Enable Single Domain</p> <p>Always disallowed. Not applicable to Luna Network HSM.</p>	N/A
36	<p>Enable Unified PED Key</p> <p>Always disallowed. Not applicable to Luna Network HSM.</p>	N/A

#	HSM Capability	HSM Policy
37	<p>Enable MofN</p> <p>Always allowed on PED-authenticated HSMs. Always disallowed on password-authenticated HSMs.</p>	<p>Allow MofN</p> <ul style="list-style-type: none"> > ON (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 "M of N Split Secrets (Quorum)" on page 23) > OFF: Users do not have the option to split PED secrets (M and N are automatically set to 1).
38	<p>Enable small form factor backup/restore</p> <p>Always disallowed. Not available in this release.</p>	N/A
39	<p>Enable Secure Trusted Channel</p> <p>Always allowed. This capability enables Secure Trusted Channel (STC) to be used for partition-client connections, and/or to encrypt traffic between the HSM and appliance (see Secure Trusted Channel). Not applicable to HSMs at firmware 7.7.0 or newer, where STC is always enabled and is optional to use in any application partition, unless Partition Policy 37 is set to make STC mandatory for that partition.</p>	<p>Allow Secure Trusted Channel</p> <ul style="list-style-type: none"> > ON: Secure Trusted Channel is enabled for partition-client connections (see Creating a Client-Partition STC Connection). STC can be used to encrypt traffic between the appliance and the HSM (see Using the STC Admin Channel). > OFF (default): All clients must access partitions using NTLS connections.
40	<p>Enable decommission on tamper</p> <p>Always allowed. This enables the HSM to be automatically decommissioned if a tamper event occurs (see "Comparing Zeroize, Decommission, Re-image, and Factory Reset" on page 255).</p>	<p>Decommission on tamper (Destructive)</p> <ul style="list-style-type: none"> > ON: The HSM is decommissioned if a tamper event occurs (see "Tamper Events" on page 172). > OFF (default): The contents of the HSM are not affected by a tamper event.
42	<p>Enable partition re-initialize</p> <p>Always disallowed. Not applicable to Luna Network 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 Luna Network HSM.</p>	N/A
43	<p>Enable low level math acceleration</p> <p>Always allowed. This capability enables acceleration of cryptographic functionality for maximum HSM performance.</p>	<p>Allow low-level math acceleration</p> <ul style="list-style-type: none"> > ON (default): Provides maximum HSM performance. > OFF: Do not turn this policy off unless instructed by Thales Technical Support.

#	HSM Capability	HSM Policy
45	<p>Enable Fast-Path</p> <p>Always disallowed. Not available in this release.</p>	N/A
46	<p>Allow Disabling Decommission</p> <p>Always allowed. This capability enables the HSM SO to disable the decommission button on the HSM.</p>	<p>Disable Decommission (Destructive)</p> <ul style="list-style-type: none"> > ON: The decommission button is disabled, preventing decommissioning of the HSM. > OFF (default): Decommission works as described in Decommissioning the HSM Appliance. <div style="border: 1px solid orange; padding: 5px; margin-top: 10px;"> <p>CAUTION! 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>Enable Tunnel Slot</p> <p>Always disallowed. Not available in this release.</p>	N/A
48	<p>Enable Controlled Tamper Recovery</p> <p>Always allowed. This capability enables the HSM SO to require tamper events to be explicitly cleared before normal operations can resume.</p>	<p>Do Controlled Tamper Recovery</p> <ul style="list-style-type: none"> > ON (default): After a tamper event, the HSM SO must explicitly clear the tamper before the HSM can resume normal operations. > OFF: The HSM must be restarted before it can resume normal operations. <p>See "Tamper Events" on page 172 for more information.</p>
49	<p>Enable Partition Utilization Metrics</p> <p>Always allowed. 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>Allow Partition Utilization Metrics</p> <ul style="list-style-type: none"> > ON: The HSM SO can view Partition Utilization Metrics. > OFF (default): Partition Utilization Metrics are not available. <p>See "Partition Utilization Metrics" on page 179 for more information.</p>

#	HSM Capability	HSM Policy
50	<p>Enable Functionality Modules</p> <p>This capability enables Functionality Modules (FMs) to be loaded to the HSM (see "Functionality Modules" on page 238).</p> <ul style="list-style-type: none"> > Allowed on FM-ready HSMs running firmware 7.4 or higher, with the FM capability license installed (see "Preparing the Luna Network HSM to Use FMs" on page 242). > Disallowed on FM-ready HSMs running firmware 7.4 or higher without the FM capability license. <p>Does not appear on HSMs that are not FM-ready or are running firmware older than 7.4.</p>	<p>Allow Functionality Modules (Destructive)</p> <ul style="list-style-type: none"> > ON: 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. <div style="border: 1px solid #ccc; padding: 10px; margin: 10px 0;"> <p>NOTE FIPS compliance requires that objects are never cloned or restored to an HSM using less secure firmware. FIPS 140 validation is performed against the HSM hardware with a specific firmware version. Since the introduction of a Functionality Module changes the firmware, allowing FMs in the HSM removes the HSM from FIPS compliance. For purposes of cloning, an HSM where FMs have <i>ever</i> been allowed is considered less secure than one where FMs have <i>never</i> been allowed. See the Caution below.</p> </div> <p>You can subsequently disable FMs, but future cloning operations will work only with other FM-HOC HSMs.</p> <ul style="list-style-type: none"> > OFF (default): FMs may not be loaded to the HSM. <div style="border: 1px solid #ccc; padding: 10px; margin: 10px 0;"> <p>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 238 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 HSM policy 50. Refer to the CCC CRN for details.</p> </div>

#	HSM Capability	HSM Policy
51	<p>Enable SMFS Auto Activation</p> <p>This capability enables the Secure Memory File System (SMFS) to be activated automatically on startup.</p> <ul style="list-style-type: none"> > Allowed on FM-ready HSMs running firmware 7.4 or higher, with the FM capability license installed (see "Preparing the Luna Network HSM to Use FMs" on page 242). > Disallowed on FM-ready HSMs running firmware 7.4 or higher without the FM capability license. <p>Does not appear on HSMs that are not FM-ready or are running firmware older than 7.4.</p>	<p>Allow SMFS Auto Activation (Destructive)</p> <ul style="list-style-type: none"> > ON: 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. > OFF (default): If disabled, the HSM SO must manually activate the SMFS each time the HSM reboots or loses power.
52	<p>Allow Restricting FM Privilege Level</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"> > Allowed on FM-ready HSMs running firmware 7.4 or higher, with the FM capability license installed (see "Preparing the Luna Network HSM to Use FMs" on page 242). > Disallowed on FM-ready HSMs running firmware 7.4 or higher without the FM capability license. <p>Does not appear on HSMs that are not FM-ready or are running firmware older than 7.4.</p>	<p>Restrict FM Privilege Level (Destructive)</p> <ul style="list-style-type: none"> > ON: FM privilege is restricted. > OFF (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).

#	HSM Capability	HSM Policy
53	<p>Allow Encrypting of Keys from FM to HSM</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"> > Allowed on FM-ready HSMs running firmware 7.4 or higher, with the FM capability license installed (see "Preparing the Luna Network HSM to Use FMs" on page 242). > Disallowed on FM-ready HSMs running firmware 7.4 or higher without the FM capability license. <p>Does not appear on HSMs that are not FM-ready or are running firmware older than 7.4.</p>	<p>Encrypt Keys Passing from FM to HSM (Destructive)</p> <ul style="list-style-type: none"> > ON: 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). > OFF (default): Keys are not encrypted before crossing to the FMCE.
55	<p>Enable Restricted Restore</p> <p>This capability allows the HSM SO to restrict a Luna Backup HSM (G7) from being used with Luna firmware older than 7.7.0, for any purpose other than to migrate cryptographic objects to Luna HSM firmware 7.7.0 or newer. See What are "pre-firmware 7.7.0", V0, and V1 partitions? for more information.</p> <p>Appears on Luna G7 Backup HSM running firmware 7.7.1 or newer.</p>	<p>Enable Restricted Restore (ON-to-OFF Destructive)</p> <ul style="list-style-type: none"> > 1: Objects backed up from pre-7.7.0 firmware partitions <i>can only be</i> restored to V0 or V1 partitions (Luna HSM firmware 7.7.0 or newer). Enable this policy to ensure FIPS compliance. > 0 (default): Objects backed up from pre-7.7.0 firmware partitions <i>can be</i> restored to pre-7.7.0 firmware partitions. Do not use this setting if you require FIPS compliance. <div style="border: 1px solid black; padding: 5px; margin-top: 10px;"> <p>NOTE FIPS compliance requires that objects are never cloned or restored to an HSM using less secure firmware. Since Luna Backup HSM (G7) firmware 7.7.1 and newer uses the same (more secure) cloning protocol as Luna V0/V1 partitions, this restriction applies to objects being restored to older Luna firmware, even if they were backed up from that same older firmware.</p> </div>

* The Backup HSM performs only backup and restore operations and is not a general-purpose HSM. It has no information about the origin of keys or objects. In the case of FIPS-mode or non-FIPS the status of a source HSM (Policy 12) is not noticed, and a target HSM decides what to do with keys from a restore operation. However, the actions of a Backup HSM can be affected by the cloning protocol that is used - see Policy 55

Setting HSM Policies Manually

The HSM SO can change available policies to customize HSM functionality. Some policies apply to all partitions on the HSM; others enable the Partition SO to customize functionality at the partition level. Refer to "[HSM Capabilities and Policies](#)" on page 150 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](#)" below.

Prerequisites

- > The HSM must be initialized (see "[Initializing the HSM](#)" on page 136).
- > 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. Log in to LunaSH as **admin**, or an **admin**-level custom user.
2. [Optional] Display the existing HSM policy settings.
lunash:> **hsm showpolicies**
3. Log in as HSM SO (see "[Logging In as HSM Security Officer](#)" on page 148).
lunash:> **hsm login**
4. Change the policy setting by specifying the policy number and the desired value (**0**, **1**, or a number in the accepted range for that policy).
lunash:> **hsm changepolicy -policy <policy_ID> -value <value>**

Setting HSM Policies Using a Template

An HSM policy template is a file containing a set of preferred HSM policy settings, used to initialize HSMs with those settings. You can use the same file to initialize multiple HSMs, rather than changing policies manually after initialization. This can save time and effort when initializing multiple HSMs that are to function together (such as in an HA group), or must comply with your company's overall security strategy. Templates enable scalable policy management and simplify future audit and compliance requirements.

See also [Setting Partition Policies Using a Policy Template](#).

NOTE This feature requires minimum firmware version 7.1.0 and appliance software version 7.1. 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](#)" above).

To zeroize the HSM and revert policies to their default values, see ["Resetting the Luna Network HSM to Factory Condition" on page 254](#).

To zeroize the HSM and keep the existing policy settings, use `lunash:> hsm zeroize`

This section provides instructions for the following procedures, and some general guidelines and restrictions:

- > ["Creating an HSM Policy Template" below](#)
- > ["Editing an HSM Policy Template" below](#)
- > ["Applying an HSM Policy Template" on the next page](#)

Creating an HSM Policy Template

The following procedures describe how to generate an HSM policy template from the HSM. This can be done optionally at two points in the HSM setup process:

- > before the HSM is initialized: this produces a template file containing the default policy settings, which can then be edited
- > after initializing and setting the HSM policies manually: this produces a template file with the current HSM policy settings, which can then be used to initialize other HSMs with the same settings. The HSM SO must complete the procedure.

To create an HSM policy template

1. Login to LunaSH as **admin**. If you are creating a template from an initialized HSM, you must log in as HSM SO.

```
lunash:> hsm login
```

2. Create the HSM policy template file with an original filename. No file extension is required. If a template file with the same name exists, it is overwritten.

```
lunash:> hsm showpolicies -exporttemplate <filename>
```

3. On a client workstation, use `pscp/scp` to transfer the template file from the source appliance.
4. Customize the template file with a standard text editor (see ["Editing an HSM Policy Template" below](#)).

Editing an HSM Policy Template

Use a standard text editor to manually edit HSM policy templates for custom configurations. This section provides template examples and customization guidelines.

HSM Policy Template Example

This example shows the contents of an HSM policy template created using the factory default policy settings. Use a standard text editor to change the policy values (0=OFF, 1=ON, or the desired value 0-255). You cannot edit the destructiveness of HSM policies. See ["HSM Capabilities and Policies" on page 150](#) 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. From a client workstation, use **pscp/pscp** to transfer the template file to the **admin** user on the destination appliance.
2. Login to LunaSH as **admin** on the destination appliance, and initialize the HSM using the policy template file.


```
lunash:> hsm init -label <label> -applytemplate <filename>
```
3. Verify that the template has been applied correctly by checking the partition's policy settings.


```
lunash:> hsm showpolicies
```

CHAPTER 7: Application Partitions

The Luna Network HSM has two types of partition:

- > one administrative partition, created when you initialize the HSM. The administrative partition is owned by the HSM Security Officer (SO). This partition is used by the HSM SO and the Auditor, and is not used to store cryptographic objects. Operations on the administrative partition are handled using LunaSH.
- > at least one application partition, created by the HSM SO. The application partition is owned by its Partition Security Officer (PO), and has its own access controls and security policies independent from the administrative partition and other application partitions. Its function is to store cryptographic objects used by your applications.

An application partition is like a safe deposit box that resides within a bank's vault. The HSM (vault) itself offers an extremely high level of security for its contents. An application partition (safe deposit box) on the HSM has its own security and access controls, so that even though the HSM SO has access to the vault, they still cannot access the contents of the individual partitions. Only the Partition Security Officer holds the partition's administrative credentials.

Depending on your Luna Network HSM model and the number of additional partition licenses you have purchased, you can create anywhere from 5 to 100 application partitions on the HSM. Each partition can store cryptographic objects according to the amount of memory you assign. The HSM SO can customize the size of individual partitions until all the memory on the HSM is allotted. To purchase additional partition licenses, see ["Upgrading HSM Capabilities and Partition Licenses" on page 224](#).

This chapter contains the following procedures for managing application partitions:

- > ["Creating or Deleting an Application Partition" below](#)
- > ["Customizing Partition Sizes" on the next page](#)

Creating or Deleting an Application Partition

The HSM Security Officer (SO) is responsible for creating the application partition and assigning it to a registered client. The HSM SO can delete the partition at any time, destroying all partition roles and stored cryptographic objects.

Prerequisites

- > The HSM must be initialized (see ["Initializing the HSM" on page 136](#)).
- > You require the HSM SO credential (blue PED key).

To create an application partition

1. Connect to the appliance via SSH or a serial connection, and log in to LunaSH as **admin** or **operator**, or a custom user with an **admin** or **operator** role (see [Logging In to LunaSH](#)).
2. Log in as HSM SO (see ["Logging In as HSM Security Officer" on page 148](#)).

lunash:> **hsm login**

3. Create the application partition, specifying a partition name. This name is distinct from the partition label assigned during initialization and can be changed later. You can also specify the desired partition size in bytes (see also "[Customizing Partition Sizes](#)" below).

Partition names created in LunaSH must be 1-32 characters in length. The following characters are allowed:

abcdefghijklmnopqurstuvwxyzABCDEFGHIJKLMNPOQRSTUVWXYZ 0123456789!@#%&^*()-_+={}[]:;./?~

Spaces are allowed; enclose the partition name in double quotes if it includes spaces.

The following characters are not allowed: & \ | ; < > ` ' " ?

No two partitions can have the same name.

lunash:> **partition create -partition <name> [-size <size> | -allfreestorage]**

4. [Optional] Confirm that the partition was created.

lunash:> **partition list**

To delete an application partition

1. Connect to the appliance via SSH or a serial connection, and log in to LunaSH as **admin** or **operator**, or a custom user with an **admin** or **operator** role (see [Logging In to LunaSH](#)).
2. Log in as HSM SO (see "[Logging In as HSM Security Officer](#)" on page 148).

lunash:> **hsm login**

3. Delete the application partition by specifying its name.

lunash:> **partition delete -partition <name>**

Customizing Partition Sizes

If you do not specify a size in bytes when creating a partition, LunaSH automatically assigns an equal share of the total HSM memory. For example, if you purchased a Luna Network HSM with 16MB of memory and 10 partition licenses, each partition would have a default size of 1.6 MB. The basic allotment ensures that you can create all licensed partitions, each with enough space to hold at least one RSA key pair.

The maximum number of partitions depends on the model of Luna Network HSM you purchased. Your HSM can be upgraded with additional partition licenses if your desired configuration calls for them.

LunaSH allows you to customize the size of a partition for its intended purpose. You can choose to do this when you create each partition, or you can re-size them later, even if the partition is initialized. You must log in as HSM SO to re-size existing partitions.

- > ["Creating a Custom-Sized Partition" on the next page](#)
- > ["Re-sizing an Existing Partition" on the next page](#)
- > ["Creating Multiple Equal Large Partitions" on page 166](#)

Prerequisites

Use lunash:> **hsm show** to see:

- > Total HSM storage

- > Current memory usage
- > Current number of partitions
- > Maximum number of partitions allowed

Use `lunash:> partition list` to see:

- > All current application partitions
- > Total storage allotted to each
- > Total used and available storage on each partition

NOTE Each partition requires 9648 bytes of memory to store security and identity information. Take this into account when creating very small specialized partitions (for example, a partition containing a single key pair for signing and verification).

Creating a Custom-Sized Partition

Use the following procedure to specify the size of a new application partition. You must be logged in as HSM SO to create new partitions.

To create a custom-sized partition

1. Connect to the appliance via SSH or a serial connection, and log in to LunaSH as **admin** or **operator**, or a custom user with an **admin** or **operator** role (see [Logging In to LunaSH](#)).
2. Log in to the HSM as HSM SO (see ["Logging In as HSM Security Officer" on page 148](#)).
3. Create the application partition, specifying the desired size in bytes. To use all remaining space on the HSM, specify **-allfreestorage** instead of **-size**.

Partition names created in LunaSH must be 1-32 characters in length. The following characters are allowed:

abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ 0123456789!@#\$\$%^*()_+={}[]:;./?~

Spaces are allowed; enclose the partition name in double quotes if it includes spaces.

The following characters are not allowed: & \ | ; < > ` ' " ?

No two partitions can have the same name.

`lunash:> partition create -partition <name> [-size <size> | -allfreestorage]`

Re-sizing an Existing Partition

Use the following procedure to change the size of an existing application partition. You can change the size of any partition on the HSM, even if it is already initialized, as long as the space is available on the HSM and target size is not less than the objects currently stored on the partition. You must be logged in as HSM SO to re-size partitions.

CAUTION! Before you re-size a partition, back up the partition contents. If a partition is at or near capacity, it might be necessary to remove some objects before re-sizing. You may need to restore the partition from backup after it has been re-sized.

To re-size an existing partition

1. Connect to the appliance via SSH or a serial connection, and log in to LunaSH as **admin** or **operator**, or a custom user with an **admin** or **operator** role (see [Logging In to LunaSH](#)).
2. Log in to the HSM as HSM SO (see ["Logging In as HSM Security Officer" on page 148](#)).
3. Re-size the desired partition by specifying the partition name and the desired size in bytes. To use all remaining space on the HSM, specify **-allfreestorage** instead of **-size**.

```
lunash:> partition resize -partition <name> {-size <size> | -allfreestorage}
```

Creating Multiple Equal Large Partitions

You can use the re-sizing function to customize the space usage on the HSM. If you prefer to have all your partitions sized equally, and to let the HSM do the calculations, the following example might be useful. In this example, the HSM has 20 partition licenses.

To create four equal-size partitions, using all the available storage

1. Start by creating 20 partitions (the maximum allowed) – each will have X bytes available to it.
2. Delete 4 of them (leaving 16).
3. Re-size one partition to use **-allfreestorage**, which makes that partition as large as five small partitions – the four partitions you just deleted, freeing their allotment, plus the one you are currently resizing – and leaves the HSM with 15 partitions having X bytes each, plus the large one.

```
lunash:> partition resize -partition <name> -allfreestorage
```
4. Delete another four small partitions.
5. Re-size one small partition to use **-allfreestorage**, which makes that partition large (there are now two equally-sized large partitions) and leaves the HSM with 10 partitions having X bytes each, plus the two large ones.
6. Delete another four small partitions.
7. Re-size one small partition to use **-allfreestorage**, which makes that partition large (there are now three equally-sized large partitions) and leaves the HSM with 5 partitions having X bytes each, plus the three large ones.
8. Delete another four small partitions.
9. Re-size the single remaining small partition to use **-allfreestorage**, which makes that partition large and leaves 0 (zero) of the original partitions with X bytes each, and the four large partitions of equal size, with no unallocated space on the HSM.

This example uses conveniently round numbers. You might have a few bytes left over, or one partition slightly larger or smaller than the others, depending on the actual configuration of your HSM.

CHAPTER 8: Security in Operation

This section addresses actions and settings with security-related implications.

- > ["Security Effects of Administrative Actions" below](#)
- > ["Tamper Events" on page 172](#)

Refer also to [Security of Your Partition Challenge](#).

Security Effects of Administrative Actions

Actions that you take, in the course of administering your Luna HSM, can have effects, including destruction, on the roles, the spaces, and the contents of your HSM and its application partition(s). It is important to be aware of such consequences before taking action.

Overt Security Actions

Some actions in the administration of the HSM, or of an application partition, are explicitly intended to adjust specific security aspects of the HSM or partition. Examples are:

- > Changing a password
- > Modifying a policy to make a password or other attribute more stringent than the original setting

Those are discussed in their own sections.

Actions with Security- and Content-Affecting Outcomes

Other administrative events have security repercussions as included effects of the primary action, which could have other intent. Some examples are:

- > HSM factory reset
- > HSM zeroization
- > Change of a destructive policy
- > HSM initialization
- > HSM firmware rollback
- > Application partition initialization

This table lists some major administrative actions that can be performed on the HSM, and compares relevant security-related effects. Use the information in this table to help decide if your contemplated action is appropriate in current circumstances, or if additional preparation (such as backup of partition content, collection of audit data) would be prudent before continuing.

Factory Reset HSM

Domain	Destroyed
HSM SO Role	Destroyed
Partition SO Role	Destroyed
Auditor Role	Destroyed
Partition Roles	Destroyed
HSM or Partition/Contents	HSM/Destroyed
HSM Policies	Reset
RPV	Destroyed
Messaging	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

Domain	Destroyed
HSM SO Role	Destroyed
Partition SO Role	Destroyed
Auditor Role	Unchanged
Partition Roles	Destroyed
HSM or Partition/Contents	HSM/Destroyed
HSM Policies	Unchanged
RPV	Unchanged
Messaging	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

Domain	Unchanged
---------------	-----------

HSM SO Role	Unchanged
Partition SO Role	Destroyed
Auditor Role	Unchanged
Partition Roles	Destroyed
HSM or Partition/Contents	HSM/Destroyed
HSM Policies	Unchanged except for new policy
RPV	Unchanged
Messaging	You are about to change a destructive HSM policy. All partitions of the HSM will be destroyed.

HSM Initialize When Zeroized (hard init)

Domain	Destroyed
HSM SO Role	Destroyed
Partition SO Role	Destroyed
Auditor Role	Unchanged
Partition Roles	Destroyed
HSM or Partition/Contents	HSM/Destroyed
HSM Policies	Unchanged
RPV	Unchanged
Messaging	You are about to initialize the HSM. All contents of the HSM will be destroyed.

HSM Initialize From Non-Zeroized State (soft init)

Domain	Unchanged
HSM SO Role	Unchanged
Partition SO Role	Destroyed

Auditor Role	Unchanged
Partition Roles	Destroyed
HSM or Partition/Contents	HSM/Destroyed
HSM Policies	Unchanged
RPV	Unchanged
Messaging	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

Domain	Destroyed
HSM SO Role	Destroyed
Partition SO Role	Destroyed
Auditor Role	Destroyed
Partition Roles	Destroyed
HSM or Partition/Contents	HSM/Destroyed
HSM Policies	Unchanged
RPV	Unchanged
Messaging	<p>WARNING: This operation will rollback your HSM to the previous firmware version !!!</p> <p>(1) This is a destructive operation. (2) You will lose all your partitions. (3) You may lose some capabilities. (4) You must re-initialize the HSM. (5) If the PED use is remote, you must re-connect it.</p>

Partition Initialize When Zeroized (hard init)

Domain	Unchanged
HSM SO Role	Unchanged

Partition SO Role	Destroyed
Auditor Role	Unchanged
Partition Roles	Destroyed
HSM or Partition/Contents	Partition/Destroyed
HSM Policies	Unchanged
RPV	Unchanged
Messaging	You are about to initialize the partition. All contents of the partition will be destroyed.

Partition Initialize From Non-Zeroized State (soft init)

Domain	Unchanged
HSM SO Role	Unchanged
Partition SO Role	Destroyed
Auditor Role	Unchanged
Partition Roles	Destroyed
HSM or Partition/Contents	Partition/Destroyed
HSM Policies	Unchanged
RPV	Unchanged
Messaging	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

Luna Network 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 150). While the HSM is in the tamper condition, only the subset of LunaSH commands required to view the HSM status or clear the tamper condition are available. For 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. The tamper state is indicated by the **HSM Tamper State** field in the output of `lunash:> hsm show`. If tamper events have been detected and not cleared, the field will read **Tamper(s) detected**. Use `lunash:>hsm tamper show` to view detailed information for the tamper event, including whether it requires an HSM reset in addition to a tamper clear.

NOTE A tamper event resets the HSM hardware, including the PCIe logic. This prevents the HSM from reporting any statuses, including the cause of the tamper condition. The only thing which is detected in this case is `k7pf0: ALM0015: PCIe Link Failure`. The HSM must be rebooted before the cause of the tamper event can be reported.

Tamper event	Response
Chassis intrusion	Halt the HSM. Deactivate activated partitions. Decommission the HSM if policy 40: Decommission on Tamper is enabled.
Card removal	Halt the HSM. Deactivate activated partitions. Decommission the HSM if policy 40: Decommission on Tamper is enabled.
Over/under temperature	Halt the HSM. Deactivate activated partitions. Decommission the HSM if policy 40: Decommission on Tamper is enabled. 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. Decommission the HSM if policy 40: Decommission on Tamper is enabled. 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. Decommission the HSM. 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 150 for more information:

Policy 40: Decommission on tamper	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).
Policy 48: Do Controlled Tamper Recovery	If enabled, the tamper condition that halted the HSM must be cleared by the HSM SO (by issuing the tamper clear 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. Use the following command to display the last tamper event:

```
lunash:> hsm tamper show
```

NOTE `hsm tamper show` only shows the last tamper event, even if several tampers have occurred. To view a complete list of the tamper events that have occurred on the HSM, use `lunash:> hsm supportinfo`.

2. Resolve the issue(s) that caused the tamper event.
3. If **Policy 48: Do Controlled Tamper Recovery** is enabled, clear the tamper condition. Otherwise, go to the next step:

```
lunash:> hsm tamper clear
```

4. If the tamper message indicates that a reset is required, reboot the HSM:

lunash:> **hsm restart**

5. Verify that all tampers have been cleared:

lunash:> **hsm tamper show**

6. If the HSM was decommissioned as a result of the tamper, you must re-create your partitions, re-initialize the partition roles (Partition SO, Crypto Officer, and Crypto User, and Audit as relevant), and restore the partition contents from backup. Refer to the following procedures:
 - a. To re-create your partitions, see "[Creating or Deleting an Application Partition](#)" on page 163.
 - 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 9: Monitoring the HSM

Thales provides different methods of monitoring activity on the HSM. This chapter contains the following sections:

- > "HSM Status Values" below
- > "System Operational and Error Messages" on the next page
- > "Performance Monitoring" on page 178
- > "Partition Utilization Metrics" on page 179
- > "Keycard and Token Return Codes" on page 181
- > "Library Codes" on page 199
- > "Vendor-Defined Return Codes" on page 203
- > "HSM Alarm Codes" on page 209

Refer also to [About the Syslog and SNMP Monitoring Guide](#).

HSM Status Values

Each HSM administrative slot shown in a LunaCM slot listing includes an HSM status. Here are the possible values and what they mean, and what is required to recover from each one. In LunaSH, this information is displayed under *HSM Details* by running **hsm show**.

Indicated Status of HSM	Meaning	Recovery
OK	The HSM is in a good state, working properly.	n/a
Zeroized	The HSM is in zeroized state. All objects and roles are unusable.	HSM initialization is required before the HSM can be used again. "Hard init" - HSM SO and domain are gone, no authentication required. (see Note1)
Decommissioned	The HSM has been decommissioned.	HSM initialization is required before the HSM can be used again. "Hard init" - HSM SO and domain are gone, no authentication required. (see Note1)
Transport Mode	The HSM is in Secure Transport Mode.	STM must be disabled before the HSM can be used.
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 Luna PCIe HSM, or ureset for 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.) The HSM is also in zeroized state. All objects and roles are unusable.	Reboot the host or restart the HSM (vreset for Luna PCIe HSM, or ureset for Luna USB HSM). The event is logged. 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.) The HSM has also been decommissioned.	Reboot the host or restart the HSM (vreset for Luna PCIe HSM, or ureset for Luna USB HSM). The event is logged. 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 136](#) for more information.

For a comparison of various destruction or denial actions on the HSM, see ["Comparison of Destruction/Denial Actions" on page 256](#).

System Operational and Error Messages

Extra slots that say "token not present"?

This happens for two reasons:

- > PKCS#11 originated in a world of software cryptography, which only later acknowledged the existence of Hardware Security Modules, so initially it did not have the concept of physically removable crypto slots. PKCS#11 requires a static list of slots when an application starts. The cryptographic "token" can be inserted into, or removed from a slot dynamically (by a user), for the duration of the application.
- > When the token is inserted, the running application must be able to detect that token. When the token is removed, the running application gets "token not present". Because we allow for the possibility of backup, we routinely declare 'place-holder' slots that might later be filled by a physical Luna USB HSM or a Luna Backup HSM.

In the `Chrystoki.conf` file (or the Windows `crystoki.ini` file), for Luna USB HSM, you can remove the empty slots by modifying the `CardReader` entry, like this:

```
CardReader = {
  LunaG5Slots=0;
}
```

For 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 Luna HSM problem.

Error during SSL Connect (RC_OPERATION_TIMED_OUT) logged to /var/log/messages by the Luna HSM Client

It means that the client did not receive the SSL handshake response from the appliance within 20 seconds (hard coded).

The following is a list of some potential causes:

- > Network issue.
- > Appliance is under heavy load with connection requests - this can happen at startup/restart, if client applications attempt to (re-)assert hundreds of connections all at once, without staging or staggering them, and the initial setup handshakes take too long for some transactions (start-up bottleneck). After a large number of simultaneous connections has been successfully established, they can be maintained without further problem.
- > Appliance is under heavy load servicing crypto requests from connected clients.
- > Appliance was powered down (perhaps the power plug was pulled) in the middle of the handshake.
- > The client computer might be experiencing high CPU load, causing it to occasionally delay responses to the appliance.

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 Luna Network HSM and 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.

Performance Monitoring

An HSM administrator might find it helpful to know how busy the HSM is and at what percentage of its capacity it has been running.

The HSM Information Monitor is a use counter that provides an indication of momentary and cumulative resource usage on the HSM, in the form of a percentage. The HSM firmware tracks the overall time elapsed since the last reset (Up-Time), and the overall time during which the processor was not performing useful work (Idle-Time).

On request, the HSM calculates "Busy-time" over an interval, by subtracting Idle-time for that interval from Up-time for the interval. Then, the load on the processor is calculated as the Busy-time divided by the Up-time, and expressed as a percentage.

You can use the available commands for a single, one-off query, which actually takes an initial reading and then another, five seconds later (the default setting), in order to calculate and show the one-time difference.

You can specify a sampling interval (five seconds is the shortest) and a number of repetitions for an extended view of processor activity/resource usage. The resulting records, showing the time of each measurement, the percentage value at that time, and the difference from the previous measurement, can be output to a file that you import into other tools to analyze and graph the trends.

By watching trends and correlating with what your application is doing, you can:

- > Determine the kinds of loads you are placing on the HSM.

- > Seek efficiencies in how your applications are coded and configured.
- > Plan for expansion or upgrades of your existing HSM infrastructure.
- > Plan for upgrades of electrical capacity and HVAC capacity.

Notes about Monitor/Counter Behavior

When performing certain operations the HSM reaches its maximum performance capability before the counter reaches 100%. This occurs because the counter measures the load on the HSM's CPU and the CPU is able to saturate the asymmetric engines and still have capacity to perform other actions.

Also, symmetric cryptographic operations cause the counter to quickly rise to 90% even though there is significant remaining capacity. This behavior occurs because, as the HSM receives more concurrent symmetric commands, its CPU is able to handle them more efficiently (by performing them in bulk) – thus achieving more throughput from the same number of CPU cycles.

See lunash:> [hsm information](#).

Partition Utilization Metrics

In order to ensure the quality of service (QoS) that you provide to applications that make use of HSM partitions, it is first necessary to know how the users and applications are making use of the HSM resources - that is, the distribution of demand.

For an HSM with a single application partition, it can be helpful to know what type of load is being imposed on the HSM and the enumeration and categorization of operations that are being performed. Application developers might have a good idea of the expected ratio of operations, but the operations team managing the application servers would like to know the real-world utilization, for their planning and management purposes.

For a 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, appliance software 7.3, 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 qos metrics show** command allows you to view the current utilization counter values for all partitions, and overall counts for the entire HSM, or to export the current counts to a file, without resetting the counters.

The **hsm qos metrics reset** command allows you to reset to zero the current utilization counter values for all partitions; additionally, you have the option to view the current counts or to export the current counts to a file, without losing any counts between the view/export action and the reset action.

To access the Partition Utilization Metrics feature

1. Ensure that your HSM is at firmware version 7.3 or newer (if needed, upgrade to a suitable version; see ["Updating the Luna HSM Firmware" on page 221](#)).
2. Log in as HSM SO (see ["Logging In as HSM Security Officer" on page 148](#)).
lunash:> **hsm login**
3. Enable HSM policy 49: Allow Partition Utilization Metrics.
lunash:> **hsm changepolicy -policy 49 -value 1**

To view or save Partition Utilization Metrics without resetting

lunash:> **hsm qos metrics show**

To reset the Partition Utilization Metrics counters to zero

Metrics are reset whenever power is lost to the HSM or the HSM is reset, or the HSM is initialized. These events do not save the metrics.

To reset the metrics without exporting:

```
lunash:> hsm qos metrics reset
```

To reset the Partition Utilization Metrics counters to zero while also viewing or exporting the information

```
lunash:> hsm qos metrics reset -export <filename>
```

The current counter values are saved to a named file before they are zeroed.

```
lunash:> hsm qos metrics reset -display
```

The counter data is displayed but not saved.

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

HSM Error	Hex Code	PKCS#11 or SFNT Defined CKR Error
LUNA_RET_PED_UNSUPPORTED_CRYPTOPROTOCOL	0x00300145	CKR_DEVICE_ERROR
LUNA_RET_PED_DEK_INVALID	0x00300146	CKR_DEVICE_ERROR
LUNA_RET_PED_CLIENT_NOT_RUNNING	0x00300147	CKR_PED_CLIENT_NOT_RUNNING
LUNA_RET_CL_ALIGNMENT_ERROR	0x00300200	CKR_DEVICE_ERROR
LUNA_RET_CL_QUEUE_LOCATION_ERROR	0x00300201	CKR_DEVICE_ERROR
LUNA_RET_CL_QUEUE_OVERLAP_ERROR	0x00300202	CKR_DEVICE_ERROR
LUNA_RET_CL_TRANSMISSION_ERROR	0x00300203	CKR_DEVICE_ERROR
LUNA_RET_CL_NO_TRANSMISSION	0x00300204	CKR_DEVICE_ERROR
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

HSM Error	Hex Code	PKCS#11 or SFNT Defined CKR Error
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
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

HSM Error	Hex Code	PKCS#11 or SFNT Defined CKR Error
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
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

HSM Error	Hex Code	PKCS#11 or SFNT Defined CKR 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
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

HSM Error	Hex Code	PKCS#11 or SFNT Defined CKR 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
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

HSM Error	Hex Code	PKCS#11 or SFNT Defined CKR 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
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

HSM Error	Hex Code	PKCS#11 or SFNT Defined CKR Error
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
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

HSM Error	Hex Code	PKCS#11 or SFNT Defined CKR 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
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

HSM Error	Hex Code	PKCS#11 or SFNT Defined CKR Error
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
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

HSM Error	Hex Code	PKCS#11 or SFNT Defined CKR Error
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
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

HSM Error	Hex Code	PKCS#11 or SFNT Defined CKR Error
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
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

HSM Error	Hex Code	PKCS#11 or SFNT Defined CKR Error
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
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

HSM Error	Hex Code	PKCS#11 or SFNT Defined CKR Error
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
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

HSM Error	Hex Code	PKCS#11 or SFNT Defined CKR Error
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
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

HSM Error	Hex Code	PKCS#11 or SFNT Defined CKR Error
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
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

HSM Error	Hex Code	PKCS#11 or SFNT Defined CKR Error
LUNA_RET_HSM_STORAGE_FULL	0x80000902	CKR_HSM_STORAGE_FULL
LUNA_RET_CONTAINER_OBJECT_STORAGE_FULL	0x80000903	CKR_CONTAINER_OBJECT_STORAGE_FULL
LUNA_RET_KEY_NOT_ACTIVE	0x80000904	CKR_KEY_NOT_ACTIVE
LUNA_RET_CB_NOT_SUPPORTED	0x80000a01	CKR_FUNCTION_NOT_SUPPORTED
LUNA_RET_CB_PARAM_INVALID	0x80000a02	CKR_CALLBACK_ERROR
LUNA_RET_CB_NO_MEMORY	0x80000a03	CKR_DEVICE_MEMORY
LUNA_RET_CB_TIMEOUT	0x80000a04	CKR_CALLBACK_ERROR
LUNA_RET_CB_RETRY	0x80000a05	CKR_CALLBACK_ERROR
LUNA_RET_CB_ABORTED	0x80000a06	CKR_CALLBACK_ERROR
LUNA_RET_CB_SYS_ERROR	0x80000a07	CKR_CALLBACK_ERROR
LUNA_RET_CB_HIOS_HANDLE_INVALID	0x80000a10	CKR_CALLBACK_ERROR
LUNA_RET_CB_HIOS_ID_INVALID	0x80000a11	CKR_CALLBACK_ERROR
LUNA_RET_CB_HIOS_CLOSED	0x80000a12	CKR_CALLBACK_ERROR
LUNA_RET_CB_HIOS_CANCELED	0x80000a13	CKR_CALLBACK_ERROR
LUNA_RET_CB_HIOS_IO_ERROR	0x80000a14	CKR_CALLBACK_ERROR
LUNA_RET_CB_HIOS_SEND_TIMEOUT	0x80000a15	CKR_CALLBACK_ERROR
LUNA_RET_CB_HIOS_RECV_TIMEOUT	0x80000a16	CKR_CALLBACK_ERROR
LUNA_RET_CB_HIOS_STATE_INVALID	0x80000a17	CKR_CALLBACK_ERROR
LUNA_RET_CB_HIOS_OUTPUT_BUFFER_TOO_SMALL	0x80000a18	CKR_CALLBACK_ERROR
LUNA_RET_CB_HIOS_INPUT_BUFFER_TOO_SMALL	0x80000a19	CKR_CALLBACK_ERROR

HSM Error	Hex Code	PKCS#11 or SFNT Defined CKR 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
LUNA_RET_CB_SYNC_ERROR	0x80000a28	CKR_CALLBACK_ERROR
LUNA_RET_CB_PROT_DATA_INVALID	0x80000a29	CKR_CALLBACK_ERROR
LUNA_RET_LOG_FILE_NOT_OPEN	0x80000d00	CKR_LOG_FILE_NOT_OPEN
LUNA_RET_LOG_FILE_WRITE_ERROR	0x80000d01	CKR_LOG_FILE_WRITE_ERROR
LUNA_RET_LOG_BAD_FILE_NAME	0x80000d02	CKR_LOG_BAD_FILE_NAME
LUNA_RET_LOG_FULL	0x80000d03	CKR_LOG_FULL
LUNA_RET_LOG_NO_KCV	0x80000d04	CKR_LOG_NO_KCV
LUNA_RET_LOG_BAD_RECORD_HMAC	0x80000d05	CKR_LOG_BAD_RECORD_HMAC
LUNA_RET_LOG_BAD_TIME	0x80000d06	CKR_LOG_BAD_TIME
LUNA_RET_LOG_AUDIT_NOT_INITIALIZED	0x80000d07	CKR_LOG_AUDIT_NOT_INITIALIZED
LUNA_RET_LOG_RESYNC_NEEDED	0x80000d08	CKR_LOG_RESYNC_NEEDED
LUNA_RET_AUDIT_LOGIN_TIMEOUT_IN_PROGRESS	0x80000d09	CKR_AUDIT_LOGIN_TIMEOUT_IN_PROGRESS
LUNA_RET_AUDIT_LOGIN_FAILURE_THRESHOLD	0x80000d0a	CKR_AUDIT_LOGIN_FAILURE_THRESHOLD

HSM Error	Hex Code	PKCS#11 or SFNT Defined CKR Error
LUNA_RET_XTC_ERROR	0x80001600	CKR_XTC_ERROR
LUNA_RET_CONTEXT_INVALID	0x80001601	CKR_CONTEXT_INVALID
LUNA_RET_SESSION_COUNT	0x80001603	CKR_MAX_SESSION_COUNT
LUNA_RET_BUSY	0x80001604	CKR_BUSY

* This error (CKR_TEMPLATE_INCONSISTENT) might be encountered when using CKDemo in a new client with firmware older than version 6.22.0. Try CKDemo option 98, sub-option 16. If it is set to "enhanced roles", try selecting it to set it to "legacy Luna roles". The setting is a toggle, and flips every time you select it.

** This error, or "unable to read public key", might be encountered when using BSAFE to encrypt data with ECC public key using curves from the Brainpool suite. As indicated on the BSAFE website (May 2012) they do not appear to support Brainpool curves. Therefore, your own applications should not attempt that combination, and you should avoid attempting to specify Brainpool curves with BSAFE ECC when using the Luna CKDemo utility.

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

Hex value	Decimal value	Return code/error description
0xC0000103	3221225731	INVALID PIN
0xC0000104	3221225732	NO TOKEN PRESENT
0xC0000105	3221225733	FUNCTION IS NOT SUPPORTED
0xC0000106	3221225734	NON-CRYPTOKI ELEMENT CLONE
0xC0000107	3221225735	INVALID BUFFER SIZE FOR CHALLENGE
0xC0000108	3221225736	PIN IS LOCKED
0xC0000109	3221225737	INVALID VERSION
0xC000010a	3221225738	NEEDED KEY NOT PROVIDED
0xC000010b	3221225739	USER NAME IS IN USE
0xC0000200	3221225984	INVALID DISTINGUISHED ENCODING RULES CLASS
0xC0000303	3221226243	OPERATION TIMED OUT
0xC0000304	3221226244	RESET FAILED
0xC0000400	3221226496	INVALID TOKEN STATE
0xC0000401	3221226497	DATA APPEARS CORRUPTED
0xC0000402	3221226498	INVALID FILENAME
0xC0000403	3221226499	FILE IS READ-ONLY
0xC0000404	3221226500	FILE ERROR
0xC0000405	3221226501	INVALID OBJECT IDENTIFIER
0xC0000406	3221226502	INVALID SOCKET ADDRESS
0xC0000407	3221226503	INVALID LISTEN SOCKET
0xC0000408	3221226504	CACHE IS NOT CURRENT
0xC0000409	3221226505	CACHE IS NOT MAPPED

Hex value	Decimal value	Return code/error description
0xC000040a	3221226506	OBJECT IS NOT IN LIST
0xC000040b	3221226507	INVALID INDEX
0xC000040c	3221226508	OBJECT ALREADY EXISTS
0xC000040d	3221226509	SEMAPHORE ERROR
0xC000040e	3221226510	END OF LIST ENCOUNTERED
0xC000040f	3221226511	WOULD ASSIGN SAME VALUE
0xC0000410	3221226512	INVALID GROUP NAME
0xC0000411	3221226513	NOT HSM BACKUP TOKEN
0xC0000412	3221226514	NOT PARTITION BACKUP TOKEN
0xC0000413	3221226515	SIM NOT SUPPORTED
0xC0000500	3221226752	SOCKET ERROR
0xC0000501	3221226753	SOCKET WRITE ERROR
0xC0000502	3221226754	SOCKET READ ERROR
0xC0000503	3221226755	CLIENT MESSAGE ERROR
0xC0000504	3221226756	SERVER DISCONNECTED
0xC0000505	3221226757	CLIENT DISCONNECTED
0xC0000506	3221226758	SOCKET WOULD BLOCK
0xC0000507	3221226759	SOCKET ADDRESS IS IN USE
0xC0000508	3221226760	SOCKET BAD FILE DESCRIPTOR
0xC0000509	3221226761	HOST RESOLUTION ERROR
0xC000050a	3221226762	INVALID HOST CERTIFICATE
0xC0000600	3221227008	NO BUFFER AVAILABLE
0xC0000601	3221227009	INVALID ENUMERATION OPTION

Hex value	Decimal value	Return code/error description
0xC0000700	3221227264	SSL ERROR
0xC0000701	3221227265	SSL CTX ERROR
0xC0000702	3221227266	SSL CIPHER LIST ERROR
0xC0000703	3221227267	SSL CERT VERIFICATION LOCATION ERROR
0xC0000704	3221227268	SSL LOAD SERVER CERT ERROR
0xC0000705	3221227269	SSL LOAD SERVER PRIVATE KEY ERROR
0xC0000706	3221227270	SSL VALIDATE SERVER PRIVATE KEY ERROR
0xC0000707	3221227271	SSL CREATE SSL ERROR
0xC0000708	3221227272	SSL LOAD CLIENT CERT ERROR
0xC0000709	3221227273	SSL GET CERTIFICATE ERROR
0xC000070a	3221227274	SSL INVALID CERT STRUCTURE
0xC000070b	3221227275	SSL LOAD CLIENT PRIVATE KEY ERROR
0xC000070c	3221227276	SSL GET PEER CERT ERROR
0xC000070d	3221227277	SSL WANT READ ERROR
0xC000070e	3221227278	SSL WANT WRITE ERROR
0xC000070f	3221227279	SSL WANT X509 LOOKUP ERROR
0xC0000710	3221227280	SSL SYSCALL ERROR
0xC0000711	3221227281	SSL FAILED HANDSHAKE
0xC0000800	3221227520	INVALID CERTIFICATE TYPE
0xC0000900	3221227776	INVALID PORT
0xC0000901	3221227777	SESSION SCRIPT EXISTS
0xC0001000	3221229568	PARTITION LOCKED

Hex value	Decimal value	Return code/error description
0xC0001001	3221229569	PARTITION NOT ACTIVATED
0xc0002000	3221233664	FAILED TO CREATE THREAD
0xc0002001	3221233665	CALLBACK ERROR
0xc0002002	3221233666	UNKNOWN CALLBACK COMMAND
0xc0002003	3221233667	SHUTTING DOWN
0xc0002004	3221233668	REMOTE SIDE DISCONNECTED
0xc0002005	3221233669	SOCKET CLOSED
0xC0002006	3221233670	INVALID COMMAND
0xC0002007	3221233671	UNKNOWN COMMAND
0xC0002008	3221233672	UNKNOWN COMMAND VERSION
0xC0002009	3221233673	FILE LOCK FAILED
0xC0002010	3221233680	FILE LOCK ERROR
0xc0002011	3221233681	FAILED TO CREATE PROCESS
0xc0002012	3221233682	USB PED NOT FOUND
0xc0002013	3221233683	USB PED NOT RESPONDING
0xc0002014	3221233684	USB PED OPERATION CANCELLED
0xc0002015	3221233685	USB PED TOO MANY CONNECTED
0xc0002016	3221233686	USB PED OUT OF SYNC
0xC0001100	3221229824	UNABLE TO CONNECT

Vendor-Defined Return Codes

Code	Name
0x80000004	CKR_RC_ERROR

Code	Name
0x80000005	CKR_CONTAINER_HANDLE_INVALID
0x80000006	CKR_TOO_MANY_CONTAINERS
0x80000007	CKR_USER_LOCKED_OUT
0x80000008	CKR_CLONING_PARAMETER_ALREADY_EXISTS
0x80000009	CKR_CLONING_PARAMETER_MISSING
0x8000000a	CKR_CERTIFICATE_DATA_MISSING
0x8000000b	CKR_CERTIFICATE_DATA_INVALID
0x8000000c	CKR_ACCEL_DEVICE_ERROR
0x8000000d	CKR_WRAPPING_ERROR
0x8000000e	CKR_UNWRAPPING_ERROR
0x8000000f	CKR_MAC_MISSING
0x80000010	CKR_DAC_POLICY_PID_MISMATCH
0x80000011	CKR_DAC_MISSING
0x80000012	CKR_BAD_DAC
0x80000013	CKR_SSK_MISSING
0x80000014	CKR_BAD_MAC
0x80000015	CKR_DAK_MISSING
0x80000016	CKR_BAD_DAK
0x80000017	CKR_SIM_AUTHORIZATION_FAILED
0x80000018	CKR_SIM_VERSION_UNSUPPORTED
0x80000019	CKR_SIM_CORRUPT_DATA
0x8000001a	CKR_USER_NOT_AUTHORIZED
0x8000001b	CKR_MAX_OBJECT_COUNT_EXCEEDED

Code	Name
0x8000001c	CKR_SO_LOGIN_FAILURE_THRESHOLD
0x8000001d	CKR_SIM_AUTHFORM_INVALID
0x8000001e	CKR_CITS_DAK_MISSING
0x8000001f	CKR_UNABLE_TO_CONNECT
0x80000020	CKR_PARTITION_DISABLED
0x80000021	CKR_CALLBACK_ERROR
0x80000022	CKR_SECURITY_PARAMETER_MISSING
0x80000023	CKR_SP_TIMEOUT
0x80000024	CKR_TIMEOUT
0x80000025	CKR_ECC_UNKNOWN_CURVE
0x80000026	CKR_MTK_ZEROIZED
0x80000027	CKR_MTK_STATE_INVALID
0x80000028	CKR_INVALID_ENTRY_TYPE
0x80000029	CKR_MTK_SPLIT_INVALID
0x8000002a	CKR_HSM_STORAGE_FULL
0x8000002b	CKR_DEVICE_TIMEOUT
0x8000002c	CKR_CONTAINER_OBJECT_STORAGE_FULL
0x8000002d	CKR_PED_CLIENT_NOT_RUNNING
0x8000002e	CKR_PED_UNPLUGGED
0x8000002f	CKR_ECC_POINT_INVALID
0x80000030	CKR_OPERATION_NOT_ALLOWED
0x80000031	CKR_LICENSE_CAPACITY_EXCEEDED
0x80000032	CKR_LOG_FILE_NOT_OPEN

Code	Name
0x80000033	CKR_LOG_FILE_WRITE_ERROR
0x80000034	CKR_LOG_BAD_FILE_NAME
0x80000035	CKR_LOG_FULL
0x80000036	CKR_LOG_NO_KCV
0x80000037	CKR_LOG_BAD_RECORD_HMAC
0x80000038	CKR_LOG_BAD_TIME
0x80000039	CKR_LOG_AUDIT_NOT_INITIALIZED
0x8000003A	CKR_LOG_RESYNC_NEEDED
0x8000003B	CKR_AUDIT_LOGIN_TIMEOUT_IN_PROGRESS
0x8000003C	CKR_AUDIT_LOGIN_FAILURE_THRESHOLD
0x8000003D	CKR_INVALID_FUF_TARGET
0x8000003E	CKR_INVALID_FUF_HEADER
0x8000003F	CKR_INVALID_FUF_VERSION
0x80000040	CKR_ECC_ECC_RESULT_AT_INF
0x80000041	CKR_AGAIN
0x80000042	CKR_TOKEN_COPIED
0x80000043	CKR_SLOT_NOT_EMPTY
0x80000044	CKR_USER_ALREADY_ACTIVATED
0x80000045	CKR_STC_NO_CONTEXT
0x80000046	CKR_STC_CLIENT_IDENTITY_NOT_CONFIGURED
0x80000047	CKR_STC_PARTITION_IDENTITY_NOT_CONFIGURED
0x80000048	CKR_STC_DH_KEYGEN_ERROR
0x80000049	CKR_STC_CIPHER_SUITE_REJECTED

Code	Name
0x8000004a	CKR_STC_DH_KEY_NOT_FROM_SAME_GROUP
0x8000004b	CKR_STC_COMPUTE_DH_KEY_ERROR
0x8000004c	CKR_STC_FIRST_PHASE_KDF_ERROR
0x8000004d	CKR_STC_SECOND_PHASE_KDF_ERROR
0x8000004e	CKR_STC_KEY_CONFIRMATION_FAILED
0x8000004f	CKR_STC_NO_SESSION_KEY
0x80000050	CKR_STC_RESPONSE_BAD_MAC
0x80000051	CKR_STC_NOT_ENABLED
0x80000052	CKR_STC_CLIENT_HANDLE_INVALID
0x80000053	CKR_STC_SESSION_INVALID
0x80000054	CKR_STC_CONTAINER_INVALID
0x80000055	CKR_STC_SEQUENCE_NUM_INVALID
0x80000056	CKR_STC_NO_CHANNEL
0x80000057	CKR_STC_RESPONSE_DECRYPT_ERROR
0x80000058	CKR_STC_RESPONSE_REPLAYED
0x80000059	CKR_STC_REKEY_CHANNEL_MISMATCH
0x8000005a	CKR_STC_RSA_ENCRYPT_ERROR
0x8000005b	CKR_STC_RSA_SIGN_ERROR
0x8000005c	CKR_STC_RSA_DECRYPT_ERROR
0x8000005d	CKR_STC_RESPONSE_UNEXPECTED_KEY
0x8000005e	CKR_STC_UNEXPECTED_NONCE_PAYLOAD_SIZE
0x8000005f	CKR_STC_UNEXPECTED_DH_DATA_SIZE
0x80000060	CKR_STC_OPEN_CIPHER_MISMATCH

Code	Name
0x80000061	CKR_STC_OPEN_DHNIST_PUBKEY_ERROR
0x80000062	CKR_STC_OPEN_KEY_MATERIAL_GEN_FAIL
0x80000063	CKR_STC_OPEN_RESP_GEN_FAIL
0x80000064	CKR_STC_ACTIVATE_MACTAG_U_VERIFY_FAIL
0x80000065	CKR_STC_ACTIVATE_MACTAG_V_GEN_FAIL
0x80000066	CKR_STC_ACTIVATE_RESP_GEN_FAIL
0x80000067	CKR_CHALLENGE_INCORRECT
0x80000068	CKR_ACCESS_ID_INVALID
0x80000069	CKR_ACCESS_ID_ALREADY_EXISTS
0x8000006a	CKR_KEY_NOT_KEKABLE
0x8000006b	CKR_MECHANISM_INVALID_FOR_FP
0x8000006c	CKR_OPERATION_INVALID_FOR_FP
0x8000006d	CKR_SESSION_HANDLE_INVALID_FOR_FP
0x8000006e	CKR_CMD_NOT_ALLOWED_HSM_IN_TRANSPORT
0x8000006f	CKR_OBJECT_ALREADY_EXISTS
0x80000070	CKR_PARTITION_ROLE_DESC_VERSION_INVALID
0x80000071	CKR_PARTITION_ROLE_POLICY_VERSION_INVALID
0x80000072	CKR_PARTITION_ROLE_POLICY_SET_VERSION_INVALID
0x80000073	CKR_REKEK_KEY
0x80000074	CKR_KEK_RETRY_FAILURE
0x80000075	CKR_RNG_RESEED_TOO_EARLY
0x80000076	CKR_HSM_TAMPERED
0x80000077	CKR_CONFIG_CHANGE_ILLEGAL

Code	Name
0x80000078	CKR_SESSION_CONTEXT_NOT_ALLOCATED
0x80000079	CKR_SESSION_CONTEXT_ALREADY_ALLOCATED
0x8000007a	CKR_INVALID_BL_ITB_AUTH_HEADER
0x80000114	CKR_OBJECT_READ_ONLY
0x80000136	CKR_KEY_NOT_ACTIVE
0x80000400	CKR_ACCESS_ID_INVALID
0x80001600	CKR_XTC_ERROR
0x80001601	CKR_CONTEXT_INVALID
0x80001603	CKR_MAX_SESSION_COUNT
0x80001604	CKR_BUSY
0x80001606	CKR_SERVICE_UNAVAILABLE

HSM Alarm Codes

The Luna PCIe HSM alarm messages indicate error conditions on the HSM card that might require user intervention. The alarms apply to a Luna HSM, compliant with security level FIPS 140-2 Level 3. The alarm messages provide appropriate detail to alert HSM users of important events. Each alarm message has a unique character string for the message ID that allows higher level tools on the host system to parse for the alarm message IDs and generate notifications.

Messages are saved to the system log file in Linux host systems, allowing host application software like SNMP to parse the log file, and to the Windows Event Viewer in Windows host systems

Messages can be retrieved with the "dmesg" utility, to read messages from the driver log, which collects messages from the bootloader (BL), the firmware (FW), or from the Host Driver itself.

This section contains the following information:

- > ["Alarm Generation and Handling" on the next page](#)
- > ["List of HSM Alarm Codes" on page 211](#)
- > ["HSM Alarm Code Samples" on page 215](#)
- > ["Stored Data Integrity" on page 219](#)

Alarm Generation and Handling

Alarm messages can be generated due to the HSM BL, FW, and Host Driver SW detecting unexpected conditions. Other alarm messages are generated after unexpected interrupts or tamper events. For each of these problems detailed error information and an alarm message is output to notify the user that something special has happened.

At least one alarm message is output as a result of each tamper event by BL, FW, or Host Driver. Depending on the type of tamper all of them may report an alarm message related to the same tamper event. The message timestamps assist you to identify which alarm messages are for the same tamper event. Tamper alarm messages from BL, FW, and Host Driver have the same text description for the same tamper event. A specific type of tamper event is not reported again until FW clears the tamper information in the tamper circuit. If the tamper event happens after that, then either a new tamper condition has been detected or the same tamper event is still active and cannot be cleared.

Alarm Handling for Special Situations

Alarm messages are still generated during rare occurrences where BL, FW, or Host Driver might be in an abnormal state.

As long as the Host Driver is running, the BL and FW are able to output their alarm messages to the DLOG (driver log), which can be parsed to notify the user. If either BL or FW stops execution due to error detection, they output an alarm message to the Host Driver, which stores it in DLOG. All BL and FW checking for alarm conditions is stopped but all HW tamper event monitoring (soft and hard tampers) is still enabled including Host Driver monitoring. The card reset caused by these tampers restarts BL and possibly FW and the alarm messages are output. The following situations are also handled:

- > **BL starts before Host Driver is loaded (System power-up):** Without Host Driver available, BL outputs all alarms only to an internal HSM log. When the Host Driver loads it resets the HSM card, causing BL to start again. BL can then send any new alarms to the host driver and either stop or proceed to FW, as the situation allows.
 - For an L3 card if FW is started it will output alarm messages for any existing tamper conditions. Any tamper event alarm messages including those not sent out while the Host Driver was not loaded can be fetched from the FRAM Log.

NOTE If needed, use `lunash:> hsm supportinfo` to output the FRAM Log in order to determine the tamper information, or to pass on to Thales Technical Support.

- > **FW halted due to internal error:** In order to get to FW the Host Driver must be running so the FW halted alarm message will be stored in DLOG. No further BL or FW alarm messages are generated in this state until the next card reset.
- > **FW in locked state (tamper clear required):** An alarm message is generated to signal locked state is active. FW is still doing periodic checks and FW alarm messages are still possible. Only a small subset of FW commands is available.
- > **FW in Secure Transport Mode (STM):** An alarm message is generated to signal STM is active. FW is still doing periodic checks and FW alarm messages are still possible. Only a small subset of FW commands are available.

- > **Host Driver loses communications with the HSM card:** If the Host Driver has any errors communicating with the K7 (BL or FW) it will generate alarm messages. The Host Driver also periodically checks that the 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 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
Host Driver			Tamper Flag
0001	Soft tamper - over voltage	HSM voltage is above the operating range. HSM will stay in reset until voltage goes back in range.	HCCSR: VST
0002	Soft tamper - temperature (nnC)	HSM temperature (nn degrees Celsius) is outside the range (-2C to 80C). HSM will stay in reset until temperature goes back in range.	HRCSR: TST
0003	Soft tamper - indeterminate cause	A soft tamper occurred but cannot determine the cause.	
0004	Hard tamper - high temperature	HSM temperature is higher than 88C.	HT_T
0005	Hard tamper - low temperature	HSM temperature is lower than -40C	LT_T
0006	Hard tamper - over voltage	HSM voltage is higher than the maximum allowed.	OV_T, TC3_T
0009	Hard tamper - oscillator failure	HSM tamper clock oscillator has failed	OSC_T
0010	Decommission signal triggered	Decommission button (connector P9) has been pressed.	TC2_T
0011	Hard tamper - indeterminate cause	A hard tamper occurred but cannot determine the cause.	

ALM ID	Alarm Message	Description	Info
0012	Hardware Error	Error detected in device hardware	
0013	High Temperature - nnC	HSM has reached nn degrees Celsius and needs to be cooled to avoid tampering	
0014	Low Battery	HSM battery voltage is below 2.75V and needs to be replaced soon.	
0015	PCIe Link Failure	HSM no longer appears on PCIe bus. Chassis may have been opened.	
0016	Device Error	Internal error detected during communications with HSM	
0017	Request Timed Out	Request to HSM took too long	

Boot Loader			Tamper Flag
1000	Unknown alarm ID xx in boot loader	Illegal alarm ID used in Boot Loader.	
1001	HSM restart required	Soft or hard tamper occurred. HSM needs to be restarted (reset) before firmware is allowed to run.	
1003	HSM halted - internal boot loader error	Boot Loader detected an error during diagnostics and did not jump to FW.	
1004	Warning - boot loader diagnostic error	Boot Loader detected an error during diagnostics that does not stop execution but needs to be investigated (i.e. fan, VPD, or RTC problems).	
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.

ALM ID	Alarm Message	Description	Info
1007	Hard tamper - high temperature	HSM voltage or temperature is outside the acceptable range. HSM will stay in reset until back in range.	HT_T
1008	Hard tamper - low temperature	HSM temperature is lower than -40C.	LT_T
1009	Hard tamper - over voltage	HSM voltage is higher than the maximum allowed.	OV_T, TC3_T
1012	Hard tamper - oscillator failure	HSM tamper clock oscillator has failed	OSC_T
1013	Hard tamper - tamper configuration invalid	HSM tamper configuration lost (set to defaults) due to power loss.	FS_T
1014	Chassis opened	Chassis open switch (connector P7) has been triggered.	TC1_T
1015	HSM removed from chassis	HSM was removed from host chassis then re-inserted	CS
1016	Decommission signal triggered	Decommission button (connector P9) has been pressed.	TC2_T

Firmware

2000	Unknown alarm ID xx in firmware	Illegal alarm ID used in firmware.	
2001	High temperature warning activated	HSM temperature is above 75C (FW checks every 2 minutes). This warning will not re-appear unless temperature drops below 75C and goes back up again.	
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.	

ALM ID	Alarm Message	Description	Info
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.	
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.	

ALM ID	Alarm Message	Description	Info
2013	HSM recovered from secure transport mode	HSM in secure transport mode was recovered back to normal mode.	
2014	Auto-activation data invalid – HSM deactivated	FW checked auto-activation data validity and failed. Re-activation required.	
2015	Hard tamper - high temperature	(L3 only) HSM temperature was higher than 88C.	HT_T
2016	Hard tamper - low temperature	(L3 only) HSM temperature was lower than -40C.	LT_T
2017	Hard tamper - over voltage	(L3 only) HSM voltage was higher than the maximum allowed.	OV_T, TC3_T
2018	Hard tamper - oscillator failure	(L3 only) HSM tamper clock oscillator has failed	OSC_T
2019	Hard tamper - tamper configuration invalid	(L3 only) HSM tamper configuration lost (set to defaults) due to power loss.	FS_T
2020	Chassis opened	Chassis open switch (connector P7) has been triggered.	TC1_T
2021	HSM was removed from chassis	HSM was removed from host chassis just before this FW execution. HSM will be deactivated.	CS
2022	Decommission signal triggered	Decommission button (connector P9) has been pressed.	TC2_T
2023	HSM fan x failure	Fault detected in HSM on-board fan (fan 1 or fan 2).	
2024	Stored data integrity verify error	Integrity of an object or CSP did not verify correctly. See "Stored Data Integrity" on page 219 .	

HSM Alarm Code Samples

This section shows the details of some of the alarm event scenarios.

ALM = alarm message.

Temperature - High Warning

If HSM temperature reaches 75 degrees Celsius and then drops back below 75C the following actions occur:

- > Temperature \geq 75C
 - After 5 minutes at this temperature or higher, the Host Driver receives a 'High Temperature Warning' interrupt and issues an ALM
 - Firmware checks temperature at start-up and once per hour
 - Firmware issues ALM for high temperature warning activated
- > Temperature $<$ 75C
 - Firmware issues ALM for high temperature warning deactivated

Temperature – High Soft Tamper

When the temperature starts below 75C and reaches the high soft tamper limit of 80C and then drops back below 75C the following actions occur:

- > Temperature \geq 75C
 - After 5 minutes at this temperature or higher, the Host Driver receives a High Temperature Warning interrupt and issues an ALM
 - Firmware issues ALM for activation of high temperature warning
- > Temperature \geq 80C
 - Soft Tamper reset – card put into reset. Stays in reset until temperature lowers.
 - Host Driver receives soft tamper interrupt and issues ALM (only one when soft tamper condition starts).
- > Temperature $<$ 80C
 - Bootloader issues soft tamper ALM, then an ALM that HSM restart is required and waits for host reset.
 - User receives ALM and goes to LunaCM/Lunash to do an “hsm restart” command.
 - Bootloader starts – jumps to firmware.
 - Firmware starts – no actions taken for the soft tamper. If temperature \geq 75C, firmware re-issues ALM for activation of high temperature warning.
- > Temperature $<$ 75C
 - Firmware issues ALM for deactivation of high temperature warning.

Temperature – High Hard Tamper

When the temperature starts below 75C and reaches high hard tamper limit of 88C and then drops back below 75C the following actions occur:

- > Same as soft tamper described above up to when card is held in soft tamper reset
- > Temperature $>$ 88C
 - Hard Tamper reset – Card in hard tamper reset for 5 seconds then returns to soft tamper reset. K7 HW does erase/reset of all internal temporary memory. Tamper chip latches time and type of tamper. Host driver receives hard tamper interrupt and issues ALM.

- HSM also erases auto-activation and STM data in tamper chip
 - If decommission on tamper is enabled then key encryption data is erased in tamper chip as well
- > Temperature < 80C
- Bootloader starts – issues hard tamper ALM and logs it in FRAM Log
 - Bootloader issues ALM that HSM restart is required and waits for host reset.
 - User receives ALM and goes to LunaCM/Lunash to perform an **hsm restart** command.
 - Bootloader starts – jumps to firmware.
 - Firmware starts – saves hard tamper latches. If controlled tamper recovery is enabled, firmware locks HSM commands to a minimal subset only, and issues ALM for HSM locked. User must go to LunaCM/Lunash and perform a “tamper clear” command to get a full HSM command set. When tamper clear is issued, firmware outputs an ALM for HSM unlocked.
 - Firmware – issues deactivation and decommission (if enabled for tamper) ALMs
 - Firmware - temperature $\geq 75C$, firmware re-issues ALM for activation of high temperature warning
- > Temperature < 75C
- Firmware issues ALM for deactivation of high temperature warning
- > Temperature < 80C
- Bootloader starts – issues hard tamper ALM
 - Bootloader erases all of flash except for Boot Loader area and issues ALM for 'HSM permanently tampered'
 - Bootloader issues ALM that 'HSM restart is required' and waits for host reset.
 - User receives ALM and goes to LunaCM/Lunash to do an “hsm restart” command.
 - Bootloader starts – Only bootloader commands are available. Bootloader again issues 'ALM for HSM permanently tampered'. User can dump the FRAM Log using LUNADIAG.

Hard Tampers During Storage

When the HSM is powered off its tamper detection is powered by the on-card battery. Some hard tampers can occur when main power is not applied. The condition that caused the tamper might not be present (for example high or low temperature) when the HSM is powered back on, while others might never turn off (for example enclosure penetration, oscillator failure). If they occur while in storage, then after the HSM is powered up, the bootloader runs and logs the tamper events in FRAM Log and the serial port. Since the host K7 driver has not started yet, none of the messages from the bootloader are sent to the host, but other alarm messages are output later to notify the user.

- Bootloader waits for the host driver to be loaded
- When the host driver starts up it immediately resets the HSM causing the bootloader to run again
- Bootloader does not re-log the same tamper events
- Bootloader jumps to firmware which outputs the ALM for the tamper event. If controlled tamper recovery is enabled firmware also outputs an ALM for the 'HSM is locked and a tamper clear is required'. The user can then use LunaCM or Lunash to clear the tamper

NOTE If needed, use lunash:> [hsm supportinfo](#) to output the FRAM Log in order to determine the tamper information, or to pass on to Thales Technical Support.

Decommission with power on

If the HSM is powered on and a decommission is triggered either by the decommission switch or by a tamper (if decommission on tamper is enabled) then the HSM goes into reset for 5 seconds. The following alarm messages are output to FRAM Log, serial port, and host driver:

- > The host driver immediately receives an interrupt and outputs an 'ALM for decommission triggered'
- > After 5 seconds lapses, the bootloader starts running and also outputs an 'ALM for decommission triggered'
- > Bootloader outputs an ALM for 'HSM restart required' and then waits
- > User gets alarm notification and performs an HSM restart
- > Bootloader restarts and jumps to firmware which finishes the decommission operations and firmware outputs an ALM for 'HSM decommissioned by firmware' and an ALM for 'HSM locked' (if enabled)

Decommission with power off

If the HSM is powered off and a decommission is triggered either by the decommission switch or by a tamper (if decommission on tamper is enabled) then the decommission is latched in the tamper chip. When the HSM is powered on the following alarm messages are output:

- > Bootloader starts running and outputs an ALM for 'Decommission triggered' only to FRAM Log and serial port since the host driver is not loaded yet
- > Bootloader waits for the driver to be loaded which then forces a host reset
- > Bootloader restarts and jumps to firmware which finishes the decommission operations and firmware outputs an ALM for 'HSM decommissioned by firmware' and an ALM for 'HSM locked' (if enabled)

NOTE If needed, use lunash:> [hsm supportinfo](#) to output the FRAM Log in order to determine the tamper information, or to pass on to Thales Technical Support.

Chassis open with power on

If the HSM is powered on and the chassis open switch triggered then a cold reset is performed on the HSM which effectively removes the HSM from the PCIe bus. After about 10 seconds the HSM is released from reset and the following alarm messages are output:

- > Host Driver notices the device is no longer present on the PCIe bus and outputs an ALM for 'HSM missing from PCIe bus'
- > Bootloader starts running and outputs an ALM for 'HSM chassis opened' only to FRAM Log and serial port
- > Bootloader waits for the driver to be loaded
- > User gets notification of missing HSM and powers off then on the host system
- > Bootloader starts running and does not re-log the same tamper events
- > Bootloader waits for the host driver to be loaded
- > When the host driver starts up it immediately resets the HSM causing Bootloader to run again

- > Bootloader jumps to firmware which finishes the chassis opened operations and firmware outputs an ALM for 'HSM chassis opened' and an ALM for 'HSM locked' (if enabled).

NOTE If the chassis is still open then the HSM performs a cold reset after the tampers are cleared by firmware.

If needed, use `lunash:> hsm supportinfo` to output the FRAM Log in order to determine the tamper information, or to pass on to Thales Technical Support.

Chassis open with power off

If the HSM is powered off and the chassis open switch triggered then the chassis open is latched in the tamper chip. When the HSM is powered on the following alarm messages are output:

- > Bootloader starts running and outputs an ALM for 'HSM chassis opened' only to FRAM Log and serial port
- > Bootloader waits for the driver to be loaded which then forces a host reset
- > Bootloader starts running and does not re-log the same tamper events
- > Bootloader jumps to firmware which finishes the chassis opened operations and firmware outputs an ALM for 'HSM chassis opened' and an ALM for 'HSM locked' (if enabled)

NOTE If the chassis is still open then the HSM performs a cold reset after the tampers are cleared by firmware.

Card removal

When an HSM is powered off and removed from the chassis a card removal latch is saved in the tamper chip. When the HSM is powered on the following alarm messages are output:

- > Bootloader starts running and outputs an ALM for 'card removal' only to FRAM Log and serial port
- > Bootloader waits for the driver to be loaded which then forces a host reset
- > Bootloader starts running and does not re-log the same tamper events
- > Bootloader restarts and jumps to firmware which outputs an ALM for 'HSM was removed from the chassis' and an ALM for 'HSM locked' (if enabled)

NOTE If needed, use `lunash:> hsm supportinfo` to output the FRAM Log in order to determine the tamper information, or to pass on to Thales Technical Support.

Stored Data Integrity

The HSM performs data integrity checks at startup and during runtime.

Startup

If a check fails during startup, meaning that an object stored in flash memory was corrupted, then ALM 2024 is generated, along with additional log messages, and the HSM firmware halts:

```
k7pf0: [HSM] ALM2024: Stored data integrity verify error
... additional messages that might include "LOG (SEVERE)" and "LOG (CRITICAL)", "Fatal error",
and possibly also
k7pf0: [HSM] ALM2009: HSM halted - internal firmware error
```

What to do

1. Restart the HSM.
2. If the ALM persists, cycle the power to the HSM.
3. If the ALM persists, zeroize the HSM.
4. If the ALM persists, contact Support.

Runtime

If a check fails during runtime, meaning that an object stored in volatile memory was corrupted, then ALM 2024 is generated, along with log messages, and the HSM is unable to perform any actions that involve the corrupted object:

```
k7pf0: [HSM] ALM2024: Stored data integrity verify error  
... additional messages that might include "LOG (SEVERE)"
```

What to do

1. Try restarting the HSM.
2. If an SDI alarm occurs during startup, see the section about "Startup", above.
3. If no SDI alarm occurs during startup, but an SDI alarm occurs later, contact Support.

CHAPTER 10: HSM Updates and Upgrades

Thales releases periodic updates to the Luna Network HSM appliance software and the HSM firmware, as well as updated versions of the Luna HSM Client software. If you have recently purchased a new Luna Network HSM and your organization requires FIPS certification, you can download and install a FIPS-validated version of the HSM firmware. You can download these updates as they become available from the Thales Customer Support Portal: <https://supportportal.thalesgroup.com>.

Depending on the model of Luna Network HSM you selected at time of purchase, you may also be able to purchase upgrades to the HSM's capabilities, or increase the number of partitions you can create. These upgrades are provided through the Thales Licensing Portal (GLP).

The Customer Release Notes (CRN) contain important information on updates:

> [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 Luna Network HSM Appliance Software](#)
- > ["Updating the Luna HSM Firmware" below](#)
- > [Updating the Luna HSM Client](#)
- > ["Updating the Luna Backup HSM \(G5\) Firmware" on page 1](#)
- > ["Rolling Back the Luna HSM Firmware" on page 223](#)
- > ["Upgrading HSM Capabilities and Partition Licenses" on page 224](#)

Updating the Luna HSM Firmware

A new Luna Network HSM is delivered with the current FIPS- validated firmware installed on the HSM card, and the most recently released firmware version saved on the Luna Network HSM hard drive as an optional update. When you install an appliance software update, this optional update is replaced with the latest firmware version. If you wish to use a different HSM firmware version, you can download it from the Thales Support Portal.

To update the firmware on a Luna Backup HSM (G5), see ["Updating the Luna Backup HSM \(G5\) Firmware" on page 1](#).

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.

Updating the HSM Firmware After an Appliance Software Update

After an appliance software update, the latest firmware version is saved on the appliance and ready to install.

Required for 7.7.0 update!

CAUTION! Before updating to appliance 7.7, you *must* install **lunasa-reboot-patch-3.spkg** first - the package is bundled with the Luna Network HSM 7.7 update package, and prevents an intermittent appliance boot issue that could have serious consequences if it occurred during a firmware update procedure. See "[Network HSM Appliance BIOS Update Patch](#)" on page 1.

NOTE If the package **lunasa-reboot-patch-3.spkg** is not installed before you begin the Luna Network Appliance 7.7 update, the software update process halts with a message directing you to install the reboot fix.

NOTE If you are updating the firmware to version 7.7.x or newer, objects and partitions must be re-sized to include additional object overhead associated with the new V1 partitions - this is included in the process, no additional action from you (see [What are "pre-firmware 7.7.0", V0, and V1 partitions?](#)). This conversion can take much longer than previous firmware updates, depending on the number of objects stored on the HSM (a few minutes to several hours). Ensure that you can leave the update operation uninterrupted for this amount of time. Do not interrupt the procedure even if the operation appears to have stalled.

To update the HSM firmware after a software appliance update

1. Log in to LunaSH on the appliance as **admin**.
2. At the LunaSH prompt, login as HSM SO.
lunash:> **hsm login**
3. [Optional Step] Check that the desired firmware version is ready to install.
lunash:> **hsm firmware show**

CAUTION! If you are using STC on the HSM Admin channel, disable it by running lunash:> **hsm stc disable** before you update the HSM firmware.

4. Update the firmware to the version currently stored on the appliance.
lunash:> **hsm firmware upgrade**

Updating the HSM Firmware to a Different Version

If you are not installing the firmware update provided in the appliance software update, download your desired HSM firmware from the Thales Support Portal. You require:

- > Luna Network HSM firmware update package file (<filename>.**spkg**)
- > the secure package authentication code, provided in a text file accompanying the update package

NOTE If HSM firmware is updated to version 7.7 or newer, from a pre-7.7 version, the sizes of existing partitions are adjusted to accommodate new overhead due to new features. Firmware rollback is destructive; the HSM is zeroized and application partitions destroyed.

To update the HSM firmware to a version downloaded from the Support Portal

1. Transfer the secure package update file to the Luna Network HSM using **pscp** or **scp**.
`pscp <filepath>/<packagename>.spkg admin@<appliance_host_or_IP>:`
2. Stop all client applications to the Luna Network HSM appliance.
3. Using a serial or SSH connection, log in to the appliance as **admin**.
4. At the LunaSH prompt, login as HSM SO.
`lunash:> hsm login`
5. [Optional Step] Verify that the secure package file is present on the Luna Network HSM.
`lunash:> package listfile`
6. [Optional Step] Verify the package file, specifying the authorization code you received from Thales.
`lunash:> package verify <filename>.spkg -authcode <code_string>`
7. Install the firmware update package, specifying the authorization code you received from Thales.
`lunash:> package update <filename>.spkg -authcode <code_string>`

NOTE If you are using a service provider model, you can use the **-useevp** option to specify the OpenSSL EVP (Digital EnVeloPe library) API to validate the update package, rather than invoking the HSM. This allows you to install the update package without logging in as HSM SO (`package update`).

The package update process takes a few seconds. The firmware package is now stored on the appliance, waiting to be applied to the HSM.

8. [Optional Step] Check that the desired firmware version is ready to apply.

`lunash:> hsm firmware show`

CAUTION! If you are using STC on the HSM Admin channel, disable it by running `lunash:> hsm stc disable` before you update the HSM firmware.

9. Update the firmware to the version currently stored on the appliance.

`lunash:> hsm firmware upgrade`

Rolling Back the Luna HSM Firmware

When updating the HSM firmware, the Luna Network HSM saves the previously-installed firmware version on the HSM. If required, you can roll back to this previously-installed version. Rollback allows you to try firmware without permanently committing to the new version.

Rollback does not create a new rollback target; a single rollback target is preserved when a firmware update is performed. After a rollback operation, no further rollback is possible until the next firmware update saves the pre-update version as the new rollback target.

CAUTION! *Update any factory-fresh Network HSM to newer firmware before rolling back.* The firmware rollback feature is intended to return the firmware to the previously installed version. Attempting a firmware rollback on a new appliance received directly from the Thales factory can result in RMA (return of product), as the pre-shipment firmware is a factory-test version that does not accept your credentials.

Firmware rollback is destructive; earlier firmware versions might have older mechanisms and security vulnerabilities that a new version does not. Back up any important materials before rolling back the firmware. This procedure 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 238](#) for details.

To roll back the Luna HSM firmware to the previous version

1. Check the previous firmware version that is available on the HSM.
lunash:> [hsm firmware show](#)
2. Back up any important cryptographic objects currently stored on the HSM (see "[Backup and Restore Using a Luna Backup HSM \(G5\)](#)" on [page 1](#) or "[Backup and Restore Using a Luna Backup HSM \(G7\)](#)" on [page 1](#)).
3. At the LunaSH prompt, login as HSM SO.
lunash:> [hsm login](#)
4. Roll back the HSM firmware.
lunash:> [hsm firmware rollback](#)
5. Re-initialize the HSM and restore your partition(s) from backup.

Upgrading HSM Capabilities and Partition Licenses

The Luna Network HSM offers most customers all the capabilities they need. If your needs change, however, Thales offers upgrades on some Luna Network HSM models. You can select these upgrades when you purchase your HSM, or you can order an upgrade license anytime after purchase and apply it yourself, using the Thales Licensing Portal (GLP).

This section provides guidelines and instructions for managing your licenses:

- > "[Purchasing an Upgrade License](#)" on [page 226](#)
- > "[Activating a License on the Thales Licensing Portal](#)" on [page 228](#)
- > "[Managing Your Thales Licensing Portal Account](#)" on [page 232](#)

- > ["Applying an Upgrade License on the HSM" on page 236](#)
- > ["Upgrade Troubleshooting" on page 237](#)

Upgrade Options

Thales offers multiple options for upgrading your Luna Network HSM.

Factory Upgrades

You can select your desired upgrades at the time you purchase your HSM. Thales installs the upgrades at the factory, so that the license is activated when you receive your order. You receive an email from Thales's order entry system with the details of your upgrade license. You do not need to take any action; the upgraded HSM is ready for service.

If you plan to use the upgraded HSM as received, you do not need to create a GLP account. If you do create an account, you can use it to transfer upgrade licenses from one Luna Network HSM to another as desired.

Field Upgrades

If you have one of the approved Luna Network HSM models, you can order upgrades at any time. After placing an upgrade order, you receive an email from Thales's order entry system with instructions on how to obtain your license through the GLP. Attached to the email is an entitlement certificate with an entitlement identifier. You need this number when you create your GLP account.

Upgradable HSM Models

Luna Network HSM comes in three models for your convenience. If you have a Luna Network HSM model 750 or 790, you can purchase upgrade licenses and apply them yourself. At this time, the 700 model does not accept upgrades.

Upgrade Types

Thales currently offers three types of HSM upgrade:

- > partition upgrade packs (of 5) to increase the maximum number of application partitions
- > Korea-specific cryptographic algorithms
- > Functionality Modules (allowed on FM-ready HSMs only)

License Revocation

You may purchase and apply upgrades to any upgradable Luna Network HSM appliance you own. If you have already applied an upgrade to an HSM and wish to remove it and apply it to a different HSM, you can revoke the license from one HSM so that it may be activated on the other. Contact Thales to revoke an upgrade license from an HSM.

Return Material Authorization

In the unlikely event that you must return an HSM to Thales, the unit that you receive in exchange or receive back will have your purchased upgrades installed, and appearing on the GLP as activated. Thales's customer care team will revoke upgrades in GLP on your behalf so that the appliance sent to you has the correct upgrades. If you receive a replacement appliance, you will need to refer to the new serial number when managing your licenses.

Purchasing an Upgrade License

To place an order for an upgrade, contact your Thales sales representative. If you are purchasing a new Luna Network HSM, you can opt for factory-installed upgrades or field upgrades that you can install yourself. Thales offers the following types of upgrade licenses:

- > partition upgrade packs (of 5) to increase the maximum number of application partitions
- > Korea-specific cryptographic algorithms
- > Functionality Modules (allowed on FM-ready HSMs only)

For example, a Luna Network HSM S790 appliance comes with the base maximum number of 10 partitions. To upgrade the maximum to allow 30 partitions, you must order four (4) partition upgrades. After you apply this full entitlement to your HSM, you have the desired maximum 30 partitions. The following table summarizes the upgrade options for different models.

HSM Model	Factory-Installed Partitions	Maximum Number of Partitions	Maximum Number of 5-Pack Upgrades
*700	5	5	N/A
*750	5	20	3
*790	10	100	18

After you place your order for an upgrade and a Thales Customer Care representative has entered the order, you receive an email with detailed instructions on how to obtain and apply your upgrade.

Entitlement Certificate

Attached to the upgrade email is an entitlement certificate. On this certificate is an entitlement identifier that you need to activate your upgrade. Here is an example of an entitlement certificate and where to find the EID.

SafeNet Luna Network HSM License Purchase

Thank you for your recent SafeNet Luna Network HSM order. Below please find your Entitlement ID as described in the user guide. Please keep this ID for your records.

We thank you for your business.

Entitlement ID:	c102f5dc-8179-4bec-9373-ffb3e633abe5		
Sold To Customer:	Customer Name		
End Customer:			
Customer Purchase Order:	Demo	Gemalto/SafeNet Sales Order:	11074136
Item Number:	908-000395-001	Quantity:	4
Description:	PARTITION 5-PACK,LUNA HSM 7+ (FIELD UPGRADE)		
Order Book Date:	05/31/2017		

Next, see ["Activating a License on the Thales Licensing Portal"](#) on the next page.

Activating a License on the Thales Licensing Portal

After receiving the entitlement confirmation email, visit the Thales Licensing Portal (GLP) and create an account to activate your upgrade license. You need the Entitlement ID from the confirmation email to complete this procedure.

To activate a license

1. Navigate to the GLP welcome page in your browser, enter the Entitlement ID from the email you received, and click **Activate**.

<https://safenetbelcamp.prod.sentinelcloud.com/ecp/>

Welcome to the Gemalto Licensing Portal (1.46.18.0731) English

gemalto

Enter Entitlement ID

Activate

OR

Email Address

Password

[Forgot your password?](#)

Sign in

gemalto

© 2006-2018 Gemalto [Privacy Policy](#) [Terms & Conditions](#) [Contact Gemalto](#) [gemalto.com](#)

2. If you do not already have an account, complete the mandatory user registration process by entering your email address and selecting a password and security questions, and click **Next**.

If you already have an account and are activating a new entitlement, click **Login** and enter your email address and password.

gemalto[®] English

Licensing Portal Asterisk (*) indicates a required field Aug 14, 2018 2:36:22 PM

Please take some time to register with us. **Already registered? Login**

Enter Your Account Information

Email Address* Password*

Confirm Email Address* Confirm Password*

Set Your Security Preferences

Security Question 1* Security Question 2*

Security Question 1 Answer* Security Question 2 Answer*

Enter Your Personal Information

Name* Company Name United States

Cancel Next

© 2006-2018 Gemalto Privacy Policy Terms & Conditions Contact Gemalto gemalto.com

NOTE The GLP is arranged as a company account. Accounts with email addresses associated with a company are able to see all of that company's purchases. The association between a license and your company is created by registration and login using the Entitlement ID.

Multiple email addresses can be associated with your company. There is no limit.

If a registered GLP user leaves the company, contact Thales Customer Support to make the adjustment.

3. On the **License Activation** screen, enter the number of licenses from the entitlement that you wish to activate, and click **Next**.

gemalto English [Home](#) / Welcome ██████████

License Activation Aug 14, 2018 12:28:59 PM

Step 1 - Select License Step 2 - Select HSM Step 3 - Finish

Company: Luna Team Order #: Luna ECP screenshot Order Date: 08/02/2018
Entitlement ID: 88065104-fbd1-458d-b9e8-██████████

Number	Product Name	Activated	Available	Quantity To Activate	
1	PARTITION 5-PACK, LUNA HSM7+ (FIELD UPGRADE) 3.0 Part# 908-000395-001 Expiration: None	1	14	3	<input checked="" type="checkbox"/>

Cancel Next

© 2006- 2018 Gemalto Privacy Policy Terms & Conditions Contact Gemalto gemalto.com

4. Specify the HSM that will use this license by clicking **Enter New HSM SN** and entering the serial number. If you previously entered the HSM's serial number, click **Use Existing HSM SN** and select it from the drop-down menu. Click **Next**.

gemalto English [Home](#) / Welcome ██████████

License Activation Aug 14, 2018 12:33:55 PM

Step 1 - Select License Step 2 - Select HSM Step 3 - Finish

Company: Luna Team Order #: Luna ECP screenshot Order Date: 08/02/2018
Entitlement ID: 88065104-fbd1-458d-b9e8-██████████

Product	Apply to
PARTITION 5-PACK, LUNA HSM7+ (FIELD UPGRADE) 3.0 Part# 908-000395-001 Quantity To Activate : 3	<input checked="" type="radio"/> Enter New HSM SN <input type="radio"/> Use Existing HSM SN HSM SN: <input type="text" value="532989"/>

Enter comments

Cancel Previous Next

© 2006- 2018 Gemalto Privacy Policy Terms & Conditions Contact Gemalto gemalto.com

5. Your activation is now complete. GLP generates a license string that the Luna Network HSM will use to validate an upgrade and apply it. Click **Download License File** to download a ZIP file containing this string. If you do not wish to install the upgrade at this time, click **Done**.

The screenshot shows the Gemalto License Activation interface. At the top, there is a navigation bar with the Gemalto logo, a language dropdown set to 'English', and a user profile section with 'Home / Welcome' and a user icon. Below this, the page title is 'License Activation' and the date/time is 'Aug 14, 2018 12:34:17 PM'. A progress bar shows three steps: 'Step 1 - Select License', 'Step 2 - Select HSM', and 'Step 3 - Finish'. Below the progress bar, a summary box contains: 'Company: Luna Team', 'Order #: Luna ECP screenshot', 'Order Date: 08/02/2018', and 'Entitlement ID: 88065104-fbd1-458d-b9e8'. A large green banner reads 'Activation Complete'. Below this is a table with two columns: 'Product Name' and 'Activated'. The table contains one row: 'PARTITION 5-PACK, LUNA HSM7+ (FIELD UPGRADE) 3.0' with 'Activated' value '3'. Below the table, there are two buttons: 'Download License File' (highlighted with a red arrow) and 'Done'. The footer contains copyright information '© 2006-2018 Gemalto' and links for 'Privacy Policy', 'Terms & Conditions', 'Contact Gemalto', and 'gemalto.com'.

6. Extract the license string file (default filename: **lservrc**) from the ZIP file. Thales recommends that you rename this file to something more distinctive, especially if you have multiple upgrades to manage. If you are managing upgrades for multiple HSMs, it is a good idea to include the HSM serial number, as in the example below.



The screenshot shows a Notepad window titled '532989_15_partitions - Notepad'. The text content is as follows:

```

16 LUNA_PARTITIONS_5PACK 1.0 LONG NORMAL STANDALONE ADD 3_KEYS INFINITE_KEYS 14 AUG 2018 16
37 NEVER NiL SLM_CODE CL_ND_LCK NiL *1RAJFAJ86KCKCPL0400 NiL NiL NiL INFINITE_MINS NiL 0
:GE9X00:sVQWvrSsHei0favqw55tUmUqmzrSZWWG10fzZ5WFY:A0IMaUI,28gfKGLuR3473OMxLhFHmdgmqgAr3WRTe
Ln4EH8JC0zKd7viMT3vhzNpQtgDJ0VbK3046,Acf1#

```

Next, see ["Applying an Upgrade License on the HSM"](#) on page 236.

For more information about navigating the GLP, see ["Managing Your Thales Licensing Portal Account"](#) on the next page.

Managing Your Thales Licensing Portal Account

Once you have created your account, you can return to it at any time to manage and get information about your purchased licenses. The **My Assets** page is the home for this information. From this page, you can find the following information:

- > "View Licenses by Product" below
- > "Activate New Entitlements" below
- > "Products" on the next page
- > "Orders" on page 234
- > "Activations" on page 234
- > "Devices" on page 235

View Licenses by Product

To sort license information by product, choose the Thales product from the drop-down menu at the top left:

English Home / Welcome [User Name]

Aug 14, 2018 5:27:51 PM

Instruction: The following list displays all products that are available to your company. To view the list of orders for a given product, click the **View** button for that product. To activate a given order, click the associated **Activate** button from the list of orders.

Product Name	Activated	Available	View
PARTITION 5-PACK, LUNA HSM7+ (FIELD UPGRADE) 3.0 Part# 908-000395-001	7	8	View

Orders (1)

© 2006-2018 Gemalto Privacy Policy Terms & Conditions Contact Gemalto gemalto.com

Activate New Entitlements

After you select the product type from the drop-down menu, you can activate any new licenses by entering the Entitlement ID in the upper right corner.

The screenshot shows the Gemalto Licensing Portal interface. At the top, there is a navigation bar with the Gemalto logo, a language dropdown set to 'English', and a home link. Below this is a search bar with 'Luna' selected. A red arrow points to a search field labeled 'Entitlement ID: Enter' with a 'GO' button. Below the search bar, the page title is 'Licensing Portal' and the date is 'Aug 14, 2018 5:35:10 PM'. The main content area is titled 'My Assets' and includes a 'Products (1)' section. An instruction states: 'The following list displays all products that are available to your company. To view the list of orders for a given product, click the View button for that product. To activate a given order, click the associated Activate button from the list of orders.' Below this is a table with columns: Product Name, Activated, Available, and View. The table contains one row: 'PARTITION 5-PACK, LUNA HSM7+ (FIELD UPGRADE) 3.0' with Part# 908-000395-001, 7 activated, and 8 available. Below the table are sections for 'Orders (1)' and 'Activations (3)'. The footer contains copyright information and links for Privacy Policy, Terms & Conditions, and Contact Gemalto.

Products

To see the licenses you have purchased, expand the **Products** view. This page is a summary of upgrades, and shows the quantity available and how many are activated. Click **View** next to a product to see details.

This screenshot is identical to the one above, showing the Gemalto Licensing Portal. The 'Products' section is expanded, showing the table with the product 'PARTITION 5-PACK, LUNA HSM7+ (FIELD UPGRADE) 3.0'. The 'View' button is highlighted in orange. The rest of the interface, including the search bar, navigation, and footer, remains the same.

Orders

The **Orders** view provides details of each order you purchased. Click **Activate** next to an order to activate available licenses.

Licensing Portal Aug 14, 2018 5:43:15 PM

My Assets ⓘ

⊕ Products (1)

☐ Orders (1)

Instruction : The following list displays all orders for your company. Click **Activate** for an order to initiate an activation.

Orders Export CSV

Order Date	Order Number	PO Number	Product Name	Entitlement ID	Activated	Available	Activate
8/2/2018	Luna ECP screenshot	Luna ECP screenshot	PARTITION 5-PACK, LUNA HSM7+ (FIELD UPGRADE) 3.0 Part# 908-000395-001 Expiration:None	88065104-fbd1-458d-b9e8-██████████	7	8	Activate

⊕ Activations (3)

© 2006- 2018 Gemalto Privacy Policy Terms & Conditions Contact Gemalto gemalto.com

Activations

The **Activations** view lists the entitlements you have previously activated. Click **Download** next to an activation to download the corresponding license string in a ZIP file.

gemalto English Home / Welcome [User]

Activations (3)

Instruction :The following list displays all activations for your company.

Activations		Export CSV					
Activation Date	Activation ID	Entitlement ID	HSM Serial Number	Locking Code	Product Activated	License File	Activated
8/3/2018	a464cca0-714f-4492-a626- [Redacted]	88065104-fbd1-458d-b9e8- [Redacted]	180802	*1DGG70 [Redacted]	PARTITION 5-PACK, LUNA HSM7+ (FIELD UPGRADE) 3.0 Part#908-000395-001 Expiration: None	Download	1
8/14/2018	9fb2eae0-4d35-4ca3-a260- [Redacted]	88065104-fbd1-458d-b9e8- [Redacted]	532989	*19CF92 [Redacted]	PARTITION 5-PACK, LUNA HSM7+ (FIELD UPGRADE) 3.0 Part#908-000395-001 Expiration: None	Download	3
8/14/2018	1e8342a5-e5d4-41a6-b6c7- [Redacted]	88065104-fbd1-458d-b9e8- [Redacted]	532018	*1RAJFA [Redacted]	PARTITION 5-PACK, LUNA HSM7+ (FIELD UPGRADE) 3.0 Part#908-000395-001 Expiration: None	Download	3

Devices (3)

© 2006-2018 Gemalto Privacy Policy Terms & Conditions Contact Gemalto gemalto.com

Devices

The **Devices** view shows all the HSMs you have registered on the portal. Click **View** next to a specific device to see more details (what features were activated and when, and the corresponding license string in a ZIP file).

gemalto English Home / Welcome [User]

Products (1)

Orders (1)

Activations (3)

Devices (3)

Instruction : The following list displays all devices that have an associated activation for your company.

Devices		Export CSV		
HSM Serial Number	Locking Code	Product Activated	Activated	View
[Redacted]	*1DGG70 [Redacted]	PARTITION 5-PACK, LUNA HSM7+ (FIELD UPGRADE) Part#908-000395-001 Expiration:None	1	View
[Redacted]	*1RAJFA [Redacted]	PARTITION 5-PACK, LUNA HSM7+ (FIELD UPGRADE) Part#908-000395-001 Expiration:None	3	View
532989	*19CF92 [Redacted]	PARTITION 5-PACK, LUNA HSM7+ (FIELD UPGRADE) Part#908-000395-001 Expiration:None	3	View

© 2006-2018 Gemalto Privacy Policy Terms & Conditions Contact Gemalto gemalto.com

Applying an Upgrade License on the HSM

The license string file you downloaded from the GLP (see ["Activating a License on the Thales Licensing Portal" on page 228](#)) is used to apply your HSM upgrade. The HSM Security Officer must complete this procedure.

Prerequisites

- > Ensure that you have the license string file that is registered to the correct HSM serial number.
- > If you are installing partition upgrades, ensure that you have space available on the HSM. By default, partitions are created at a size that will utilize the entire HSM space based on the number of partition licenses at the time. If your existing partitions use all available space on the HSM, the new license application may fail with an error (LUNA_RET_RM_CONFIG_CHANGE_FAILS_DEPENDENCIES). To prevent this, reclaim space on the HSM by resizing the existing partitions (see ["Customizing Partition Sizes" on page 164](#)) before you apply the upgrade license.

To apply an upgrade license on the HSM

1. Open a command prompt, navigate to the directory containing the license string file, and use **pscp/scp** to transfer it to an **admin**-level account on the Luna Network HSM appliance.

```
pscp [options] <license_file> admin@<host/IP>:
```

2. Connect to the appliance via SSH or a serial connection, and log in to LunaSH using the **admin**-level account that received the file (see [Logging In to LunaSH](#)).
3. Log in as HSM SO (see ["Logging In as HSM Security Officer" on page 148](#)).

```
lunash:> hsm login
```

4. [Optional] Confirm that the HSM fingerprint matches the one in the license string. If this string does not match, the upgrade will not be applied.

```
lunash:> sysconf fingerprint license
```

```
Fingerprint for Use With Entitlement Management System
```

```
-----
HSM serial #532018 : *1RAJFAJ86KCKCPL
```

```
License string:
```

```
16 LUNA_PARTITIONS_5PACK 1.0 LONG NORMAL STANDALONE ADD 3_KEYS INFINITE_KEYS 14 AUG 2018 16 37
NEVER NiL SLM_CODE CL_ND_LCK NiL *1RAJFAJ86KCKCPL0400 NiL NiL NiL INFINITE_MINS NiL 0
:GE9X00:sVQWvrSsHei0favqw55tUmUqmzrSZWWG10fzZ5WFY:A0IMaUI,28gfKGLuR3473OMxLhFHmdgmqqAr3WRTEln4E
H8JC0zKd7viMT3vhzNpQtgDJ0VbK3046,Acf1#
```

5. Apply the upgrade to the HSM.

```
lunash:> sysconf license apply -filename <license_file>
```

6. [Optional] Verify that the license has been applied.

```
lunash:> sysconf license list
```

NOTE The **QUANTITY** column represents the total number of additional partitions associated with a specific license. This column does not apply to other types of license upgrades.

Upgrade Troubleshooting

If you are unable to apply an upgrade license from the Thales Licensing Portal (GLP), the table below provides descriptions of possible failure messages (lunash:> [sysconf license apply](#)).

Message	Description
Cannot find <filename>	The file that you specified containing the license string cannot be found on the HSM appliance. Use lunash:> my file list to see what files are available.
Cannot find lserverc	You should not encounter this message. If you do, please contact Thales Technical Support for assistance.
Invalid licensed feature	The license string is corrupted in the feature attribute. Confirm that you saved the license string without modification after activating the upgrade in the GLP.
Invalid licensed feature version	The license string is corrupted in the feature version attribute. Confirm that you saved the license string without modification after activating the upgrade in the GLP.
Invalid licensed HSM serial number	The license string is for an HSM with a different serial number. Ensure that you transferred the correct license string file to the appliance.
<feature> not licensed for this appliance	The license string is for an HSM with a different serial number. Ensure that you transferred the correct license string file to the appliance.
License is already applied	The license string matches an entitlement already applied on this HSM appliance.
LUNA_RET_HSM_TAMPERED	The HSM is in a tampered state and must be cleared of the tampered state before the upgrade can be applied.
Update Result : 12 (Error detecting HSM)	The HSM Security Officer is not logged in.
License is unknown/not available (feature)	The HSM appliance software needs to be updated to support a newer feature.
Upgrades not available for this model of HSM	Only 750 and 790 models of HSM support upgrades.
Upgrade to <#> partitions not available for this model of HSM	Applying the upgrade would exceed the upper limit for the maximum number of partitions on the HSM.
Unable to determine model of HSM	You should not encounter this message. If you do, please contact Thales Technical Support for assistance.

CHAPTER 11: Functionality Modules

Functionality Modules (FMs) consist of your own custom-developed code, loaded and operating within the logical and physical security of a Luna Network HSM as part of the HSM firmware. FMs allow you to customize your Luna Network 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 Luna Network 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, appliance software 7.4.0, and client 7.4. See [Version Dependencies by Feature](#) for more information.

This feature has hardware dependencies described in "[Preparing the Luna Network HSM to Use FMs](#)" on page 242.

This chapter contains the following sections:

- > ["FM Deployment Constraints" below](#)
- > ["Preparing the Luna Network HSM to Use FMs" on page 242](#)
- > ["Building and Signing an FM" on page 244](#)
- > ["Loading an FM Into the HSM Firmware" on page 248](#)
- > ["Deleting an FM From the HSM Firmware" on page 249](#)
- > ["Recovering the HSM After FM Failure" on page 250](#)

FM Deployment Constraints

This section describes important considerations and constraints associated with deploying your Functionality Modules (FMs). Your Luna Network HSM must meet all the criteria described in "[Preparing the Luna Network HSM to Use FMs](#)" on page 242.

Introducing FMs into your Luna Network HSM deployment will change the functionality of certain HSM features. Please take the following constraints into consideration before using FMs:

- > ["FMs and FIPS Mode" on the next page](#)

- > ["FMs and High-Availability \(HA\)" below](#)
- > ["FMs and Backup/Restore/Cloning" on the next page](#)
- > ["FMs and Secure Trusted Channel \(STC\)" on the next page](#)
- > ["FMs and Appliance Re-imaging" on the next page](#)
- > ["FMs and HSM Firmware Rollback" on page 241](#)
- > ["FM Configuration and Remote PED" on page 241](#)
- > ["FM-Enabled HSM Cannot be Verified With CMU" on page 241](#)
- > ["Key Attributes" on page 241](#)
- > ["No EDDSA or EC_MONTGOMERY Private Keys with C_CreateObject" on page 241](#)
- > ["FM Sample Applications Dependent on General Cryptoki Samples" on page 241](#)
- > ["Memory for FMs" on page 242](#)

CAUTION! Enabling FMs (**HSM policy 50**) introduces changes to Luna HSM functionality, some of which are permanent; they cannot be removed by disabling the policy. FM-enabled status is **not** reversible by Factory Reset.

If you are using Crypto Command Center, ensure that your CCC version supports FM-enabled HSMs before you enable **HSM policy 50**. Refer to the CCC CRN for details.

FMs and FIPS Mode

FMs change the abilities of the HSM firmware, adding new cryptographic algorithms or other functions. Since the new functionality is not certified by NIST, be sure that your FM does not preclude FIPS compliance.

To be certain that your organization is meeting FIPS requirements, ensure that you are using a FIPS-certified version of the Luna HSM firmware, and that your Luna Network HSM has the following HSM policy settings:

- > **HSM policy 12: Allow non-FIPS algorithms: 0**
- > **HSM policy 50: Allow Functionality Modules: 0**

If FIPS 140 compliance is not a requirement of your use-case, then enabling FMs does not present an issue for you. Enabling the Functionality Modules Policy (setting Policy 50 to "1") is not reversible. For more information about HSM policies, see ["HSM Capabilities and Policies" on page 150](#).

FMs and High-Availability (HA)

FM-specific functions must specify the exact HSM that will handle the operations. Therefore, the Luna HSM Client's HA implementation currently cannot accommodate FM functionality. If you want your FM-specific operations to be load-balanced across multiple HSMs, you must program this functionality into your applications yourself.

HA will still work with standard Luna operations.

For HA to function with Functionality Modules, all HSMs with application partitions in the HA group must have the same algorithms and functionality available. If one member partition does not have a required algorithm available in HSM firmware, cryptographic objects using that algorithm cannot be cloned to that partition, and this will disrupt HA functions.

Therefore, all HSMs containing HA group members must have FMs enabled (as described in "[Preparing the Luna Network HSM to Use FMs](#)" on page 242), and they must all have the same FM(s) loaded. HA login requires two FM-enabled HSMs.

For more information about HA, see [High-Availability Groups](#).

FMs and Backup/Restore/Cloning

To back up and restore objects on FM-enabled partitions, you require the following minimum Luna Backup HSM firmware versions:

- > Luna Backup HSM (G7) requires minimum firmware version 7.7.1
- > Luna Backup HSM (G5) requires minimum firmware version 6.28.0

As a general rule, cryptographic objects can be cloned from a partition with less-secure settings to one with identical or more secure settings. Therefore, it is not possible to clone objects from a standard partition to an FM-enabled partition, unless the FM-enabled partition uses a stronger cloning protocol. This rule applies to backup/restore operations as well. For example:

- > cloning from a pre-7.7.0 standard partition to a V0 or V1 FM partition is allowed
- > cloning from a V0 standard partition to a V1 FM partition is allowed

This is to ensure that you can migrate objects to a Luna HSM with firmware 7.7.0 or newer, whether you have enabled FMs or not. These are considered migration scenarios only, and Thales does not recommend them for production environments.

To back up keys stored in the SMFS, your application must provide all the functions to back up and restore these keys.

FMs and Secure Trusted Channel (STC)

To use Functionality Modules (FMs) with STC client connections, you require Luna HSM firmware 7.7.0 or newer. To use FMs with earlier firmware versions, you must use NTLS connections.

FMs and Appliance Re-imaging

The FM-ready configuration required to make FMs work makes it impossible to re-image the appliance to the baseline version. This restriction comes into effect once **HSM policy 50: Enable Functionality Modules** is set to **1**, and it continues to apply even if the policy is set back to **0**. Attempting to re-image the appliance software once **HSM policy 50** has been enabled will return the following:

```
lunash:>sysconf reimage start
```

```
The HSM Administrator is logged in. Proceeding...
```

```
The HSM Functionality Module policy (policy 50) has
previously been enabled.
```

```
Enabling this policy at any time causes the Appliance Re-image feature
to become unavailable.
```

```
ERROR, Not all required pre-conditions to re-image the appliance were satisfied
```

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


FMs and HSM Firmware Rollback

Enabling **HSM Policy 50** permanently disables the ability to roll back the HSM firmware to a version lower than 7.4.0. Attempting to roll back the firmware once **HSM policy 50** has been enabled will return the following error:

```
ERROR, failed to roll back HSM F/W!!!
```

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

FM Configuration and Remote PED

Various FM functions require HSM resets (for example, creating a partition or enabling an FM).

If you are configuring FMs while authenticating with Remote PED, the Remote PED connection is broken with each reset. LunaCM continues to show an active Remote PED connection until you restart LunaCM. You must close that apparent connection with `lunash:>hsm ped disconnect` and then open it again with `lunash:>hsm ped connect` before you can resume remote configuration.

This might be required several times during Luna Network HSM 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 recommends that first time configuration of FM's be done locally, to minimize the issues mentioned above.

FM-Enabled HSM Cannot be Verified With CMU

The FM-enabled Luna Network HSM does not currently support confirming the HSM's authenticity using `cmu verifyhsm`, as described in [Verifying the HSM's Authenticity](#), or retrieving and confirming a Public Key Confirmation from the HSM using `cmu getpkc` and `cmu verifypkc`.

Key Attributes

On an HSM with FMs enabled, keys that are derived or generated have the "always-sensitive" and the "never-extractable" attributes set to "false".

No EDDSA or EC_MONTGOMERY Private Keys with C_CreateObject

This release of the Luna Network HSM firmware does not allow FMs to use `C_CreateObject` to create EDDSA or `EC_MONTGOMERY` private keys. Use `C_GenerateKeyPair` to create these types of key.

FM Sample Applications Dependent on General Cryptoki Samples

When you install the FM SDK, the installation script ensures that the general Luna (PKCS) SDK and samples are also installed (first). This satisfies source dependencies for the FM samples. If you later delete or remove the Luna SDK, you might break those dependencies, and the FM samples will not build. You can manually correct this by performing a manual `rpm -i` of the `cksample` package.

Memory for FMs

Multiple FMs can be loaded into the FM space of the HSM, with a total memory limit of:

- > 8 megabytes for FMs
- > 4 megabytes of SMFS

Unused FMs can be deleted, to free some memory space.

Preparing the Luna Network HSM to Use FMs

This section provides information on how to prepare your Luna Network 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 Appliance Software and 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 238](#) for details before enabling.

If you are using Crypto Command Center, ensure that your CCC version supports FM-enabled HSMs before you enable **HSM policy 50**. Refer to the CCC CRN for details.

Step 1: Ensure You Have FM-Ready Hardware

The FM feature requires a specific Luna Network HSM hardware configuration that must be created by Thales at the factory. Luna Network HSMs that have this configuration are "FM-ready". If your Luna Network HSM is not FM-ready, contact your Thales representative or Thales Customer Support for further guidance.

Determining Whether the HSM is FM-Ready

Starting with release 7.4, all Luna Network 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 appliance label:

Product Part #:
908-XXXXXX-003-A
Product Serial #:
XXXXXXXX



If the last 3-digit section of the Product Part # is **003** or higher, your HSM is FM-ready. If **002** or lower, contact your Thales representative or Thales Customer Support for guidance on how to obtain FM-ready hardware.

NOTE Exception: If your Luna Network HSM includes 10GB optical Ethernet ports, your HSM is FM-Ready, even though the Product Part # ends in **001**.

Step 2: Update to Luna Appliance Software and HSM Firmware 7.4.0 or Higher

To use FMs, you require appliance software 7.4 or higher, and HSM firmware version 7.4.0 or higher. You can download the latest software/firmware packages from the Thales Support Portal (see ["Updating the Luna Network HSM Appliance Software" on page 1](#) and ["Updating the Luna HSM Firmware" on page 221](#)).

When you have completed the upgrade, you can check the output from `lunash:>hsm show` to ensure that the HSM is FM-ready:

```
Functionality Module HW:           FM Ready
=====
```

Step 3: Purchase and Apply the FM Capability License

To use FMs, contact your Thales sales representative to purchase the FM capability license. You can validate the license on the Thales Licensing Portal (GLP) and install it with LunaSH. Refer to ["Upgrading HSM Capabilities and Partition Licenses" on page 224](#) for the procedure.

When you have activated your license on the HSM, you can use `lunash:>hsm displaylicenses` to check that it is installed:

```
HSM CAPABILITY LICENSES
License ID      Description
=====
621000068-000  K7 Base
621010185-003  Key backup via cloning protocol
621000046-002  Maximum 100 partitions
621000134-002  Enable 32 megabytes of object storage
621000135-002  Enable allow decommissioning
621000021-002  Maximum performance
621000138-001  Controlled tamper recovery
621000154-001  Enable decommission on tamper with policy off
621000074-001  Enable Functionality Modules
```

Step 4: Apply HSM Policy Settings

Applying the FM capability license allows you to set 4 new HSM policies that affect FMs on the Luna Network HSM (see ["HSM Capabilities and Policies" on page 150](#)). Use `lunash:>hsm showpolicies` to list HSM policies.

Description	Value	Code	Destructive
=====	=====	=====	=====
Allow Functionality Modules	Off	50	Yes
Allow SMFS Auto Activation	Off	51	Yes
Restrict FM Privilege Level	Off	52	Yes
Encrypt keys passing from FM to HSM	Off	53	Yes

HSM Policy 50: Allow Functionality Modules

With this policy enabled, Functionality Modules may be loaded to the HSM, permitting custom cryptographic operations. Allows use of the `ctfm` utility and FM-related commands, and the use of Functionality Modules in general with this HSM.

The HSM SO must set HSM policy 50 to 1 (ON) to use FMs on the Luna Network HSM. 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 238](#) for details before enabling.

If you are using Crypto Command Center, ensure that your CCC version supports FM-enabled HSMs before you enable **HSM policy 50**. Refer to the CCC CRN for details.

HSM Policy 51: Allow SMFS Auto Activation

With this policy enabled, the Secure Memory File System (SMFS) is automatically activated on startup, providing a secure, tamper-enabled location in the HSM memory where Functionality Modules can load keys and parameters. Auto-activation for SMFS, like auto-activation for 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 recommends setting HSM policy 51 to 1 (ON) to avoid having to manually re-activate the SMFS if you need to reboot the HSM. Changing this policy destroys all existing application partitions.

HSM Policy 52: Restrict FM Privilege Level

With this policy enabled, FM privilege is restricted. By default, FM privilege permits FMs to see the sensitive key attributes (including key values) of cryptographic objects on application partitions. This privilege is necessary for most FMs, so that the Crypto Officer (CO) and Crypto User (CU) roles can use partition objects with the FM. However, some FMs might not require this privilege and it can be restricted to satisfy some certification requirements (such as Common Criteria).

FM privilege permits FMs to see the sensitive key attributes (including key values) of cryptographic objects on application partitions. This privilege is necessary for most FMs, so that the Crypto Officer (CO) and Crypto User (CU) roles can use partition objects with the FM. However, some FMs might not require this privilege and it can be restricted to satisfy some certification requirements (such as Common Criteria).

Unless you require CC certification, Thales does not recommend changing this policy from its default setting (OFF). Changing this policy destroys all existing application partitions.

HSM Policy 53: Encrypt Keys Passing from FM to HSM

With this policy enabled, keys created by an FM are encrypted before crossing from the FM to the Functionality Module Crypto Engine interface (FMCE). This internal encryption may be required to satisfy some certification requirements (such as Common Criteria).

Unless you require CC certification, Thales does not recommend changing this policy from its default setting (OFF). Changing this policy (OFF-to-ON or ON-to-OFF) will destroy all existing application partitions.

Building and Signing an FM

Once you have written your FM code, you must build the binary and then sign it using a private key on the HSM. A self-signed certificate is used to confirm the authenticity of the FM. This procedure will allow you to install the FM into your HSM firmware. Luna FMs must be built on a Linux system, so you can use the native **make**

command. The following example uses the **skeleton** sample FM, included with the Luna FM SDK.

The FM binary must be signed with a private key, and loaded into the HSM firmware with a self-signed certificate from the same keypair to verify its authenticity. You can use **mkfm**, included with the Luna HSM Client FM Tools, to sign your FM using a Luna application partition or your own Cryptoki signing station. The procedure below will show you how to use **mkfm**.

Prerequisites

- > The FM binary must be built on a Linux client. You can use either a Windows or Linux client to perform the signing operation.
- > The FM Tools option in the Luna HSM Client software must be installed on the client or signing station.
- > The client must have access to an application partition on the Luna Network HSM. The Crypto Officer can create the keypair and certificate required.
- > **mkfm** requires access to a Cryptoki token (such as a Luna application partition) capable of using the CKM_SHA512_RSA_PKCS mechanism.

To build an FM binary

1. On your Linux client, navigate to the directory containing your FM code (<filename>.c). By default, FM samples provided with the Luna FM SDK are installed in **/usr/safenet/lunafmsdk/samples/**.

```
[user@myLunaClient ~]# cd /usr/safenet/lunafmsdk/samples/skeleton/fm/
[user@myLunaClient fm]# ls
hdr.c  makefile  skeleton.c
```

2. Use the Linux **make** command to build the FM binary.

make

The **make** process creates two new sub-directories, **bin-ppc** and **obj-ppc**. Your FM binary is located in **bin-ppc**, named <filename>.bin.

```
[user@myLunaClient ~]# cd /usr/safenet/lunafmsdk/samples/skeleton/fm/bin-ppc/
[user@myLunaClient bin-ppc]# ls
skeleton.bin
```

To create an FM signing certificate on an application partition

1. If this is the first FM you are signing, you must first create a keypair and self-signed certificate on the application partition. If you already have a certificate for FM signing stored on the appliance, skip this procedure.

NOTE A certificate used to sign an FM must have attribute CKA_PRIVATE set as true. If an existing certificate has Private=0, you can use the CMU tool to export that cert, then re-import it while setting -private=1. Or, if the partition retains the FM signing keypair, you can run the "cmu selfsigncertificate" command again to re-create the certificate, this time setting -private=1 explicitly.

To sign an FM with **mkfm**, you must use an RSA private key at least 2048 bits long. The Crypto Officer can use the **cmu** utility to create the keypair. You will be prompted for the CO credential.

NOTE Always provide unique labels for your keys. If multiple private keys exist with the same label, **mkfm** will use the newest key (with the greatest object handle value).

"cmu generatekeypair" 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) : Thales
Enter Subject Organization Unit Name (OU) :
```

```

Enter Subject Common Name (CN) : FMsign
Enter EMAIL Address (E) :
Enter validity start date
  Year   : 2018
  Month  : 12
  Day    : 05
Enter validity end date
  Year   : 2019
  Month  : 12
  Day    : 31
Using "CKM_SHA256_RSA_PKCS" Mechanism

```

4. Export the certificate to the client file system, specifying the desired filename with **.cert** extension.

cmu export -slot <slot_number> -label <cert_label> -outputfile=<filename.cert>

```

[user@myLunaClient bin]# ./cmu export -slot 3 -label FMsign -outputfile=FMsign.cert
Certificate Management Utility (64-bit) v7.4.0-208. Copyright (c) 2018 SafeNet. All rights
reserved.

```

Please enter password for token in slot 3 : *****

To sign an FM

1. Use the **mkfm** utility included with the Luna HSM Client FM Tools to sign the FM, specifying the unsigned FM binary, the desired FM filepath/filename (with **.fm** extension), the slot number/name of the partition/token where the keypair is stored, and the private key label.

If you are specifying a slot number, include **-k SLOTID=<#>** instead of the partition name. If you are using a Cryptoki signing station other than a Luna 7.x application partition, include the **-c** option. You are prompted for the partition/token credential. By default, the Crypto Officer role is used; to use the Crypto User role instead, include the **-u** option.

mkfm -f <filepath/name>.bin **-o** <filepath/name>.fm **-k** <token_or_partition_name/<private_key_label> [**-c**] [**-u**]

```

[root@k7tower bin-ppc]# ./mkfm -f /usr/safenet/lunafmsdk/samples/skeleton/fm/bin-
ppc/skeleton.bin -o /usr/safenet/lunafmsdk/samples/skeleton/fm/bin-ppc/skeleton.fm -k
myLunaPartition/FMpriv
Luna Functionality Module Signer Utility (64-bit) v7.4.0-208. Copyright (c) 2018 SafeNet. All
rights reserved.

```

Please Enter the PIN: (for user 'co' on slot 3) *****

mkfm: Processing ELF file /usr/safenet/lunafmsdk/samples/skeleton/fm/bin-ppc/skeleton.bin

File successfully signed

The signed FM is now located in the directory you specified:

```

[user@myLunaClient ~]# cd /usr/safenet/lunafmsdk/samples/skeleton/fm/bin-ppc/
[user@myLunaClient bin-ppc]# ls
skeleton.bin skeleton.fm

```

Next, see ["Loading an FM Into the HSM Firmware" on the next page.](#)

Loading an FM Into the HSM Firmware

A signed FM must be loaded into the HSM firmware to provide new functionality. The HSM SO can load FMs using LunaSH and the following procedure.

NOTE A certificate used to sign an FM must have attribute `CKA_PRIVATE` set as true. If an existing certificate has `Private=0`, you can use the CMU tool to export that cert, then re-import it while setting `-private=1`. Or, if the partition retains the FM signing keypair, you can run the `"cmu selfsigncertificate"` command again to re-create the certificate, this time setting `-private=1` explicitly.

Prerequisites

- > Your HSM must meet the criteria described in ["Preparing the Luna Network HSM to Use FMs" on page 242](#).
- > **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 244](#), 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 appliance **admin** files.

NOTE If you load an FM with the same FM ID as an already-loaded FM, it is considered an update, and replaces the existing FM.

To load an FM into the HSM firmware

1. Use **pscp** or **scp** to transfer the signed FM to the appliance **admin** account.
`pscp <signed_FM> admin@<host/IP>:`
2. Use **pscp** or **scp** to transfer the signing certificate to the appliance **admin** account. If you have previously loaded an FM signed by the same key, it should already be in the appliance **admin** files.
3. Connect to the appliance via SSH or a serial connection, and log in to LunaSH as **admin**.
4. Log in as HSM SO.
`lunash:> hsm login`
5. [Optional] Confirm that the signed FM and the correct certificate are present in the **admin** files.
`lunash:> my file list`
6. Load the FM to the HSM by specifying the FM and signing certificate files.
`lunash:> hsm fm load -certFile <cert_file> -fmFile <FM_file>`

- Restart the HSM. It is not necessary to reboot the appliance.

```
lunash:> hsm restart
```

NOTE If you have FMs loaded, you must restart the HSM whenever you perform any of the following operations:

- > create a new partition and assign it to a client (even if it has the same slot number as a recently-deleted partition),
- > make a destructive change like re-initializing or zeroizing the HSM, or changing a destructive policy.

You will be unable to use the loaded FMs with new partitions until you restart the HSM. Use lunash:> **hsm restart**.

- Log back in as HSM SO.

```
lunash:> hsm login
```

- Activate the Secure Memory File System.

```
lunash:> hsm fm smfs activate
```

- [Optional] Confirm that the FM was loaded and is now enabled.

```
lunash:> hsm fm status
```

Deleting an FM From the HSM Firmware

This procedure allows the HSM SO to delete a specified FM from the HSM firmware using LunaSH.

NOTE If you are replacing the currently-loaded FM with an updated version, you do not need to delete the old version. If the new version has the same FM ID, it will replace the original version in the HSM firmware (see "[Loading an FM Into the HSM Firmware](#)" on the previous page).

In addition to the procedure below, other actions can cause FMs to be deleted from the HSM and the SMFS to be erased. See "[Effects of Administrative Actions on Functionality Modules](#)" on page 251.

Prerequisites

- > You require the FM ID of the FM you wish to delete.

To delete an FM from the HSM firmware

- [Optional] List the FMs currently loaded on the HSM to obtain the desired FM ID.

```
lunash:> hsm fm status
```

- Log in as HSM SO.

```
lunash:> hsm login
```

- Delete the FM by specifying its FM ID.

```
lunash:> hsm fm delete -id <FM_ID>
```

4. [Optional] Check the FM status again. The deleted FM's status is listed as "Zombie". At this point the FM is disabled, and its data will be fully deleted the next time you restart the HSM.

```
lunash:> hsm fm status
```

```
Getting status of the FM on all available devices
```

```
Current Functionality Module Configuration for device 0:
```

```
Serial # : 66331
Model   : Luna K7
SMFS    : Activated

FM Label      : skeleton
FM ID         : a000
Version      : 1.01
Manufacturer  : Safenet Inc.
Build Time    : Wed Dec 5 14:44:47 2018 - EST
Fingerprint  : 78 7C E3 C2 01 54 B3 99 08 59
ROM size     : 7302
Status       : Zombie (reboot HSM to cleanup)
Startup Status: OK
```

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

5. Restart the HSM. It is not necessary to reboot the appliance.

```
lunash:> hsm restart
```

Recovering the HSM After FM Failure

In the event that an FM bug causes problems on the HSM, such as halting the HSM or other functionality issues, the HSM SO can take steps to recover the HSM. If you have important FM key objects stored in the Secure Memory File System (SMFS), you may be able to regain access to them. If you encounter issues with FM functionality, try the following before you proceed with recovery operations:

1. Debug your FM code. Build and sign the FM ("[Building and Signing an FM](#)" on page 244), and attempt to load it onto the HSM ("[Loading an FM Into the HSM Firmware](#)" on page 248). Loading an updated FM with the same FM ID will erase the old version and replace it.
2. If this does not fix the problem, or you are unable to load the patched FM, delete the old FM first ("[Deleting an FM From the HSM Firmware](#)" on the previous page).
3. If this does not work, continue to the recovery procedure below.

LunaSH includes the **hsm fm recover** command, which allows you to delete all FMs currently loaded on the HSM, erase the SMFS, or both. This provides a last resort for recovering HSM functionality when an FM causes a failure.

Prerequisites

- > Try the methods above before continuing. If you are running multiple FMs, it may be simpler to delete and replace the one that is causing the issue.

To recover the HSM after FM failure

1. Log in as HSM SO.

```
lunash:> hsm login
```

2. Erase all FMs currently loaded on the HSM. This will leave the SMFS intact and preserve any key material you may have stored there.

```
lunash:> hsm fm recover -erase fm
```

You may now attempt to load a patched version of your FM that addresses the cause of the issue. If this does not resolve the problem, continue to step 3.

3. Choose one of the following options:

CAUTION! Both of these options will erase the SMFS and any cryptographic objects you have stored there. If this is important key material, erasing the SMFS is a last resort to restore HSM functions.

- a. Erase the SMFS.

```
lunash:> hsm fm recover -erase smfs
```

- b. Erase both the loaded FMs and the SMFS

```
lunash:> hsm fm recover -erase both
```

4. Load your patched FM and restart the SMFS (see "[Loading an FM Into the HSM Firmware](#)" on page 248).

Effects of Administrative Actions on Functionality Modules

Action	Deletes FMs
Destructive HSM Policy	Yes
Zeroize on 3 bad SO attempts	No
hsm zeroize command	No
hsm factoryReset command	Yes
Decommission	Yes
hsm init when already initialized	No
Destructive CUF application	Yes

NOTE: In all the above cases, the Secure Memory File System is re-initialized, destroying all contents.

NOTE Ensure that all destructive policies are set before you load FMs into the HSM firmware. Any change of a destructive policy will erase all loaded FMs.

CHAPTER 12: Zeroizing or Resetting the HSM to Factory Conditions

During the lifetime of a Luna HSM, you might have cause to take the HSM out of service, and wish to perform actions to ensure that no trace of your sensitive material remains. Those events might include:

- > Placing the unit into storage, perhaps as a spare
- > Shipping to another location or business unit in your organization
- > Shipping the unit back to Thales for repair/re-manufacture
- > Removing the HSM permanently from operational use, for disposal at end-of-life

This chapter describes the available options in the following sections:

- > ["HSM Zeroization" below](#)
- > ["Resetting the Luna Network HSM to Factory Condition" on the next page](#)
- > ["Comparing Zeroize, Decommission, Re-image, and Factory Reset" on page 255](#)
- > ["Comparison of Destruction/Denial Actions" on page 256](#)
- > ["Stored Data Integrity" on page 257](#)
- > ["Effects of Administrative Actions on Functionality Modules" on page 251](#)

See also [Re-Imaging or Decommissioning the HSM Appliance](#).

HSM Zeroization

In the context of HSMs in general, the term "zeroize" means to erase all plaintext keys. Some HSMs keep all keys in plaintext within the HSM boundary. Luna HSMs do not.

In the context of Luna HSMs, keys at rest (keys or objects that are stored in the HSM) are encrypted. Keys are decrypted into a volatile working memory space inside the HSM only while they are being used. Items in volatile memory disappear when power is removed. The action that we loosely call "zeroizing", or clearing, erases volatile memory as well as destroying the key that encrypts stored objects.

Any temporarily decrypted keys are destroyed, and all customer keys on the HSM are immediately rendered inaccessible and unrecoverable whenever you:

- > perform **hsm factoryreset**
- > make too many bad login attempts on the SO account
- > press the Decommission button on the Luna Network HSM back panel
- > set a "destructive" HSM policy
- > perform HSM firmware rollback

The KEK (key encryption key that encrypts all user objects, partition structure, cloning vectors, masking vectors, etc.) is destroyed by a zeroization (erasure) or decommission event. At that point, any objects or identities in the HSM become effectively random blobs of bits that can never be decoded.

NOTE The next HSM power-up following a KEK zeroization automatically erases the contents of user storage, which were already an indecipherable blob without the original KEK. That is, any zeroizing event instantly makes encrypted objects unusable, and as soon as power is re-applied, the HSM immediately erases even the encrypted remains before it allows further use of the HSM.

The HSM must now be re-initialized in order to use it again, and initialization overwrites the HSM with new user parameters. Everything is further encrypted with a new KEK unique to that HSM.

Keys not encrypted by the KEK are those that require exemption and are not involved in user identities or user objects:

- > The Master Tamper Key, which enables tamper handling
- > The Remote PED Vector, to allow Remote PED-mediated recovery from tamper or from Secure Transport Mode
- > The hardware origin key that certifies the HSM hardware as having been built by Thales

Resetting the Luna Network HSM to Factory Condition

These instructions will allow you to restore your Luna Network 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 and appliance software updates, those remain in place, and are not affected by this procedure.

To revert to a baseline appliance software/firmware, see [Re-Imaging the Appliance to Factory Baseline](#).

To roll back the HSM firmware to the previous version, see ["Rolling Back the Luna HSM Firmware" on page 223](#).

For eIDAS compliance, 'hsmrecover' function is added to factoryreset commands - see ["Stored Data Integrity" on page 257](#).

The standalone "hsmrecover" tool in the tools folder performs the same action, but can present additional messages that might be useful to Support engineers.

Prerequisites

- > Only the HSM SO can perform factory reset.
- > If you have STC enabled on the HSM, disable it by turning off **HSM policy 39** before continuing (see ["Setting HSM Policies Manually" on page 160](#)).
- > You must access LunaSH via a serial console to execute [hsm factoryreset](#).

To reset the HSM to factory condition

1. Login as HSM SO.

```
lunash:> hsm login
```

2. Reset the HSM to factory settings.

lunash:> **hsm factoryreset**

3. Reset the appliance configuration (network settings, ssh, ntl, etc.) to factory settings.

lunash:> **sysconf config factoryreset -service all**

4. Reboot the appliance.

Comparing Zeroize, Decommission, Re-image, and Factory Reset

You can clear the contents of your Luna Cloud HSM service, or the HSM may be cleared in response to an event. How this affects the contents and configuration of your HSM depends on whether the user partitions were deleted or whether the HSM was zeroized, decommissioned, re-imaged, or factory reset as detailed below:

Action	Command/Event	Description
Erase User Partitions	<ul style="list-style-type: none"> > Enable or disable a destructive HSM policy 	<p>Destroy/erase all user partitions, but do not zeroize the HSM. Policy 46 "Disable Decommission" is the exception in that it zeroizes the HSM and erases all user partitions if the policy is changed. To bring the HSM back into service, you need to:</p> <ol style="list-style-type: none"> 1. Recreate the partitions 2. Reinitialize the partition roles
Zeroize	<ul style="list-style-type: none"> > Too many bad login attempts on the HSM SO account > Perform an HSM firmware rollback > lunash:> hsm zeroize 	<p>Deletes all partitions and their contents, but retains the HSM configuration (audit role and configuration, policy settings). To bring the HSM back into service, you need to:</p> <ol style="list-style-type: none"> 1. Reinitialize the HSM 2. Recreate the partitions 3. Reinitialize the partition roles
Decommission	<ul style="list-style-type: none"> > Press the decommission button on the rear of the appliance. > Enable HSM Policy 40: Decommission on Tamper, and tamper the HSM. 	<p>Deletes all partitions and their contents, the audit role, and the audit configuration. Retains the HSM policy settings. To bring the HSM back into service, you need to:</p> <ol style="list-style-type: none"> 1. Reinitialize the HSM 2. Reinitialize the audit role and reconfigure auditing 3. Recreate the partitions 4. Reinitialize the partition roles

Action	Command/Event	Description
Re-image the Appliance	lunash:> sysconf reimage start	Formats the Luna Network HSM file system, zeroizes the HSM, erases the appliance configuration, and resets the software/firmware to the baseline version. You will need to reconfigure the appliance and the HSM as if it were new, including setting a password for the admin role.
Factory Reset	lunash:> hsm factoryreset	Deletes all partitions and their contents, and resets all roles and policy configurations to their factory default values. To bring the HSM back into service, you need to completely reconfigure the HSM as though it were new from the factory.

Comparison of Destruction/Denial Actions

Various operations on the Luna Network HSM are intended to make HSM contents unavailable to potential intruders. The effect of those actions are summarized and contrasted in the following table, along with notes on how to recognize and how to recover from each scenario.

Scenario 1: MTK is destroyed, HSM is unavailable, but use/access can be recovered after reboot (See Note 1)

Scenario 2: KEK is destroyed (Real-Time Clock and NVRAM), HSM contents cannot be recovered without restore from backup (See Note 2)

Scenario 3: Appliance admin password reset

Event	Scen. 1	Scen. 2	Scen. 3	How to discover (See Note 3)	How to recover
<ul style="list-style-type: none"> > Three bad SO login attempts > lunash:> hsm zeroize > lunash:> hsm factoryreset > Any change to a destructive policy > Firmware rollback (See Note 4) 	NO	YES	NO	<ul style="list-style-type: none"> > Log entry > "HSM IS ZEROIZED" in HSM Details (from hsm show) 	Restore HSM objects from Backup
Log in to Luna Network HSM "recover" account (local serial connection)	NO	NO	YES	Log entry shows login by "recover"	Log into appliance as admin, using the reset password "PASSWORD" and change to a secure password

Event	Scen. 1	Scen. 2	Scen. 3	How to discover (See Note 3)	How to recover
Hardware tamper <ul style="list-style-type: none"> > Undervoltage or overvoltage during operation > Under-temperature or over-temperature during operation > Chassis interference (such as cover, fans, etc.) Software (command-initiated) tamper <ul style="list-style-type: none"> > <code>lunash:> hsm stm transport</code> 	YES	NO	NO	Parse logs for text like "tamper", "TVK was corrupted", or "Generating new TVK", indicating that a tamper event was logged. Example: <pre>RTC: external tamper latched/ MTK: security function was zeroized on previous tamper event and has not been restored yet</pre> Also, keywords in logs like: "HSM internal error", "device error" Luna Network HSM appliance front panel flashes error 30.	Reboot [See Note 1]
Decommission <ul style="list-style-type: none"> > Pressing the Decommission button on the back of the appliance 	NO	YES	NO	Look for log entry like: <pre>RTC: tamper 2 signal/Zeroizing HSM after decommission...LOG(INFO): POWER-UP LOG DUMP END</pre>	Restore HSM objects from Backup

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 136](#).

Stored Data Integrity

Beginning with Luna HSM firmware 7.7.0 a new eIDAS-supporting feature called SDI, Stored Data Integrity, has been added that checks the integrity of the stored data. The HSM firmware will halt if it detects that objects have been corrupted. An `hsmrecover` function has been introduced, as part of the **hsm factoryReset**

command to clear the storage and recover the HSM from the halt state without requiring RMA of the appliance.

If the HSM firmware halts because data in the volatile memory is corrupted, restarting the HSM using `lunash:>hsm restart` or rebooting the appliance (**`sysconf appliance reboot`**) should recover the HSM without losing data in permanent storage.

If the HSM firmware halts because data in the permanent flash storage is corrupted, the HSM is recovered by using the newly enhanced **`hsm factoryReset`** command which deletes all the partitions, zeroizes all the objects, and resets the policies.

Since **`hsm factoryReset`** is destructive, it is important to keep a regular backup of HSM objects in case the HSM ever goes into a state that requires factory reset.

Running the **`hsm factoryReset`** command, while the HSM is in normal working state, has the same behavior as before firmware 7.7.0.

Running the **`hsm factoryReset`** command, while the HSM is in a halt state (where the normal "factoryReset" fails), invokes the recovery process, which takes several minutes (6+ minutes) to complete. It is important to wait for the **`hsm factoryReset`** command to complete without interruption.

For an example of the output, see [hsm factoryreset](#). Also see "[Comparison of Destruction/Denial Actions](#)" on [page 256](#).

