



# Thales Luna USB HSM 7

## HSM ADMINISTRATION GUIDE



# Document Information

---

Last Updated	2025-08-27 11:21:34 GMT-05:00
--------------	-------------------------------

## Trademarks, Copyrights, and Third-Party Software

Copyright 2001-2025 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 .....	8
Customer Release Notes .....	8
Audience .....	9
Document Conventions .....	9
Support Contacts .....	11
Chapter 1: Luna USB HSM 7 Hardware Installation .....	12
Verifying the Integrity of Your Shipment .....	12
Luna USB HSM 7 Required Items .....	15
Basic Luna USB HSM 7 order items .....	15
Optional Multifactor Quorum-Authentication Items .....	16
Installing the Luna USB HSM 7 Hardware .....	18
Luna USB HSM 7 Hardware Functions .....	18
Chapter 2: Luna HSM Client Software Installation .....	20
Windows Luna HSM Client Installation .....	21
Command line options overview .....	21
Installing all components and features .....	24
Installing the Luna HSM Client for the Luna Network HSM 7 .....	25
Installing the Luna HSM Client for the Luna PCIe HSM 7 .....	25
Installing the Luna HSM Client for the Luna USB HSM 7 .....	25
Installing the Luna HSM Client for the Luna Backup HSM .....	26
Installing the Luna HSM Client for Remote PED .....	26
Installation Location .....	26
ChrystokiConfigurationPath Environment Variable .....	27
Logging .....	27
Uninstalling the Luna HSM Client .....	27
Windows Interactive Luna HSM Client Installation .....	28
Required Client Software .....	28
Prerequisites .....	28
Installing the Luna HSM Client Software .....	29
Modifying the Installed Windows Luna HSM Client Software .....	31
Java .....	32
Luna CSP and KSP .....	32
Modifying the Number of Luna Backup HSM Slots .....	32
Uninstalling the Luna HSM Client Software .....	33
After Installation .....	34
Troubleshooting .....	34
Linux Luna HSM Client Installation .....	36
Prerequisites .....	36

Where to install, and SELinux .....	37
About Installing the Luna HSM Client Software .....	38
Scripted or Unattended Installation .....	40
Interrupting the Installation .....	41
Controlling User Access to Your Attached HSMs and Partitions .....	44
Uninstalling the Luna HSM Client Software or Removing Components .....	45
Java .....	45
Modifying the Number of Luna Backup HSM Slots .....	45
Effects of Kernel Upgrades .....	46
Troubleshooting .....	46
Adding a Luna Cloud HSM Service .....	46
Initializing a Luna Cloud HSM Service .....	48
Dynamic Partition Loading for Luna Cloud HSM Services .....	49
Configuration File Summary .....	51
Dynamic UserID Loading for Luna Cloud HSM Services .....	76
Updating the Luna HSM Client Software .....	77
<b>Chapter 3: Secure Transport Mode .....</b>	<b>78</b>
When STM is enabled on the HSM .....	78
Recovering an HSM From Secure Transport Mode .....	79
Placing an HSM In Secure Transport Mode .....	80
<b>Chapter 4: Multifactor Quorum Authentication .....</b>	<b>82</b>
Multifactor Quorum Authentication Architecture .....	82
Comparing Password and Multifactor Quorum Authentication .....	83
iKeys .....	83
iKey Types and Roles .....	84
Shared iKey Secrets .....	85
M of N Split Secrets (Quorum) .....	86
iKey Management Using Luna USB HSM 7 .....	87
Creating iKey Using Luna USB HSM 7 .....	87
Authenticating a Role Using Luna USB HSM 7 .....	89
Consequences of Losing iKeys .....	91
Identifying an iKey Secret Using Luna USB HSM 7 .....	93
Duplicating an Existing iKey Using Luna USB HSM 7 .....	93
Changing an iKey Credential .....	94
<b>Chapter 5: Audit Logging .....</b>	<b>97</b>
Audit Logging Features .....	97
Audit limitations and Controlled tamper recovery state .....	102
The Audit Role .....	102
Audit Log Secret .....	103
Audit Log Records .....	104
Audit Log Message Format .....	105
Timestamping .....	106
Log Capacity .....	106
Audit Logging General Advice and Recommendations .....	106

Configuring and Using Audit Logging .....	109
Configuring Audit Logging .....	110
Exporting the Audit Logging Secret and Importing to a Verifying HSM .....	111
Audit Role Authentication Considerations .....	113
Logging In as Auditor .....	113
Audit Log Categories and HSM Events .....	114
Partition Role IDs .....	114
HSM Access .....	114
Log External .....	116
HSM Management .....	116
Key Management .....	117
Key Usage and Key First Usage .....	119
Per-Key Authorization .....	120
Audit Log Management .....	120
Audit Log Troubleshooting .....	121
Cryptographic Operations Blocked During Remote PED Operations When Audit Logging Is Enabled ..	122
<b>Chapter 6: Initializing the Luna USB HSM 7 .....</b>	<b>123</b>
Initializing a New or Factory-reset HSM .....	123
Re-initializing the Luna USB HSM 7 .....	126
<b>Chapter 7: HSM Roles .....</b>	<b>127</b>
Administrator (AD) .....	128
Logging In as HSM Security Officer .....	128
Changing a Role Credential .....	128
Name, Label, and Password Requirements .....	129
HSM Labels .....	129
Cloning Domains .....	130
Partition Labels .....	130
Role Passwords or Challenge Secrets .....	130
<b>Chapter 8: HSM Capabilities and Policies .....</b>	<b>131</b>
Setting HSM Policies Manually .....	138
Setting HSM Policies Using a Template .....	138
Creating an HSM Policy Template .....	139
Editing an HSM Policy Template .....	139
Applying an HSM Policy Template .....	140
<b>Chapter 9: Application Partitions .....</b>	<b>141</b>
Creating the Application Partition .....	141
Deleting the Application Partition .....	141
<b>Chapter 10: Security in Operation .....</b>	<b>143</b>
Physical Security and Tamper Events .....	143
Tamper Events .....	144
Recovering from a Tamper Event .....	144
Security Effects of Administrative Actions .....	145

Overt Security Actions .....	145
Actions with Security- and Content-Affecting Outcomes .....	145
Elsewhere .....	148
<b>Chapter 11: Monitoring the HSM .....</b>	<b>149</b>
HSM Status Values .....	149
System Operational and Error Messages .....	150
Performance Monitoring .....	152
Partition Utilization Metrics .....	153
Rules of acquisition .....	153
Availability of Partition Utilization Metrics .....	154
Cryptographic Module and Token Return Codes .....	154
Library Codes .....	172
Vendor-Defined Return Codes .....	176
<b>Chapter 12: HSM Updates .....</b>	<b>183</b>
Updating the Luna USB HSM 7 Firmware .....	183
Changing the Firmware Upgrade Permissions (Linux only) .....	184
Rolling Back the Luna HSM Firmware .....	184
<b>Chapter 13: Zeroizing or Resetting the HSM to Factory Conditions .....</b>	<b>186</b>
Comparing Zeroize and Factory Reset .....	186
HSM Zeroization .....	187
Resetting the Luna USB HSM 7 to Factory Condition .....	188
Stored Data Integrity .....	188

# 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:

- > "Luna USB HSM 7 Hardware Installation" on page 12
- > "Luna HSM Client Software Installation" on page 20
- > "Secure Transport Mode" on page 78
- > "Multifactor Quorum Authentication" on page 82
- > "Audit Logging" on page 97
- > "Initializing the Luna USB HSM 7" on page 123
- > "HSM Roles" on page 127
- > "HSM Capabilities and Policies" on page 131
- > "Application Partitions" on page 141
- > "Security in Operation" on page 143
- > "Monitoring the HSM" on page 149
- > "HSM Updates" on page 183
- > "Zeroizing or Resetting the HSM to Factory Conditions" on page 186

The preface includes the following information about this document:

- > "Customer Release Notes" below
- > "Audience" on the next page
- > "Document Conventions" on the next page
- > "Support Contacts" on page 11

For information regarding the document status and revision history, see "Document Information" on page 2.

## Customer Release Notes

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

## Audience

---

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

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

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

## Document Conventions

---

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

### Notes

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

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

### Cautions

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

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

### Warnings

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

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

## Command syntax and typeface conventions

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

## Support Contacts

---

If you encounter a problem while installing, registering, or operating this product, please refer to the documentation before contacting support. If you cannot resolve the issue, contact your supplier or [Thales Customer Support](#). Thales Customer Support operates 24 hours a day, 7 days a week. Your level of access 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: Luna USB HSM 7 Hardware Installation

This chapter describes how to install and connect a Luna USB HSM 7. To ensure a successful installation, perform the following tasks in the order indicated:


1. Before unpacking your new hardware, refer to ["Verifying the Integrity of Your Shipment" below](#) for safe unpacking instructions.
2. Ensure that you have all of the required components, as listed in ["Luna USB HSM 7 Required Items" on page 15](#).
3. Install and connect the hardware, as described in ["Installing the Luna USB HSM 7 Hardware" on page 18](#).
4. Familiarize yourself with the hardware features as described in ["Luna USB HSM 7 Hardware Functions" on page 18](#).



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

## Verifying the Integrity of Your Shipment

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

Step	Yes	No
1. Do the items received (individual items, part numbers) match those listed in the enclosed packing list? If yes, go to the next step. If no, contact Thales support.		
2. Before you received the product, did you receive an advanced shipping notification providing details regarding the shipment (part numbers and serial numbers for the product, and for tamper-evident bag(s))? If yes, go to the next step. If no, contact Thales support.		

Step	Yes	No
<p>3. Are any tamper-evident bag serial numbers that are listed in the advanced shipping notification present, and do they match the actual bag(s) received? The tamper-evident bag serial numbers appear as shown below.</p>  <p>If yes, go to the next step. If no, contact Thales support.</p> <div><b>NOTE</b> The serial number of the bag is tracked. Serial numbers of additional stickers on the bag are not tracked, and are meant only for inspection against physical alteration.</div>		
<p>4. Did you receive any tamper-evident bags that are <i>not</i> listed on the advance shipping notification? If yes, contact Thales support. If no, go to the next step.</p>		



Step	Yes	No
<p>5. There are no tamper labels on the device itself. The device is in an anti-static bag and then that bag and device are inside an anti-tamper bag. The anti-tamper bag has a serial number as shown inside the dotted-lines, below. Does the tamper-evident bag appear intact, and with the correct serial number?</p> <div></div> <p>If no, contact Thales support. If yes, go to the next step.</p>		
<p>6. Are there any signs of physical tampering? The tamper seals on the tamper bag indicate tampering if they show the ALERT markings as illustrated.</p> <div></div> <p>If yes, contact Thales support. If no, go to the next step.</p>		
<p>7. Once you have verified all of the received items, you can proceed with the installation.</p>		



# Luna USB HSM 7 Required Items

This section provides a list of the components you should have received with your Luna USB HSM 7 order, as well as descriptions of some optional items you may have ordered.

## Basic Luna USB HSM 7 order items

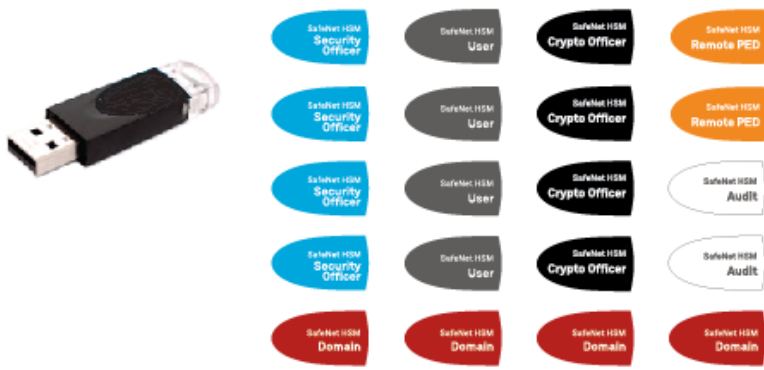
The standard items that you should have received as your basic order for a Luna USB HSM 7 are:

Qty	Item
1	<div>Luna USB HSM 7</div> <div></div>
1	<div>5V Power Supply with replaceable plug modules for international use</div> <div></div>

Qty	Item
1	<b>USB-C to USB 3 connector cable</b> 
1	<b>USB 3 to USB-C adapter</b>  Used to connect iKeys to the Luna USB HSM 7.

## Optional Multifactor Quorum-Authentication Items

Your order may include iKeys for multifactor quorum authentication.

Qty	Item																														
1	<div><div>Set of iKeys and Labels</div><div><p>The image shows a Luna USB HSM 7 device on the left. To its right is a grid of 20 peel-and-stick labels arranged in 5 rows and 4 columns. The labels are color-coded and labeled as follows:</p><table><tr><th>Row</th><th>Label 1</th><th>Label 2</th><th>Label 3</th><th>Label 4</th></tr><tr><td>1</td><td>SafelNet HSM Security Officer</td><td>SafelNet HSM User</td><td>SafelNet HSM Crypto Officer</td><td>SafelNet HSM Remote PED</td></tr><tr><td>2</td><td>SafelNet HSM Security Officer</td><td>SafelNet HSM User</td><td>SafelNet HSM Crypto Officer</td><td>SafelNet HSM Remote PED</td></tr><tr><td>3</td><td>SafelNet HSM Security Officer</td><td>SafelNet HSM User</td><td>SafelNet HSM Crypto Officer</td><td>SafelNet HSM Audit</td></tr><tr><td>4</td><td>SafelNet HSM Security Officer</td><td>SafelNet HSM User</td><td>SafelNet HSM Crypto Officer</td><td>SafelNet HSM Audit</td></tr><tr><td>5</td><td>SafelNet HSM Domain</td><td>SafelNet HSM Domain</td><td>SafelNet HSM Domain</td><td>SafelNet HSM Domain</td></tr></table></div><p>Your order may include a set of iKeys and peel-and-stick labels.</p></div>	Row	Label 1	Label 2	Label 3	Label 4	1	SafelNet HSM Security Officer	SafelNet HSM User	SafelNet HSM Crypto Officer	SafelNet HSM Remote PED	2	SafelNet HSM Security Officer	SafelNet HSM User	SafelNet HSM Crypto Officer	SafelNet HSM Remote PED	3	SafelNet HSM Security Officer	SafelNet HSM User	SafelNet HSM Crypto Officer	SafelNet HSM Audit	4	SafelNet HSM Security Officer	SafelNet HSM User	SafelNet HSM Crypto Officer	SafelNet HSM Audit	5	SafelNet HSM Domain	SafelNet HSM Domain	SafelNet HSM Domain	SafelNet HSM Domain
Row	Label 1	Label 2	Label 3	Label 4																											
1	SafelNet HSM Security Officer	SafelNet HSM User	SafelNet HSM Crypto Officer	SafelNet HSM Remote PED																											
2	SafelNet HSM Security Officer	SafelNet HSM User	SafelNet HSM Crypto Officer	SafelNet HSM Remote PED																											
3	SafelNet HSM Security Officer	SafelNet HSM User	SafelNet HSM Crypto Officer	SafelNet HSM Audit																											
4	SafelNet HSM Security Officer	SafelNet HSM User	SafelNet HSM Crypto Officer	SafelNet HSM Audit																											
5	SafelNet HSM Domain	SafelNet HSM Domain	SafelNet HSM Domain	SafelNet HSM Domain																											

## Installing the Luna USB HSM 7 Hardware

This section describes how to connect the Luna USB HSM 7 to a client computer.

### Prerequisites

- > Ensure that the Luna HSM Client software with the **USB** option is installed on the client (see "[Luna HSM Client Software Installation](#)" on page 20). This includes the necessary device drivers.

**NOTE** If you are installing Luna HSM Client on Windows, the driver may not be installed unless the Luna device is connected to the computer first; refer to [Backup/USB/PCIe Drivers Not Installed on Windows 10 or Windows Server 2022 Unless Device is Connected](#).

### To connect the Luna USB HSM 7 to a client

1. Use the included USB-C to USB cable to connect the Luna USB HSM 7 to a USB port on the client computer.

**NOTE** On most Luna HSM Client computers, the USB port provides adequate power, and connecting the provided power supply is not recommended. Wait and confirm that the HSM boots properly. If the HSM fails to boot up:

1. Disconnect the HSM from the USB port.
2. Connect the HSM to power using the provided power supply. Wait for it to boot completely.
3. Reconnect the HSM to the USB port on the client.

If the HSM is connected to the USB port before the power supply, you may encounter an issue where the HSM occasionally loses contact with the client, and must be power cycled.

2. Run LunaCM on the client computer to ensure the Luna USB HSM 7 is visible to the client.

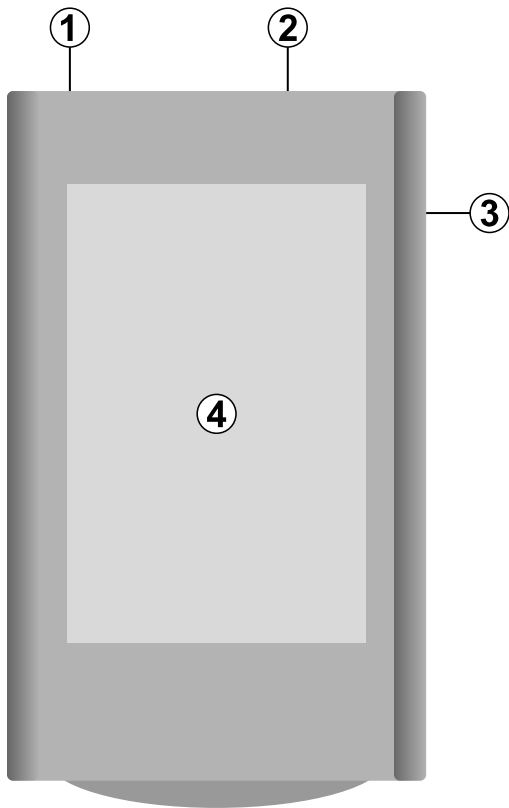
Available HSMs:

```
Slot Id -> 4
Label ->
Serial Number -> 556677
Model -> Luna G7
Firmware Version -> 7.7.2
Bootloader Version -> 1.6.0
Configuration -> Luna HSM Admin Partition (PW) Key Export With Cloning Mode
Slot Description -> Admin Token Slot
HSM Status -> L3 Device, Zeroized
```

Current Slot Id: 4

## Luna USB HSM 7 Hardware Functions

The Luna USB HSM 7 hardware is illustrated below, with important features labeled.



1	5V power supply connector. Required only if the USB port connected to (2) does not supply adequate power to the Luna USB HSM 7.
2	USB-C connector. Used for connecting to the client computer and for file transfer to the Luna USB HSM 7.
3	USB-C connector. Used for connecting iKeys to authenticate roles on the HSM. Requires the included USB-A to USB-C adapter.
4	LED touchscreen. Displays information about the Luna USB HSM 7 and is used to input role-specific information like PINs.

The Luna USB HSM 7 does not contain an internal battery, and maintains the integrity of its stored key material without being connected to power.

## CHAPTER 2: Luna HSM Client Software Installation

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

- > For Luna Network HSM 7, install the Luna HSM Client on any computer that must connect to the appliance as a client.
- > For Luna PCIe HSM 7, install the Luna HSM Client on the workstation into which the Luna PCIe HSM 7 is installed.
- > For Luna USB HSM 7, install the Luna HSM Client on the workstation connected to the Luna USB HSM 7.
- > Install the Luna HSM Client on any computer that is to have a Remote Luna PED connected.
- > Install the Luna HSM Client on any computer that is to serve as a Remote Backup server.

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

- > [Customer Release Notes](#)

Choose the instructions for your operating system:

- > ["Windows Luna HSM Client Installation" on the next page](#)
  - ["Windows Interactive Luna HSM Client Installation" on page 28](#)
- > ["Linux Luna HSM Client Installation" on page 36](#)
- > ["Adding a Luna Cloud HSM Service" on page 46](#)
- > ["Dynamic Partition Loading for Luna Cloud HSM Services" on page 49](#)
- > ["Configuration File Summary" on page 51](#)
- > ["Updating the Luna HSM Client Software" on page 77](#)

## Windows Luna HSM Client Installation

This section describes how to invoke the Windows Luna HSM Client perform unattended or scripted installations on Windows platforms.

**NOTE** The GUI interactive installer (see ["Windows Interactive Luna HSM Client Installation" on page 28](#)) is deprecated, and will be removed from a future release.

Use the **/quiet** switch (see below) to ensure no pauses or prompting during installation. The following procedures are described:

- > ["Command line options overview" below](#)
- > ["Installing the Luna HSM Client for the Luna Network HSM 7" on page 25](#)
- > ["Installing the Luna HSM Client for the Luna PCIe HSM 7" on page 25](#)
- > ["Installing the Luna HSM Client for the Luna USB HSM 7" on page 25](#)
- > ["Installing the Luna HSM Client for the Luna Backup HSM" on page 26](#)
- > ["Installing the Luna HSM Client for Remote PED" on page 26](#)
- > ["Installation Location" on page 26](#)
- > ["ChrystokiConfigurationPath Environment Variable" on page 27](#)
- > ["Logging" on page 27](#)
- > ["Uninstalling the Luna HSM Client" on page 27](#)

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

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

### Command line options overview

The following command-line options are available:

Option	Values	Description
addlocal=	Various (see below)	Takes one-or-more device values, and one-or-more feature values, as a comma-separated list. Case insensitive. Values may be quoted or not.
installdir=	A fully qualified folder path to install the client software	Case insensitive. Default value is "c:\program files\safenet\lunaclient". Enclose paths containing spaces in "".
/install	N/A	Install the product and features.

Option	Values	Description
/uninstall	N/A	Remove the product and features.
/quiet	N/A	Performs a silent installation; no prompts or messages. <b>NOTE</b> Windows defaults to launching the interactive graphical installer, unless you specify <b>/quiet</b> at the command line. Always include the <b>/quiet</b> option for scripted/unattended Luna HSM Client installation.
/norestart	N/A	Prevents a reboot, post-installation. Any reboots must be performed manually.
/log	The name of a log file	Generates a highly detailed series of logs of the installation progress. This is required only for product support.

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

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

The device names are not case-sensitive.

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

Feature identifier value	Can be installed with these Luna devices	Description
CSP_KSP	NETWORK, PCI, USB	Microsoft CSP and KSP
FMSDK	NETWORK, PCIe *	Functionality Modules Software Development Kit
FMTTOOLS	NETWORK, PCIe *	Tools for use when preparing Functionality Modules
JCPProv	NETWORK, PCIe, USB	JCPROV PKCS#11

Feature identifier value	Can be installed with these Luna devices	Description
JSP	NETWORK, PCIe, USB	Java Provider component
SDK	NETWORK, PCIe, USB	Software SDK – Java / C++ samples

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

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

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

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

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

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

## Installing all components and features

**NOTE** CSP or KSP registration includes a step that verifies the DLLs are signed by our certificate that chains back to the DigiCert root of trust G4 (in compliance with industry security standards).

This step can fail if your Windows operating system does not have the required certificate. If you have been keeping your Windows OS updated, you should already have that certificate.

If your Luna HSM Client host is connected to the internet, use the following commands to update the certificate manually:

```
certutil -urlcache -f http://cacerts.digicert.com/DigiCertTrustedRootG4.crt
```

```
certutil -addstore -f root DigiCertTrustedRootG4.crt
```

### To manually update a non-connected host

1. Download the DigiCert Trusted Root G4 (<http://cacerts.digicert.com/DigiCertTrustedRootG4.crt>) to a separate internet-connected computer.
2. Transport the certificate, using your approved means, to the Luna HSM Client host into a <downloaded cert path> location of your choice
3. Add the certificate to the certificate store using the command:  
**certutil -addstore -f root** <downloaded cert path>

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

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

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

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

- > Install the full Luna HSM Client software with drivers for all Luna HSMs (Luna Network HSM 7, Luna PCIe HSM 7, Luna Backup HSM, Remote PED), as well as all the features (CSP/KSP, JSP, JCProv, C++ SDK, SNMP Subagent)

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

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

- > [Optional logging] Install the full Luna HSM Client software with drivers for all Luna HSMs (Luna Network HSM 7, Luna PCIe HSM 7, Luna Backup HSM, Remote PED), as well as all the features (CSP/KSP, JSP, JCProv, C++ SDK, SNMP Subagent), and log the process.

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

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

## Installing the Luna HSM Client for the Luna Network HSM 7

Use the **ADDLOCAL=NETWORK** option to install the base client software for the Luna Network HSM 7. Include the values for any optional, individual software components you desire. The base software must be installed first.

### To install the Luna HSM Client for the Luna Network HSM 7

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

- > Install the base Luna HSM Client software necessary to communicate with Luna Network HSM 7

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

[Optional] Install the base Luna HSM Client software and any of the optional components for the Luna Network HSM 7 that you desire:

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

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

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

## Installing the Luna HSM Client for the Luna PCIe HSM 7

Use the **ADDLOCAL=PCI** option to install the base client software for the Luna PCIe HSM 7. Include any features you desire. The base software must be installed first.

### To install the Luna HSM Client for the Luna PCIe HSM 7

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

- > Install the base Luna HSM Client software for Luna PCIe HSM 7

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

- > Install the base Luna HSM Client software and any of the optional features for the Luna PCIe HSM 7 that you desire:

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

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

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

## Installing the Luna HSM Client for the Luna USB HSM 7

Use the **ADDLOCAL=USB** option to install the base client software for the Luna USB HSM 7. Include any features you desire. The base software must be installed first.

### To install the Luna HSM Client for the Luna USB HSM 7

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

- > Install for Luna USB HSM 7

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

- > Install the base Luna HSM Client software and any of the optional features for the Luna USB HSM 7 that you desire:

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

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

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

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

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

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

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

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

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

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

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

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

### Installing the Luna HSM Client for Remote PED

Use the **ADDLOCAL=** option with component value **PED** to install the client software for the Remote PED Server.

### To install the Luna HSM Client for the Remote PED Server

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

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

### Installation Location

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

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

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

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

## ChrystokiConfigurationPath Environment Variable

During installation of Luna HSM Client components, a new entry is added to the Windows environment variables: **ChrystokiConfigurationPath**. This variable contains the path to the Luna HSM Client configuration file, **Chrystoki.ini** (see ["Configuration File Summary" on page 51](#) for a full description).

**NOTE** After first-time installation or a re-installation where the path to **Chrystoki.ini** changed, any open command prompts must be closed and reopened to recognize the new **ChrystokiConfigurationPath** environment variable setting.

## Logging

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

Example commands that include logging are:

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

**LunaHSMClient.exe /uninstall /quiet /log uninstall.log**

## Uninstalling the Luna HSM Client

You can also perform scripted/unattended uninstallation.

### To uninstall the Luna HSM Client

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

**LunaHSMClient.exe /uninstall /quiet**

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

**LunaHSMClient.exe /uninstall /quiet /log uninstall.log**

# Windows Interactive Luna HSM Client Installation

**NOTE** The GUI interactive installer (see ["Windows Interactive Luna HSM Client Installation" above](#)) is deprecated, and will be removed from a future release.

This section describes how to install the Luna HSM Client software on Windows, using the GUI interactive installer. It contains the following topics:

- > ["Required Client Software" below](#)
- > ["Prerequisites" below](#)
- > ["Installing the Luna HSM Client Software" on the next page](#)
- > ["Modifying the Installed Windows Luna HSM Client Software" on page 31](#)
- > ["Java" on page 32](#)
- > ["Luna CSP and KSP" on page 32](#)
- > ["Modifying the Number of Luna Backup HSM Slots" on page 32](#)
- > ["Uninstalling the Luna HSM Client Software" on page 33](#)
- > ["After Installation" on page 34](#)
- > ["Troubleshooting" on page 34](#)
- > ["Windows Luna HSM Client Installation" on page 21](#)

Applicability to specific versions of Windows is summarized in the [Customer Release Notes](#) for this release.

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

## Required Client Software

Each computer that contains, or is connected to a Luna PCIe HSM 7 or a Luna USB HSM 7 must have the cryptoki library and other utilities and supporting files installed.

## Prerequisites

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

1. March 2014 Windows servicing stack update (see <https://support.microsoft.com/en-us/help/2919442>)
2. April 2014 Windows update (see <https://support.microsoft.com/en-us/help/2919355>)
3. Visual C++ Redistributable for Visual Studio 2015 (see <https://www.microsoft.com/en-in/download/details.aspx?id=481450>)

**NOTE** CSP or KSP registration includes a step that verifies the DLLs are signed by our certificate that chains back to the DigiCert root of trust G4 (in compliance with industry security standards).

This step can fail if your Windows operating system does not have the required certificate. If you have been keeping your Windows OS updated, you should already have that certificate.

If your Luna HSM Client host is connected to the internet, use the following commands to update the certificate manually:

```
certutil -urlcache -f http://cacerts.digicert.com/DigiCertTrustedRootG4.crt
```

```
certutil -addstore -f root DigiCertTrustedRootG4.crt
```

#### To manually update a non-connected host

1. Download the DigiCert Trusted Root G4 (<http://cacerts.digicert.com/DigiCertTrustedRootG4.crt>) to a separate internet-connected computer.
2. Transport the certificate, using your approved means, to the Luna HSM Client host into a <downloaded cert path> location of your choice
3. Add the certificate to the certificate store using the command:  
**certutil -addstore -f root <downloaded cert path>**

## Installing the Luna HSM Client Software

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

For compatibility of our HSMs with Windows CAPI we have Luna CSP, and for the newer Windows CNG we have Luna KSP. See "[Luna CSP and KSP](#)" on [page 32](#) for more information.

Interactive (prompted, this page) and non-interactive (no prompts "[Windows Luna HSM Client Installation](#)" on [page 21](#)) installation options are available.

#### **NOTE Compatibility of Luna PCIe HSM 7 version, Client version, and Windows OS versions**

[Luna HSM Client 10.3.0](#) was the last client version to support Windows Server 2012 R2, which accepts the Luna PCIe HSM 7 6.x driver.

If you have Windows Server 2012 R2 computer with a Luna PCIe HSM 7 6.x onboard, do not install [Luna HSM Client 10.4.0](#) or newer there; these client versions will not load the Luna PCIe HSM 7 6.x driver.

If you have Luna PCIe HSM 7 6.x and 7.x HSM card in the same system, failure of the 6.x driver would prevent loading of the 7.x driver as well. If your application works with Linux, the Luna PCIe HSM 7 6.x will continue to work there, and will not block Luna PCIe HSM 7 7.x.

## To install the Luna HSM Client software

1. Log into Windows as **Administrator**, or as a user with administrator privileges (see "[Troubleshooting](#)" on [page 34](#)).

- Uninstall any previous versions of the Client software before you proceed (see "[Uninstalling the Luna HSM Client Software](#)" on page 33).


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

- Download the Luna HSM Client from the Thales Support Portal at <https://supportportal.thalesgroup.com>.

**TIP** Thales recommends verifying the integrity of the Luna HSM Client packages, by calculating their SHA256 hash values and comparing with the hash values posted on the Support Portal, before installing them on your client machines.

You can use the sha256sum tool on Linux machines to calculate the SHA256 hash values.

- Extract the .zip to an appropriate folder.
- In the extracted directory, locate the folder for your Windows architecture and double click **LunaHSMClient.exe**.
- The Custom Setup dialog allows you to choose which software components you wish to install. Click a product to select the components to install, or click Select All to install all available components.

**Luna HSM Client** 

Version:

**Welcome to the Luna HSM Client setup wizard**  
This setup wizard will install Luna HSM Client on your computer. Please customize the install below.

Install location:  
C:\Program Files\SafeNet\LunaClient Select folder

**Install options:**

**Luna Devices**


- ☒ Select All
- ☐ Network
- ☐ PCIe
- ☐ USB
- ☐ Backup
- ☐ Remote PED

**Features**

- ☒ Select All
- ☐ CSP (CAPI) / KSP (CNG)
- ☐ JCE / JCA Provider (JSP)
- ☐ PKCS #11 (JCPProv)
- ☐ Software SDK
- ☐ SNMP Subagent
- ☐ FM Tools
- ☐ FM SDK

☐ I agree to the terms of the [Thales Software License Agreement](#).

INSTALL QUIT

**Luna HSM Client** 

Version:

**Welcome to the Luna HSM Client setup wizard**  
This setup wizard will install Luna HSM Client on your computer. Please customize the install below.

Install location:  
C:\Program Files\SafeNet\LunaClient Select folder

**Install options:**

**Luna Devices**

- ☒ Select All
- ☐ Network
- ☐ PCIe

**Features**

- ☒ Select All
- ☒ CSP (CAPI) / KSP (CNG)
- ☒ JCE / JCA Provider (JSP)

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

- a. Agree to the terms of the License Agreement to proceed with installation. To view the agreement text, click the link in the dialog. The installer loads a PDF version if a PDF reader is available; otherwise it launches a text editor and a plain-text version of the agreement.
  - b. If Windows presents a security notice asking if you wish to install the device driver from Thales, click "Always trust software from Thales DIS CPL USA, Inc." and click **Install** to accept.
  - c. If you choose not to install the driver(s), your Luna HSM Client cannot function with any locally-connected Luna hardware (which includes Luna PCIe HSM 7, Luna USB HSM 7, or Luna Backup HSMs).
7. When the installation completes, the button options are Uninstall, Modify, or Quit; click **Quit** to finish.
  8. [Optional] For easy use of the Luna HSM Client command-line tools, add the directory to the system PATH variable.

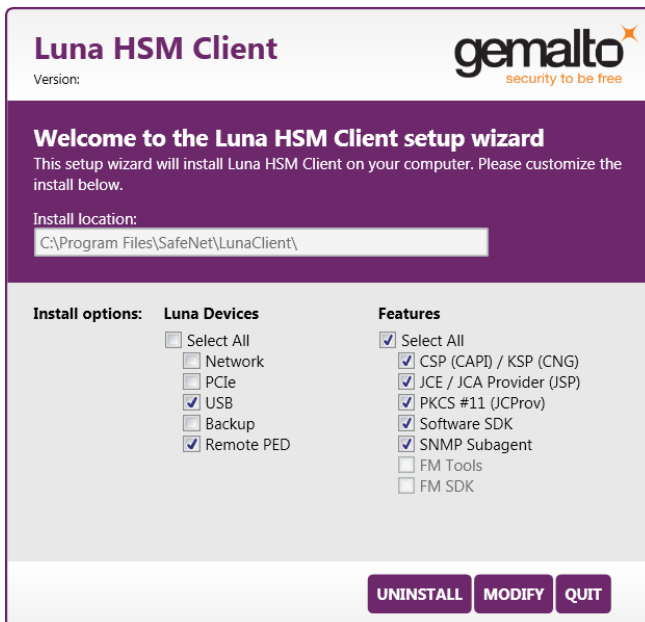
**"C:\Program Files\SafeNet\Lunaclient"**

## Modifying the Installed Windows Luna HSM Client Software

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

### To modify the installed Luna HSM Client software

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



2. Select or deselect individual Devices or Features, as desired.
3. Click **Modify**. The client software is updated (items are added or removed).

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

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

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

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

## Java

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

## Luna CSP and KSP

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

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

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

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

## Modifying the Number of Luna Backup HSM Slots

By default, the Luna HSM Client allows for three slots reserved for each model of Luna Backup HSM. You can edit **cryptoki.ini** to modify the number of reserved slots. See also "[Configuration File Summary](#)" on page 51.

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

1. Navigate to the **cryptoki.ini** file and open in a text editor.
2. Add the following line(s) to the **CardReader** section of the file:
  - For Luna Backup HSM G5:  
**LunaG5Slots = <value>;**
  - For Luna Backup HSM 7:  
**LunaG7Slots = <value>;**

## Uninstalling the Luna HSM Client Software

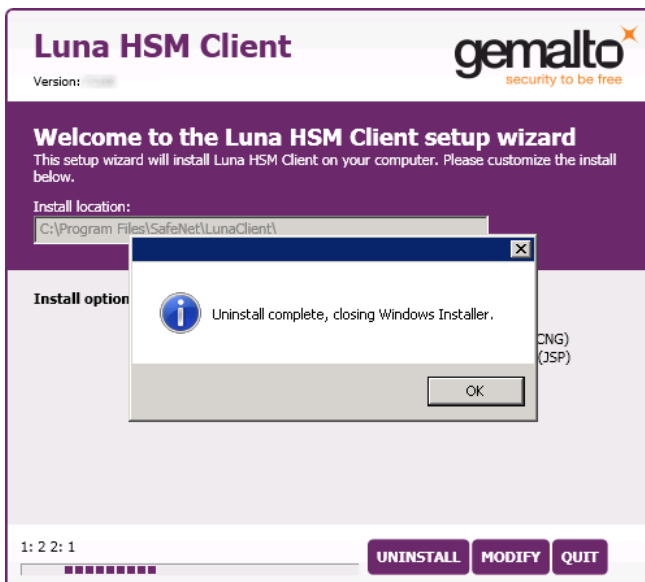
You need to uninstall Luna HSM Client before installing a new version. If you wish to modify the installation (perhaps to add a component or product that you did not previously install), you must uninstall the current installation and re-install with the desired options. If you have a Luna Backup HSM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

### To uninstall the Luna HSM Client software

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



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

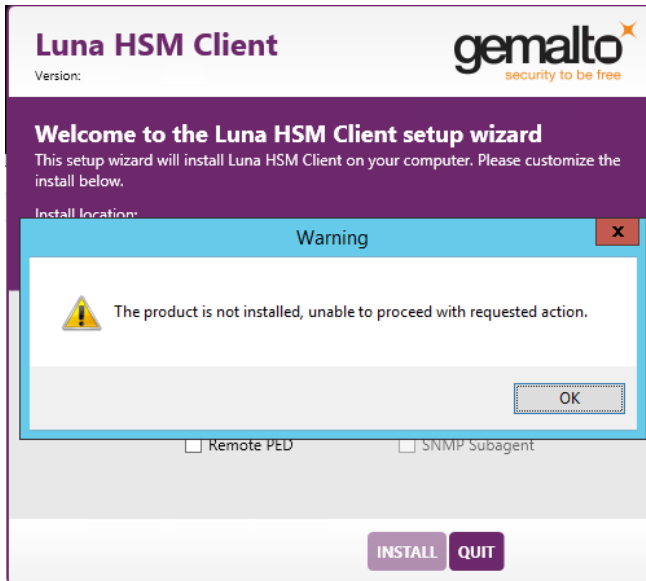


- When the uninstallation is complete, click **OK** to dismiss the operating system's confirmation dialog.

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

### Uninstall if not present

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



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

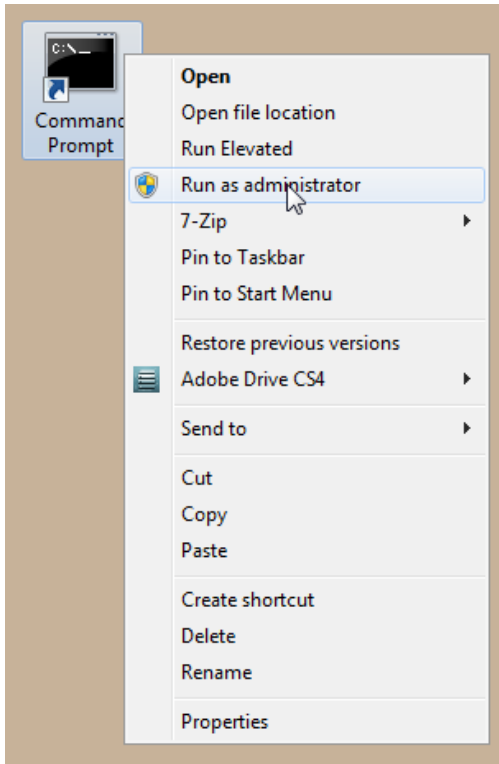
### After Installation

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

### Troubleshooting

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

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



If that option is available, then you can use the command line to move to the location of the **LunaHSMClient.exe** file and launch it there, which permits the needed services to load for PEDclient. See "[Windows Luna HSM Client Installation](#)" on page 21 for instructions on how to install the client software from the command line.

## Linux Luna HSM Client Installation

---

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

- > ["Prerequisites" below](#)
- > ["Where to install, and SELinux" on the next page](#)
- > ["About Installing the Luna HSM Client Software" on page 38](#)
- > ["Scripted or Unattended Installation" on page 40](#)
- > ["Controlling User Access to Your Attached HSMs and Partitions" on page 44](#)
- > ["Uninstalling the Luna HSM Client Software or Removing Components" on page 45](#)
- > ["Java" on page 45](#)
- > ["Interrupting the Installation" on page 41](#)
- > ["Modifying the Number of Luna Backup HSM Slots" on page 45](#)

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

### Prerequisites

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

#### CentOS 8.4 Missing Dependency

Due to a missing dependency on CentOS 8.4 [specifically the symlink (libnsl.so.1) to libnsl was removed], when installing [Luna HSM Client 10.5.0](#) or newer, you must install an additional rpm package first:

Run **yum install libnsl** before invoking the **install.sh** script.

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

On Linux, the PCIe driver module (and optionally the Backup HSM driver) is built by the client as part of the installation if you choose to install the Luna PCIe HSM 7 component or the Backup HSM. To build the driver, the client requires the following items:

- > Kernel headers for build
- > **kernel-devel** package
- > **rpmbuild** package
- > C and C++ compilers
- > **make** command
- > **libelf-dev**, **libelf-devel**, or **elfutils-libelf-devel**

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

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

For the PCIe, USB, or Backup HSM drivers to be available immediately after installation on RHEL, you must install **chkconfig** before the Luna HSM Client software. If this package is not installed, you must reboot the client computer after installing the client.

### Debian Requires alien

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

### SUSE Linux on IBM PPC

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

## Where to install, and SELinux

The instructions on this page assume that much of the installation goes into /usr. You can change that install location (see ["Flexible Install paths" on page 39](#)). There might be some interaction with SELinux that you would need to consider. Security Enhanced Linux or SELinux is a security mechanism built into the Linux kernel used by RHEL-based distributions. By default, in CentOS 8 and newer, SELinux is enabled and in enforcing mode.

SELinux adds an additional layer of security to the system by allowing administrators and users to control access to objects based on policy rules. SELinux policy rules specify how processes and users interact with each other as well as how processes and users interact with files. When there is no rule explicitly allowing access to an object, such as for a process opening a file, access is denied.

SELinux has three modes of operation:

- > Enforcing: SELinux allows access based on SELinux policy rules.
- > Permissive: SELinux only logs actions that would have been denied if running in enforcing mode. This mode is useful for debugging and creating new policy rules.
- > Disabled: No SELinux policy is loaded, and no messages are logged.

So if, for example, your non- /usr installation completes uneventfully, but pedclient errors show up in the logs, then consider setting SELinux to "Permissive" mode. Or set explicit rules that will comply with SELinux's Enforcing mode.

**NOTE MutexFolder:** For Luna clients on Linux, the callback service (CBS) employed by pedclient originally placed mutex entries in /tmp. This was fine in most cases, but could be an issue if operating system services cleared the /tmp folder, causing the cbs process to stop. The workaround was to restart the service. A solution was provided that moved the mutex folder to /var/log. However, this was found to be an issue for installations by non-root users, where the service did not have permission to write into /var/log.

Beginning with [Luna HSM Client 10.4.0](#), a chrystoki.conf entry "MutexFolder =" is added. If access to the default folder /tmp is not desired or is restricted, the MutexFolder= entry allows an administrator to specify an accessible folder.

```
Misc = {
...
    MutexFolder = /usr/lock;
}
```

However, the indicated folder must exist. If this is set to a non-existent folder, the service fails to start properly, such as in this example of logs for the cbs service:

(MutexFolder = /nosuchfolder/lock)

```
.. daemon info systemd: Starting CallBack Server...
... user notice root: cbs started.
... daemon info cbs: Starting cbs:[ OK ]#015LunaNamedSystemMutex: open()
failed: No such file or directory
... daemon info cbs: LOGGER_init failed
... daemon info cbs: Failed to initialize the logger. Exiting.
... user crit pedClient: Failed to initialize the logger. Exiting.
... daemon info systemd: Started CallBack Server.
```

## About Installing the Luna HSM Client Software

It is recommended that you refer to the [Customer Release Notes](#) for any installation-related issues or instructions before installing the client software.

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

### The installation script

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

- > interactive: **sh install.sh [-install\_directory <prefix>]**
- > all: **sh install.sh all [-install\_directory <prefix>]**
- > scriptable: **sh install.sh -p [network|pci|usb|backup|ped] [-c sdk|jsp|jcprov|snmp]]fmsdk|fm\_tools [-install\_directory </usr>]**

The options on the script are:

- > device(s)
  - **network** is the Luna Network HSM 7 (software only, no drivers)
  - **pci** is the Luna PCIe HSM 7 (software plus PCI driver)

- **usb** is the Luna USB and Backup HSMs (software plus driver for the USB-connected HSMs)
  - **backup** is software to enable Remote Backup
  - **ped** is software for the Luna Remote PED
- > components include the optional Software Development kit, Java providers, SNMP instance (not needed for Luna Network HSM 7 which has it built in), Functionality Module tools, and the Functionality Module SDK

### Install.sh syntax and options:

```
[myhost]$ sh install.sh help
```

usage:

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

```
install.sh -p [network|pci|usb|backup|ped] [-c sdk|jsp|jcprov|snmp|fmsdk|fm_tools] [-install_
directory </usr>]
```

```
-p <list of Luna products>
-c <list of Luna components|all> - Optional. Default components are installed if not provided
-install_directory <Defaults to /usr> - Optional. Sets the installation directory prefix.
Non-root install is restricted to installation of Luna Network HSM
product and Luna SDK, Luna JSP (Java) and Luna JC PROV (Java) components.
```

Luna products options

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

Luna components options

```
sdk      - Luna SDK
jsp      - Luna JSP (Java) --> Luna Network HSM, Luna PCIe HSM and Luna USB HSM default
component
jcprov   - Luna JC PROV (Java) --> Luna Network HSM, Luna PCIe HSM and Luna USB HSM default
component
snmp     - Luna SNMP subagent
```

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

### Flexible Install paths

An administrative (root) user, in charge of installing and uninstalling the software, has access wherever the installed material eventually resides. However, the operational, application-level use of Luna HSM Client might be assigned to a non-root user with constrained access and privileges. That non-root user might be a person or a departmental function or an application. By changing the install path to (for example)

**%home/bigapplication/safenet/luna** you allow that non-root user access to tools and files for connecting to the HSM and using HSM partitions.

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

The prefix, or major location is your choice, and replaces the /usr default portion. (See mention of SELinux, earlier on this page)

**NOTE** Avoid the use of space characters in directory names.

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

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

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

**TIP** Thales recommends verifying the integrity of the Luna HSM Client packages, by calculating their SHA256 hash values and comparing with the hash values posted on the Support Portal, before installing them on your client machines.

You can use the `sha256sum` tool on Linux machines to calculate the SHA256 hash values.

## Scripted or Unattended Installation

If you prefer to provide all installation options from the command-line (script), rather than interactively, do the following.

### To install the Luna HSM Client software in non-interactive or scripted fashion on a Linux workstation

1. Ensure that you have **sudo** privileges on the client workstation.
2. Access the installation software:  
Copy or move the **.tar** archive to a suitable directory where you can untar the archive and extract the contents:  
**tar xvf <filename>.tar**
3. Go to the untarred directory for your operating system (**32** or **64**-bit):  
**cd /<untarred\_dir>/<32/64>**
4. To see the syntax and all available options, run the command with **help**
5. To install the software, run the **install.sh** installation script with the options **-p** <list of Luna products> and **-c** <list of Luna components>.

```
install.sh -p [network|pci|usb|backup|ped] [-c sdk|jsp|jcprov|snmp|fmsdk|fm_tools] [-install_directory </usr>]
```

Be sure to include the **-install\_directory** option.

**NOTE** Following the "-c" option, you can provide a space-separated list of components to include in the installation. If JSP and JCProv are not explicitly listed, they are installed by default, but if one is explicitly listed, then only the listed component is included.

If the SNMP component is selected, it works with Luna PCIe HSM, Luna USB HSM, and Luna Backup HSM products only.

Following the "-p" option, you can provide a space-separated list of HSM products to include in the installation.

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

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

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

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

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

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

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

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

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

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

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

## Interrupting the Installation

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

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

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

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

1. Ensure that you have **sudo** privileges on the client workstation.
2. Access the installation software:  
Copy or move the **.tar** archive to a suitable directory where you can untar the archive and extract the contents:  
**tar xvf <filename>.tar**
3. Go to the untarred directory for your operating system (**32** or **64**-bit):  
**cd /<untarred\_dir>/<32/64>**
4. To install the software, run the **install.sh** installation script. You can run the script in interactive mode, or you can script the installation, as described in ["Scripted or Unattended Installation" on page 40](#).
  - To display the help, or a list of available installer options, type:  
**sudo sh install.sh -? or sudo sh install.sh help**
  - To install all available products and optional components, type:  
**sudo sh install.sh all**
  - To selectively install individual products and optional components, type the command without arguments:  
**sudo sh install.sh**

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

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

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

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

```
*[1]: Luna Network HSM
```

```
[2]: Luna PCIe HSM
```

```
*[3]: Luna USB HSM
```

```
[4]: Luna Backup HSM
```

```
[5]: Luna Remote PED
```

```
[N|n]: Next
```

```
[Q|q]: Quit
```

```
Enter selection: 4
```

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

Advanced

Choose Luna Components to be installed

```
[1]: Luna SDK

[2]: Luna JSP (Java)

[3]: Luna JCPProv (Java)

[4]: Luna SNMP subagent

[5]: Luna Functionality Module Tools

[6]: Luna Functionality Module Software Development Kit

[B|b]: Back to Products selection

[I|i]: Install

[Q|q]: Quit
```

Enter selection:

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

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

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

8. The system installs all packages related to the products and any optional components that you selected.
9. [Optional] For easy use of the Luna HSM Client tools, add their directories to the \$PATH.
  - a. Edit your system's **bash\_profile** file using an editing tool.
 

```
vi ~/.bash_profile
```
  - b. Add the following lines to the end of the file:
 

```
export PATH="$PATH:/usr/safenet/lunaclient/bin"
export PATH="$PATH:/usr/safenet/lunaclient/sbin"
```
  - c. Source the updated **bash\_profile**.
 

```
source ~/.bash_profile
```

## Controlling User Access to Your Attached HSMs and Partitions

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

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

**TIP** Users on your system that are not members of **hsmusers** group are not able to see the slots/partitions when using lunacm, other Luna tools, or your applications. If you open lunacm, expecting to see one or more slots, and none are visible, check that your current user is a member of **hsmusers** before doing other troubleshooting.

### Adding users to hsmusers group

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

#### To add a user to hsmusers group

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

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

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

### Removing users from hsmusers group

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

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

#### To remove a user from hsmusers group

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

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

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

## Uninstalling the Luna HSM Client Software or Removing Components

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

### To uninstall the client software

1. Ensure that you have **sudo** privileges on the client workstation.
2. Go to the client installation directory:  
**cd /usr/safenet/lunaclient/bin**
3. Run the uninstall script:  
**sudo sh uninstall.sh**

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

### To remove individual components

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

## Java

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

## Modifying the Number of Luna Backup HSM Slots

By default, the Luna HSM Client allows for three slots reserved for each model of Luna Backup HSM. You can edit **Chrystoki.conf** to modify the number of reserved slots. See also ["Configuration File Summary" on page 51](#).

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

1. Navigate to the **Chrystoki.conf** file and open in a text editor.
2. Add the following line(s) to the **CardReader** section of the file:
  - For Luna Backup HSM G5:  
**LunaG5Slots = <value>;**
  - For Luna Backup HSM 7:  
**LunaG7Slots = <value>;**

## Effects of Kernel Upgrades

If you upgrade the Linux kernel after successful installation of Luna HSM Client, then you must install the kernel-headers for the new kernel and build the UHD, K6 and K7 drivers again for the new kernel. The new kernel takes effect after reboot.

### To update the kernel and then bring the system back to readiness:

1. Install development tools if not already installed.
2. Update kernel if needed.
3. Reboot.
4. Install kernel-headers for the new kernel, example: **yum install kernel-headers-\$(uname -r)**
5. Rebuild the drivers for the new kernel: **rpmbuild --rebuild uhd-7.3.0-165.src**  
Do the same for k6 and k7 drivers.

## Troubleshooting

**Problem #1A:** No slots visible for Luna Network HSM 7 = user can't read certs directory.

**Problem #1B:** No slots visible for Luna PCIe HSM 7 or Luna USB HSM 7 = user can't read device (/dev/k7pf0, /dev/viper0, or /dev/lunauhd0).

**Solution:** You might have left a user out of **hsmusers** group, or you might have set an overly restrictive umask.

**Problem #2:** You receive the following error: **./setenv:24: = not found**

**Solution:** The setenv command is only supported while using bash.

## Adding a Luna Cloud HSM Service

Luna HSM Client allows you to use both Luna partitions and Thales Data Protection on Demand (DPoD) Luna Cloud HSM services. Using a single client workstation, you can back up or migrate your keys between Luna and the Luna Cloud HSM service, or combine partitions and services into an HA group.

**NOTE** Refer to the [Luna HSM Client Releases](#) for supported client versions. Thales recommends keeping your Luna HSM Client software updated to the latest version, especially if your deployment includes Luna Cloud HSM.

### Prerequisites

- > If Luna HSM Client is not installed at the default location, the **ChrystokiConfigurationPath** must be set for the Luna Cloud HSM service to use the correct location.
- > DPoD Luna Cloud HSM services support Windows and Linux operating systems only. This procedure presumes that you have already set up Luna HSM Client on your Windows or Linux workstation:
  - ["Windows Luna HSM Client Installation" on page 21](#)
  - ["Windows Interactive Luna HSM Client Installation" on page 28](#)
  - ["Linux Luna HSM Client Installation" on page 36](#)

- > For more information on Luna/Luna Cloud HSM service compatibility, refer to [Cloning Keys Between Luna 6, Luna 7, and Luna Cloud HSM](#).

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

1. After purchasing a Luna Cloud HSM service, refer to the [DPoD Luna Cloud HSM documentation](#) for instructions on downloading the Luna Cloud HSM service client. Transfer the zip file to your workstation using **pscp**, **scp**, or other secure means.
2. Extract the zip file into a directory on your client workstation.
3. Extract or untar the appropriate client package for your operating system. Do not extract to a new subdirectory; place the files in the Luna Cloud HSM service client install directory. The other client package can be safely deleted.

- [Windows] **cvclient-min.zip**
- [Linux] **cvclient-min.tar**

# **tar -xvf cvclient-min.tar**

Run the provided **setenv** script to automatically copy the necessary Luna Cloud HSM service configuration entries to the existing Luna HSM Client configuration file. The existing Luna HSM Client configuration file must be writable to execute **setenv**.

**CAUTION!** Running **setenv** will overwrite any existing Luna Cloud HSM service configurations in the Luna HSM Client configuration file.

**NOTE** If Luna HSM Client is not installed in the default directory, or if **setenv** was run previously, you must clear the **ChrystokiConfigurationPath** environment variable or update it to point to the location of the correct configuration file:

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

# **export ChrystokiConfigurationPath=/etc/**

- [Windows **cmd** prompt] Open a command prompt as **Administrator** and run the script with the **-addcloudhsm** option.  
 > **.\setenv.cmd -addcloudhsm**
  - [Linux] Source the **setenv** script with the **--addcloudhsm** option.  
 # **source ./setenv --addcloudhsm**
4. Launch or relaunch LunaCM to verify that both your Luna partitions and Luna Cloud HSM service are available. Once the Luna Cloud HSM service has been added to the Luna HSM Client, you can delete the client package downloaded from Thales DPoD.

## Initializing a Luna Cloud HSM Service

You must now initialize the Luna Cloud HSM service for use with your existing Luna partitions. If your Luna HSMs are password-authenticated, the cloning domain you set on the Luna Cloud HSM service must match the partition(s) with which it will share keys.

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

If you will be using the Luna Cloud HSM service with multifactor quorum-authenticated Luna partitions, LunaCM provides the option to import the credential from a red domain iKey to Luna Cloud HSM, as described below.

**NOTE** This feature requires minimum [Luna HSM Client 10.4.1](#), and is available for Luna Cloud HSM only. For cloning between password- and multifactor quorum-authenticated Luna HSMs, see [Universal Cloning](#).

### Prerequisites

- > The uninitialized Luna Cloud HSM service must be available in LunaCM on a client computer with [Luna HSM Client 10.4.1](#) or newer installed.
- > The client computer must have the Luna PED driver installed:
  - Windows:** ["Modifying the Installed Windows Luna HSM Client Software" on page 31](#) (**Remote PED** package)
  - Linux:** ["About Installing the Luna HSM Client Software" on page 38](#) ([5] **Luna Remote PED** package or **-p ped** in scripted installation)
- > Connect a Luna PED to the client computer and set it to **Local PED-USB** mode.
- > If you were previously using this client computer as a Remote PED server, you must stop PEDserver before continuing:
  - pedserver -mode stop**
- > If your Luna partition domain uses an M of N iKey scheme, ensure that you have enough keys on hand to provide the M of N quorum.

### To initialize a Luna Cloud HSM service using an imported domain secret

1. Launch LunaCM on the client computer.
2. Set the active slot to the uninitialized Luna Cloud HSM service.
 

```
lunacm:> slot set -slot <slot#>
```
3. Initialize the Luna Cloud HSM service, specifying an identifying label and including the **-importpeddomain** option.
 

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

Follow the prompts in LunaCM and on the Luna PED to import the domain secret and complete the initialization process.

**CAUTION!** HA failover from multifactor quorum-authenticated Luna partitions to Luna Cloud HSM requires minimum [Luna HSM Client 10.5.0](#). Refer to known issue [LUNA-23945](#).

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

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

- > [Cloning Objects to Another Application Partition](#)
- > [Partition Backup and Restore](#)
- > [Configuring a High-Availability Group](#)

## Dynamic Partition Loading for Luna Cloud HSM Services

[Luna HSM Client 10.5.0](#) and newer provide access to dynamic partition loading for Luna Cloud HSM services. Dynamic partition loading allows you to add additional sets of client UserIDs (combination of unique AuthTokenClientID, AuthTokenClientSecret, AuthTokenConfigURI) to the crystoki.conf or Chrystoki.ini file and automatically access the added partitions without restarting LunaCM or impacting other applications using LunaCM. Deleted partitions will not be removed from the LunaCM list until you restart LunaCM.

The default maximum number of users that can be added to a crystoki.conf or Chrystoki.ini file is 100. For more information about configuring the maximum number of client UserIDs see MaxUserIDCount in the ["Configuration File Summary"](#) on page 51.

**NOTE** Dynamic Partition Loading using mixed FIPS mode partitions may show incorrect results for the HSM operation mode of each partition.

### Prerequisites

- > [Luna HSM Client 10.5.0](#) or newer
  - An HSM client downloaded from the Thales Support Portal. If using an HSM client this procedure assumes that you have already set up your HSM client on your Windows or Linux workstation. In addition, this procedure requires the REST and XTC sections of the Luna Cloud HSM service be available in the client configuration file. See ["Adding a Luna Cloud HSM Service"](#) on page 46 for more information about adding your first Luna Cloud HSM service and the necessary configuration file entries to an existing HSM client.
    - ["Windows Interactive Luna HSM Client Installation"](#) on page 28
    - ["Linux Luna HSM Client Installation"](#) on page 36
  - A minimal client downloaded from Thales Data Protection on Demand.
- > A Luna Cloud HSM service partition to load dynamically.
- > If HSM client is not installed at the default location, the ChrystokiConfigurationPath must be set for the Luna Cloud HSM service to use the correct location.

## To dynamically load a partition

1. Open the client configuration file (the Chrystoki.conf (Linux) or crystoki.ini/crystoki-template.ini (Windows)), for the HSM client that you are adding the Luna Cloud HSM service partition to, in a text editor.
2. In the REST section, add the client UserID values for the new partition. Append the client UserID values with a unique numerical value to associate the client UserID values with each other.

**TIP** The client UserID values can be accessed from the Chrystoki.conf (Linux) or crystoki.ini/crystoki-template.ini (Windows) configuration files included in the Luna Cloud HSM service client package.

### Linux example:

```
REST = {
AuthTokenConfigURI=*****
AuthTokenClientId=*****
AuthTokenClientSecret=*****
AuthTokenConfigURI2=*****
AuthTokenClientId2=*****
AuthTokenClientSecret2=*****
AuthTokenConfigURI3=*****
AuthTokenClientId3=*****
AuthTokenClientSecret3=*****
RestClient=1
ClientTimeoutSec=120
ClientPoolSize=32
ClientEofRetryCount=15
ClientConnectRetryCount=900
ClientConnectIntervalMs=1000
PartitionData00=1334054167371, na.hsm.dpondemand.io, 443
SSLClientSideVerifyFile=.\server-certificate.pem;
}
```

### Windows example:

```
[REST]
AuthTokenConfigURI=*****
AuthTokenClientId=*****
AuthTokenClientSecret=*****
AuthTokenConfigURI2=*****
AuthTokenClientId2=*****
AuthTokenClientSecret2=*****
AuthTokenConfigURI3=*****
AuthTokenClientId3=*****
AuthTokenClientSecret3=*****
RestClient=1
ClientTimeoutSec=120
ClientPoolSize=32
ClientEofRetryCount=15
ClientConnectRetryCount=900
ClientConnectIntervalMs=1000
PartitionData00=1334054167371, na.hsm.dpondemand.io, 443
SSLClientSideVerifyFile=.\server-certificate.pem;
```

3. Execute the "slot list" command in LunaCM to display the additional partitions.

**TIP** Additional sets of client UserIDs can be exported and secured as described in "Configuration File Summary" below.

## Configuration File Summary

The Luna HSM Client software installation includes a configuration file that controls many aspects of client operation. The fields in the configuration file are used to alter the default behavior of the library. So the default value is the value that would result in the normal (non-altered) behavior (but see TIP below). The configuration file can be found in the following default locations:

### > Luna HSM Client

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

### > Luna Cloud HSM

- Windows: <service\_client\_path>\crystoki.ini
- Linux: <service\_client\_path>/Chrystoki.conf

**NOTE** The crystoki.ini and Chrystoki.conf files included with the Luna Cloud HSM service client provide a default set of configuration options.

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

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

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

**TIP Configuration settings and Section Headings**

Some of the sections and entries listed here do not appear in the base configuration file as you would receive it via download; in many use-cases, your application's employment of the HSM would not require any direct intervention in the configuration file. "Factory" settings would be sufficient. If an application would benefit from a setting that differs from the stock values, and a visible entry is not already in the configuration file on your host system, then you must add a relevant entry in order to change the behavior described in the table below.

- > If the configuration file contains no explicit entries that would reside under a particular heading, then the heading itself would also not be present.
- > If you intend to add a setting to the file, and there is no pre-existing section-heading for it, then create a heading as indicated in the table, below, following the format of the other sections in your config file, appropriate for the host operating system (Linux/UNIX or Windows).

The majority of fields are Boolean (true/false or 0/1), or a range of values.

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

**Exceptions:**

- > If an explicit location is not set for the library location (which is normally inserted as part of installation if you use the Client installer), or if you moved the library after a path value was included, an error message is generated about the field/path/file not being found, and you must provide a proper library location in order to proceed.
- > If you intend to use an NTLS connection (Luna Network HSM 7) or an XTC connection (Luna Cloud HSM), then the relevant settings must be present to define that connection, or the connection does not take place.

**Do not edit the Chrystoki.conf or crystoki.ini file unless you need to do so.** If you need to edit, refer to the guidance in the table below, and ask for help from our technical support engineers if this document is not sufficient.

Section/Setting	Description
<b>Chrystoki2</b>	
LibNT	Path to the Chrystoki2 library on Windows operating systems. <b>Default: C:\Program Files\SafeNet\LunaClient\cryptoki.dll</b>

Section/Setting	Description
LibNT32	<p>Path to the Chrystoki2 library on 32-bit Windows systems only.</p> <p><b>Default:</b> <code>C:\Program Files\SafeNet\LunaClient\win32\libCryptoki2.dll</code></p> <div> <p><b>NOTE</b> Luna HSM Client 10.1.0 and newer includes libraries for 64-bit operating systems only.</p> </div>
LibUNIX64	<p>Path to the Chrystoki2 library on 64-bit Linux/UNIX operating systems.</p> <p><b>Default:</b></p> <ul style="list-style-type: none"> <li>&gt; <b>Linux/AIX:</b> <code>/usr/safenet/lunaclient/libs/64/libCryptoki2_64.so</code></li> <li>&gt; <b>Solaris:</b> <code>/opt/safenet/lunaclient/libs/64/libCryptoki2_64.so</code></li> </ul>
<b>Luna (see * below this table)</b>	
CloningCommandTimeout	<p>The amount of time (in milliseconds) the library allows for the HSM to respond to a cloning command.</p> <p><b>Default: 300000</b></p>
CommandTimeoutPedSet	<p>This is an exception to DefaultTimeout (below). It defines the time (in milliseconds) allowed for all PED-related HSM commands. PED-related commands can take longer than ordinary commands governed by DefaultTimeout.</p> <p>Generally, the following formula applies:  <math>\text{CommandTimeOutPedSet} = \text{DefaultTimeOut} + \text{PEDTimeout1} + \text{PEDTimeout2} + \text{PEDTimeout3}</math></p> <p><b>Default: 720000</b></p>
DefaultTimeOut	<p>Defines the time (in milliseconds) the HSM driver in the host system waits for HSM commands to return a result. If a result is not returned in that time, the driver halts the HSM and returns <code>DEVICE_ERROR</code> to all applications using the HSM. The only exceptions are when a command's timeout is hard-coded in the Cryptoki library, or the command falls into a class governed by one of the other timeout intervals described elsewhere in this section.</p> <p><b>Default: 500000</b></p>
DomainParamTimeout	<p>Timeout (in milliseconds) for Domain Parameter Generation.</p> <p><b>Default: 5400000</b></p>

Section/Setting	Description
KeypairGenTimeOut	<p>Defines the time (in milliseconds) the library waits for a keypair generation operation to return a value. The randomization component of keypair generation can cause large keypairs to take a long time to generate, and this setting keeps the attempts within a reasonable time. You can change this value to manage your preferred balance between long waits and the inconvenience of restarting a keygen operation.</p> <p><b>Default: 2700000</b></p>
PEDTimeout1	<p>Defines the time (in milliseconds) the HSM attempts to ping the PED before sending a PED operation request. If the PED is unreachable, the HSM returns a code indicating that the PED is not connected.</p> <p><b>Default: 100000</b></p>
PEDTimeout2	<p>Defines the time (in milliseconds) that the HSM waits for the local PED to respond to a PED operation request. If the local PED does not respond to the request within the span of PEDTimeout2, the HSM returns an appropriate result code (such as PED_TIMEOUT). This is the timeout you might increase from the Default value if you were initializing larger MofN PED Key sets - the HSM allows M and N to each be up to 16 splits - maybe applying PED PINS, and making a duplicate set as well.</p> <p><b>Default: 200000</b></p>
PEDTimeout3	<p>Defines the additional time (in milliseconds) the HSM waits for a remote PED to respond to a PED operation request. Therefore, the actual time the firmware waits for a remote PED response is PEDTimeout2 + PEDTimeout3.</p> <p><b>Default: 20000</b></p>
<b>CardReader</b>	
LunaG5Slots	<p>Number of Luna Backup HSM G5 slots reserved so that the library will check for connected devices.</p> <p><b>Valid Values:</b></p> <ul style="list-style-type: none"> <li>&gt; <b>0:</b> If you have no Luna Backup HSM G5s and wish to eliminate the reserved spaces in your slot list, use this setting.</li> <li>&gt; <b>1-N:</b> Can be set to any number, but is effectively limited by the number of external USB devices supported by your client workstation.</li> </ul> <p><b>Default: 3</b></p>

Section/Setting	Description
LunaG7Slots	<p>Number of Luna Backup HSM 7 slots reserved so that the library will check for connected devices.</p> <p><b>Valid Values:</b></p> <ul style="list-style-type: none"> <li>&gt; <b>0:</b> If you have no Luna Backup HSM 7s and wish to eliminate the reserved spaces in your slot list, use this setting.</li> <li>&gt; <b>1-N:</b> Can be set to any number, but is effectively limited by the number of external USB devices supported by your client workstation.</li> </ul> <p><b>Default: 3</b></p>
RemoteCommand	<p>This setting was used when debugging older Luna products. For modern products it is ignored.</p> <p><b>Valid Values:</b></p> <ul style="list-style-type: none"> <li>&gt; <b>0:</b> false</li> <li>&gt; <b>1 (default):</b> true</li> </ul>
CKLog2	
<p><b>NOTE</b> See <a href="#">Using CKlog</a>. Config is done using the <b>vtl</b> utility or by editing this config file directly.</p>	
RBS	<p><b>NOTE</b> RBS is not supported with Luna Cloud HSM services.</p>
CmdProcessor	<p>The location of the RBS library.</p> <p><b>Default:</b></p> <ul style="list-style-type: none"> <li>&gt; <b>Windows:</b> C:\Program Files\SafeNet\LunaClient\rbs_processor2.dll</li> <li>&gt; <b>Linux/AIX:</b> /usr/safenet/lunaclient/rbs/lib/librbs_processor2.dll</li> <li>&gt; <b>Solaris:</b> /opt/safenet/lunaclient/rbs/lib/librbs_processor2.dll</li> </ul>
HostPort	<p>The port number used by the RBS server.</p> <p><b>Valid Values:</b> any unassigned port</p> <p><b>Default: 1792</b></p>

Section/Setting	Description
ClientAuthFile	<p>The location of the RBS Client authentication file.</p> <p><b>Default:</b></p> <ul style="list-style-type: none"> <li>&gt; <b>Windows:</b> C:\Program Files\SafeNet\LunaClient\config\clientauth.dat</li> <li>&gt; <b>Linux/AIX:</b> /usr/safenet/lunaclient/rbs/clientauth.dat</li> <li>&gt; <b>Solaris:</b> /opt/safenet/lunaclient/rbs/clientauth.dat</li> </ul>
ServerSSLConfigFile	<p>The location of the OpenSSL configuration file used by RBS Server or Client.</p> <p><b>Default:</b></p> <ul style="list-style-type: none"> <li>&gt; <b>Windows:</b> C:\Program Files\SafeNet\LunaClient\rbs\server.cnf</li> <li>&gt; <b>Linux/AIX:</b> /usr/safenet/lunaclient/rbs/server/server.cnf</li> <li>&gt; <b>Solaris:</b> /opt/safenet/lunaclient/rbs/server/server.cnf</li> </ul>
ServerPrivKeyFile	<p>The location of the RBS Server certificate private key file.</p> <p><b>Default:</b></p> <ul style="list-style-type: none"> <li>&gt; <b>Windows:</b> C:\Program Files\SafeNet\LunaClient\cert\server\serverkey.pem</li> <li>&gt; <b>Linux/AIX:</b> /usr/safenet/lunaclient/rbs/server/serverkey.pem</li> <li>&gt; <b>Solaris:</b> /opt/safenet/lunaclient/rbs/server/serverkey.pem</li> </ul>
ServerCertFile	<p>The location of the RBS Server certificate file.</p> <p><b>Default:</b></p> <ul style="list-style-type: none"> <li>&gt; <b>Windows:</b> C:\Program Files\SafeNet\LunaClient\cert\server\server.pem</li> <li>&gt; <b>Linux/AIX:</b> /usr/safenet/lunaclient/rbs/server/server.pem</li> <li>&gt; <b>Solaris:</b> /opt/safenet/lunaclient/rbs/server/server.pem</li> </ul>
NetServer	<p>Determines whether RBS acts as a server or client.</p> <p><b>Valid Values:</b></p> <ul style="list-style-type: none"> <li>&gt; <b>0:</b> Client</li> <li>&gt; <b>1 (default):</b> Server</li> </ul>

Section/Setting	Description
HostName	The hostname or IP address that the RBS server will listen on. <b>Valid Value:</b> any hostname or IP address <b>Default:</b> 0.0.0.0 (any IP on the local host)
Available	Lists the serial numbers of Luna Backup HSMs available on the RBS server.
<b>LunaSA Client</b>	
ReceiveTimeout	Time in milliseconds before a receive timeout. <b>Default:</b> 20000
SSLConfigFile	Location of the OpenSSL configuration file. <b>Default:</b> <ul style="list-style-type: none"> <li>&gt; <b>Windows:</b> C:\Program Files\SafeNet\LunaClient\openssl.cnf</li> <li>&gt; <b>Linux/AIX:</b> /usr/safenet/lunaclient/bin/openssl.cnf</li> <li>&gt; <b>Solaris:</b> /opt/safenet/lunaclient/bin/openssl.cnf</li> </ul>
ClientPrivKeyFile	Location of the client private key. This value is set by <b>vtl</b> or <b>lunacm</b> :> <b>clientconfig deploy</b> . <b>Default:</b> <ul style="list-style-type: none"> <li>&gt; <b>Windows:</b> C:\Program Files\SafeNet\LunaClient\cert\client\ &lt;ClientName&gt;<b>Key.pem</b></li> <li>&gt; <b>Linux/AIX:</b> /usr/safenet/lunaclient/cert/client/ &lt;ClientName&gt;<b>Key.pem</b></li> <li>&gt; <b>Solaris:</b> /opt/safenet/lunaclient/cert/client/ &lt;ClientName&gt;<b>Key.pem</b></li> </ul>

Section/Setting	Description
ClientCertFile	<p>Location of the client certificate that is uploaded to Luna Network HSM 7 for NTLS. This value is set by <b>vtl</b> or <b>lunacm</b>:&gt; <b>clientconfig deploy</b>.</p> <p><b>Default:</b></p> <ul style="list-style-type: none"> <li>&gt; <b>Windows:</b> C:\Program Files\SafeNet\LunaClient\cert\client\ &lt;ClientName&gt;Cert.pem</li> <li>&gt; <b>Linux/AIX:</b> /usr/safenet/lunaclient/cert/client/ &lt;ClientName&gt;Cert.pem</li> <li>&gt; <b>Solaris:</b> /opt/safenet/lunaclient/cert/client/ &lt;ClientName&gt;Cert.pem</li> </ul>
LNHServerKeepAliveTimer##	<p>Set the keepalive timer (in milliseconds) for connections to the cluster, specified by ## (refer to "LNHServer##" on the next page).</p> <p><b>Valid Range: 10000-50000</b></p> <p><b>Default: 30000</b></p> <div style="border: 1px solid black; padding: 5px; margin-top: 10px;"> <p><b>NOTE</b> This feature requires Luna HSM Client 10.5.2 or newer, and the <b>cluster</b> package (1.0.2) included with Luna Network HSM 7 Appliance Software 7.8.2 or newer.</p> </div>
LNHServerLoadBalancingMode##	<p>Selects the load-balancing mode the client will use to distribute requests among the members of the cluster, specified by ## (refer to "LNHServer##" on the next page).</p> <p><b>Valid Values:</b></p> <ul style="list-style-type: none"> <li>&gt; <b>pick_first</b> (default): Operation requests are sent to the first cluster member where a connection can be successfully made.</li> <li>&gt; <b>round_robin</b>: Connections are made to all active members, and operation requests are distributed to each active member in turn.</li> </ul> <div style="border: 1px solid black; padding: 5px; margin-top: 10px;"> <p><b>NOTE</b> This feature requires Luna HSM Client 10.5.2 or newer, and the <b>cluster</b> package (1.0.2) included with Luna Network HSM 7 Appliance Software 7.8.2 or newer.</p> </div>

Section/Setting	Description
ServerCAFile	<p>Location of the server certificate file on the client workstation. This value is set by <b>vtl</b> or lunacm:&gt; <b>clientconfig deploy</b>.</p> <p><b>Default:</b></p> <ul style="list-style-type: none"> <li>&gt; <b>Windows:</b> C:\Program Files\SafeNet\LunaClient\cert\server\CAFile.pem</li> <li>&gt; <b>Linux/AIX:</b> /usr/safenet/lunaclient/cert/server/CAFile.pem</li> <li>&gt; <b>Solaris:</b> /opt/safenet/lunaclient/cert/server/CAFile.pem</li> </ul>
NetClient	<p>Determines whether the library searches for network slots.</p> <p><b>Valid Values:</b></p> <ul style="list-style-type: none"> <li>&gt; <b>0:</b> The library does not search for network slots.</li> <li>&gt; <b>1 (default):</b> The library searches for network slots.</li> </ul>
TCPKeepAlive	<p>TCPKeepAlive is a TCP stack option, available at the Luna HSM Client and the Luna Network HSM 7 appliance. It is controlled via an entry in the Luna HSM Client configuration file, and an equivalent file on the Luna Network HSM 7.</p> <p>The settings at the appliance and the client are independent. This allows a level of assurance, in case (for example) a firewall setting blocks communication in one direction.</p> <p><b>Valid Values:</b></p> <ul style="list-style-type: none"> <li>&gt; <b>0:</b> false</li> <li>&gt; <b>1 (default):</b> true</li> </ul>
ServerName##	<p>These entries identify NTLS-linked Luna Network HSM 7 servers/ports, and determines the order in which they are polled to create a slot list. These values are set by <b>vtl</b> or lunacm:&gt; <b>clientconfig deploy</b>.</p>
ServerPort##	
LNHServer##	The IP address and port of a Luna Network HSM 7 cluster member connected to this client.
LNHServerClientCert##	The location and filename of the Luna HSM Client certificate used to access this Luna Network HSM 7 cluster.
LNHServerClientKey##	The location and filename of the Luna HSM Client private key used to access this Luna Network HSM 7 cluster.
LNHServerCAFile##	The location and filename of the Luna Network HSM 7 cluster server certificate.

Section/Setting	Description
LNHServerCN##	The Common Name for the cluster certificate.
LNHStandbyServer##	<p>Reports the affinity group the client is directing traffic to. See <a href="#">Moving a Member to a Different Affinity Group</a>.</p> <div> <p><b>NOTE</b> This feature requires Luna HSM Client 10.5.2 or newer, and the <b>cluster</b> package (1.0.2) included with Luna Network HSM 7 Appliance Software 7.8.2 or newer.</p> </div>
<b>Presentation</b>	<p><b>NOTE</b> This section is not created automatically. To change any of the following values, you must first create this section in the configuration file.</p>
OneBaseSlotId	<p>Determines whether slot listing begins at <b>0</b> or <b>1</b>.</p> <p><b>Default: 0</b></p>
ShowAdminTokens	<p>Determines whether the Admin partitions of locally-installed Luna PCIe HSM 7s are visible in the slot list.</p> <p><b>Valid Values:</b></p> <ul style="list-style-type: none"> <li>&gt; <b>no</b>: Admin slots are hidden.</li> <li>&gt; <b>yes</b> (default): Admin slots are visible.</li> </ul>
ShowEmptySlots	<p>Determines whether slot numbers are reserved for partitions that have not yet been created on the HSM. When this setting is enabled, slot numbers remain consistent over time, even when new partitions are created.</p> <p><b>Valid Values:</b></p> <ul style="list-style-type: none"> <li>&gt; <b>no</b> (default): Only existing partitions are assigned slot numbers.</li> <li>&gt; <b>yes</b>: Slot numbers are reserved for the maximum number of partitions that can be created on HSMs connected to the client.</li> </ul> <div> <p><b>NOTE</b> This does not apply to Luna Network HSM 7 partitions assigned to the client, which will always appear in the lowest-numbered slots, causing locally-connected and Luna Cloud HSM service slots to increment higher.</p> </div>

Section/Setting	Description
ShowUserSlots	<p>Allows you to set permanent slot numbers for specific partitions. If you use this setting, you must specify a slot for all partitions on a specific HSM, or the partitions not listed here will not be visible to the client.</p> <p><b>Valid Values:</b> Comma-delimited list in the format &lt;slotnum&gt;(&lt;serialnum&gt;)</p> <p><b>Example:</b>  <b>ShowUserSlots=1(351970018022),2(351970018021),3(351970018020),...</b></p>
VirtualToken	<p><b>NOTE</b> This section is created only if the HA auto-recovery mode is set to <b>activeEnhanced</b>. See <a href="#">Configuring HA Auto-Recovery</a>.</p>
VirtualToken##Label	<p>The label of the HA group.</p> <p>This value is set by using the lunacm:&gt; <a href="#">hagroup creategroup</a> command to set up an HA group. See <a href="#">Configuring a High-Availability Group</a>.</p>
VirtualToken##SN	<p>The pseudo serial number of the HA group.</p> <p>This value is set by using the lunacm:&gt; <a href="#">hagroup creategroup</a> command to set up an HA group. See <a href="#">Configuring a High-Availability Group</a>.</p>
VirtualToken##Members	<p>The serial number of the HA group members.</p> <p>This value is set by using the lunacm:&gt; <a href="#">hagroup addmember</a> command to add a member to the HA group. See <a href="#">Configuring a High-Availability Group</a>.</p>
VirtualTokenActiveRecovery	<p>The HA auto-recovery mode.</p> <p>This value is set by using the lunacm:&gt; <a href="#">hagroup recoverymode</a> command to configure the HA auto-recovery mode. See <a href="#">Configuring HA Auto-Recovery</a>.</p>
<b>HAConfiguration</b>	
AutoReconnectInterval	<p>Specifies the interval (in seconds) at which the library will attempt to reconnect with a missing HA member, until the set number of attempts is reached. This value is set using lunacm:&gt; <a href="#">hagroup interval</a>.</p> <p><b>Valid Values:</b></p> <ul style="list-style-type: none"> <li>&gt; <b>60-1200:</b> Wait the specified number of seconds between reconnection attempts.</li> </ul> <p><b>Default: 60</b> seconds</p>

Section/Setting	Description
HAOnly	<p>Determines whether individual HA member slots are visible to client applications. Hiding individual members helps prevent synchronization errors by preventing applications from directing calls to individual member partitions. If a member partition fails, the other slots in the system change, which can cause applications to send calls to the wrong slot number. This setting prevents this by hiding all physical slots from applications.</p> <p><b>Valid Values:</b></p> <ul style="list-style-type: none"> <li>&gt; <b>0</b> (default): All partitions are visible to applications as slots.</li> <li>&gt; <b>1</b>: Only HA virtual slots are visible to applications.</li> </ul> <div style="border: 1px solid #ccc; padding: 10px; margin-top: 10px;"> <p><b>NOTE</b> This setting does not affect how slots are numbered in LunaCM; you can still configure individual member partitions with HAOnly mode enabled.</p> </div>
ProbeTimeout	<p>By default, if the HA probing thread makes a request to the Luna Network HSM 7 where the internal cryptographic module (HSM card) is locked up, the probing thread can also lock up, and failover does not occur. To deal with that possibility, this setting, with a value greater than 0, initiates a timeout (in seconds).</p> <p><b>Valid Values:</b></p> <ul style="list-style-type: none"> <li>&gt; <b>0</b> (default): This is the same effect as the ProbeTimeout setting not existing in this configuration file - no timeout is set.</li> <li>&gt; <b>1 - ?</b>: A number of seconds greater than zero. This is a balancing decision, unique to your application situation. If you wish to set a ProbeTimeout, choose a value <ul style="list-style-type: none"> <li>• large enough to allow your usual crypto processes to complete normally, but</li> <li>• not so large that a failover, from a failed HA-group member to a healthy member, is never triggered before your application concludes that the entire HA group has failed.</li> </ul> </li> </ul> <p>This feature requires <a href="#">Luna HSM Client 10.7.2</a> or newer (with the default 0 value for backward compatibility).</p>

Section/Setting	Description
reconnAtt	<p>Specifies the number of reconnection attempts the client makes to a missing HA member. Once this number is reached, you must manually reconnect the member when it becomes available (see <a href="#">Manually Recovering a Failed HA Group Member</a>).</p> <p>This value is set using lunacm:&gt; <b>hagroup retry</b>.</p> <p><b>Valid Values:</b></p> <ul style="list-style-type: none"> <li>&gt; <b>-1</b>: Perform infinite reconnection attempts.</li> <li>&gt; <b>0</b>: Disable HA auto-recovery.</li> <li>&gt; <b>1-500</b>: Perform the specified number of reconnection attempts.</li> </ul>
statusTimeout	<p>This value (in seconds) is the amount of time the CA_GetCurrentHState function will try to verify the status of HA group members, before stopping and reporting the statuses collected up to that cutoff.</p> <p><b>Valid Values:</b></p> <ul style="list-style-type: none"> <li>&gt; <b>3</b> (default): This is the shortest reasonable value in good network conditions.</li> <li>&gt; <b>4-60</b>: Any value between the default and 60 second.</li> </ul> <div style="border-left: 2px solid black; padding-left: 10px; margin-top: 10px;"> <p><b>NOTE</b> After 60 seconds, the status check could conflict with other processes, so the cap is set at 60.</p> </div>
<b>Misc</b>	
Appld = <xxx>	<p>Application IDs are generated when the application starts, and are 16 bytes for Luna HSM Firmware 7.7.0 and newer, and <a href="#">Luna HSM Client 10.3.0</a> and newer. Application IDs are not supported for Luna Cloud HSM services. You can override this functionality and specify an Appld if desired.</p> <p>For HSM firmware version 7.8.4 onward, see <b>**NOTE</b> below this table.</p>

Section/Setting	Description
CopyRSAPublicValuesFromPrivateTemplate	<p>Controls whether the public exponent of an RSA key can be copied from the private key template, if the public key template does not already have a public exponent attribute set.</p> <p><b>Valid Values:</b></p> <ul style="list-style-type: none"> <li>&gt; <b>0</b>: if no public exponent is provided in the public template, an error is returned (expected behavior).</li> <li>&gt; <b>1</b>(default): if no public exponent is provided in the public template, the private exponent is copied from the private template to populate the public template.</li> </ul> <p>For PKCS#11 compliance, this should be set to <b>0</b>.</p>
ECCPointEncodingStrategy=	<p>Allows you to force (or not) the assumption that an Elliptic Curve point is provided in RAW octet string format.</p> <p><b>Valid Values:</b></p> <ul style="list-style-type: none"> <li>&gt; <b>1</b>: Queries HSM for correct EC Point Size, then determines whether encoding is required or not.</li> <li>&gt; <b>2</b>: Does not query the HSM for EC point size. Assumes EC point is RAW and always encodes it.</li> </ul> <p>(Included in client since Luna HSM Client 10.5.0; available as a patch for Luna HSM Client 10.4.0 and 10.4.1. Beginning with HSM firmware version 7.8.1 this entry is no longer needed.)</p>
FunctionBindLevel	<p>Determines what action to take if a function binding fails during a CryptokiConnect() operation.</p> <p><b>Valid Values:</b></p> <ul style="list-style-type: none"> <li>&gt; <b>0</b> (default): fail if not all functions can be resolved</li> <li>&gt; <b>1</b>: do not fail but issue warning for each function not resolved</li> <li>&gt; <b>2</b>: do not fail and do not issue warning (silent mode)</li> </ul>

Section/Setting	Description
LoginAllowedOnFMEnabledHSMs	<p>Determines whether the client can log in to a partition on an HSM that uses Functionality Modules (FMs). FMs consist of custom-designed code that introduces new functionality, which can be more or less secure than standard HSM functions.</p> <p>Possible values include:</p> <ul style="list-style-type: none"> <li>&gt; <b>0</b>: the client does not allow login to an FM-enabled partition</li> <li>&gt; <b>1</b>: the client allows login to an FM-enabled partition</li> </ul> <p>This entry is added to the configuration file the first time you initialize or log in to an FM-enabled partition using LunaCM. You are prompted to confirm that you want to allow login.</p> <div style="border: 1px solid black; padding: 10px; margin-top: 10px;"> <p><b>NOTE</b> References to Functionality Modules (FMs) do not apply to Luna USB HSM 7 as that platform does not support FMs. If you need to customize a Luna HSM beyond the extensive configuration and capability update options, consider the Luna PCIe HSM 7 and the Luna Network HSM 7 which do support tailoring or extending the HSM firmware with your own custom functionality.</p> </div>
MutexFolder=	<p>For non-Windows platforms. Several Luna features write temporary files to <b>/tmp</b>. If systemd service deletes the temporary files the affected services can be disrupted - example Remote PED callback service (cbs). An administrator can use this setting to specify an alternative location like this example:</p> <pre>Misc = { ...   MutexFolder = /usr/lock; }</pre> <p>The specified folder must exist, or the service fails to start properly.</p> <ul style="list-style-type: none"> <li>&gt; <b>Linux default:</b> &lt;install_dir&gt;/lock</li> </ul>

Section/Setting	Description
PE1746Enabled	<p>Enables the SafeXcel 1746 security co-processor on Luna 6 HSMs, which is used to offload packet processing and cryptographic computations from the host processor. Does not apply to Luna 7 HSMs or Luna Cloud HSM services.</p> <p><b>Valid Values:</b></p> <ul style="list-style-type: none"> <li>&gt; <b>0:</b> SafeXcel co-processor is disabled on Luna 6 HSMs.</li> <li>&gt; <b>1 (default):</b> SafeXcel co-processor is enabled on Luna 6 HSMs.</li> </ul>
PluginModuleDir	<p>Specifies the location of client plugins. This setting is required to use the cloud plugin to access Luna Cloud HSM services.</p> <p><b>Default:</b></p> <ul style="list-style-type: none"> <li>&gt; <b>Windows:</b> C:\Program Files\SafeNet\LunaClient\plugins</li> <li>&gt; <b>Linux:</b> /usr/safenet/lunaclient/libs/64/plugins</li> </ul>
ProtectedAuthenticationPathFlagStatus	<p>Specifies which role to check for challenge request status.</p> <p><b>Valid Values:</b></p> <ul style="list-style-type: none"> <li>&gt; <b>0 (default):</b> no challenge request</li> <li>&gt; <b>1:</b> check for Crypto Officer challenge request</li> <li>&gt; <b>2:</b> check for Crypto User challenge request</li> </ul>
ToolsDir	<p>The location of the Luna HSM Client tools.</p> <p><b>Full Luna HSM Client Default:</b></p> <ul style="list-style-type: none"> <li>&gt; <b>Windows:</b> C:\Program Files\SafeNet\LunaClient\</li> <li>&gt; <b>Linux/AIX:</b> /usr/safenet/lunaclient/bin/</li> <li>&gt; <b>Solaris:</b> /opt/safenet/lunaclient/bin/</li> </ul> <p><b>Minimal Luna HSM Client Default:</b></p> <ul style="list-style-type: none"> <li>&gt; <b>Linux:</b> /usr/safenet/lunaclient/bin/64/</li> </ul>
ValidateHost=	<p>Set this flag to have the Luna HSM Client validate the server's hostname/IP against the Subject Alternate Name (SAN) values in the server's certificate.</p> <p><b>Default: 0</b></p>
<b>Secure Trusted Channel</b>	<p><b>NOTE</b> Secure Trusted Channel is not supported with Luna Cloud HSM Services.</p>

Section/Setting	Description
ClientTokenLib (for 64-bit Windows systems)	<p>Specifies the location of the token library on 64-bit Windows systems. This value must be correct in order to use a client token. If you are using a hard token, you must manually change this value to point to the hard token library for your operating system. The exact location of the hard token library may vary depending on your installer.</p> <p><b>Default: C:\Program Files\SafeNet\LunaClient\softtoken.dll</b></p>
ClientTokenLib32 (for 32-bit Windows systems)	<p>Specifies the location of the token library on 32-bit Windows systems. This entry appears on Windows only.</p> <p>By default, <b>ClientTokenLib32</b> points to the location of the soft token library. If you are using a hard token, you must manually change this value to point to the hard token library for your operating system. The exact location of the hard token library may vary depending on your installer.</p> <p><b>Soft Token Default: C:\Program Files\SafeNet\LunaClient\win32\softtoken.dll</b></p> <p><b>Hard Token Default:</b> <b>C:\Windows\SysWOW64\etoken.dll</b></p> <div> <p><b>NOTE</b> Luna HSM Client 10.1.0 and newer includes libraries for 64-bit operating systems only.</p> </div>
<b>Session</b>	<p><b>NOTE</b> This section is not created automatically. To change any of the following values, you must first create this section in the configuration file.</p>
AutoCleanUpDisabled	<p>Determines whether AutoCleanUp closes orphaned sessions in the event that an application leaves sessions open. Useful for Luna PCIe HSM hosts. AutoCleanUp runs during C_Finalize on the client. Luna Network HSM 7 sessions are tracked and closed by the NTLS service.</p> <p><b>Valid Values:</b></p> <ul style="list-style-type: none"> <li>&gt; <b>0</b> (default): Run AutoCleanUp if your application leaks sessions and you cannot rewrite the application.</li> <li>&gt; <b>1</b>: Disable AutoCleanUp if you have a Luna PCIe HSM 7 and your client application does proper housekeeping, or if your application is connecting via NTLS to a Luna Network HSM 7.</li> </ul>
<b>Shim2</b>	<p><b>NOTE</b> This section is not created automatically. To change any of the following values, you must first create this section in the configuration file.</p>

Section/Setting	Description
(Linux) LibUNIX64=/usr/safenet/lunaclient/lib/libCryptoki2_64.so; (Windows) LibNT=C:\Program Files\SafeNet\LunaClient\cryptoki.dll	This section is required when a shim is to be used. If the cryptoki library is not at the indicated location, then adjust the example path value to reflect the actual location.
<b>Toggles</b>	<b>NOTE</b> This section is not created automatically. To change any of the following values, you must first create this section in the configuration file.
legacy_memory_rep =	Controls the manner in which the HSM reports the available RAM space. <b>Valid Values:</b> <ul style="list-style-type: none"> <li>&gt; <b>0</b> (default): the public and private memory total/free values reported in the CK_TOKEN_INFO structure indicate the available flash memory for permanent (TOKEN) objects that are in either the public or private space respectively; this method is PKCS#11 compliant.</li> <li>&gt; <b>1</b>: the public memory values indicate the total/free RAM memory; this non-standard legacy method was used by some customers to determine space available for session based objects, and must be explicitly selected in order to continue using the legacy method.</li> </ul>
lunacm_cv_ha_ui =	Controls whether Thales DPoD Luna Cloud HSM services can be active members of an HA group. <b>Valid Values:</b> <ul style="list-style-type: none"> <li>&gt; <b>0</b>: Luna Cloud HSM services can be added as active HA members.</li> <li>&gt; <b>1</b> (default): Luna Cloud HSM services can be added to HA groups as standby members only. This is the default behavior to maximize HA performance, which may suffer due to network latency.</li> </ul>

Section/Setting	Description
fetch_partition_label =	<p>Allows the client to refresh the slot list without requiring an application restart.</p> <p><b>Valid Values:</b></p> <ul style="list-style-type: none"> <li>&gt; <b>0</b> (default): A new session must be opened (C_Initialize) to refresh the slot list cache.</li> <li>&gt; <b>1</b>: Slot list cache is refreshed without requiring C_Initialize.</li> </ul> <p><b>NOTE</b> This functionality requires <a href="#">Luna HSM Client 10.5.1</a> or newer.</p>
map_aes_cmac_general_old=	<p>Allows the library to automatically map relevant values to the required mechanism <a href="#">CKM_AES_CMAC_GENERAL</a>. Refer to resolved issue <a href="#">LUNA-30232</a>.</p> <p><b>NOTE</b> This functionality requires <a href="#">Luna HSM Client 10.7.0</a> or newer.</p>
<b>REST</b>	<p><b>NOTE</b> This section configures a connection to a Luna Cloud HSM and applies only to a Luna Cloud HSM. This section is not created automatically for clients obtained from the Thales Support Portal. See "<a href="#">Adding a Luna Cloud HSM Service</a>" on <a href="#">page 46</a> for detailed instructions on adding a Luna Cloud HSM service client to a Luna HSM Client.</p> <p>This section governs Luna Cloud HSM service functionality only and is not related to the Luna REST API. This functionality requires <a href="#">Luna HSM Client 10.2.0</a> or newer.</p>

Section/Setting	Description
AppLogLevel	<p>Defines the maximum severity level of application logs to be displayed in the application console.</p> <p><b>Valid Values:</b></p> <ul style="list-style-type: none"> <li>&gt; <b>trace</b> (unavailable for <a href="#">Luna HSM Client 10.4.0</a> and newer)</li> <li>&gt; <b>debug</b> (unavailable for <a href="#">Luna HSM Client 10.4.0</a> and newer)</li> <li>&gt; <b>error</b></li> <li>&gt; <b>warning</b></li> <li>&gt; <b>info</b></li> </ul> <p>Application Error Logs are printed to the Event Viewer on Windows 10 and to the system and console on Linux.</p> <p><b>Windows:</b> Windows operating systems print application error logs to the Event Viewer. Access the logs by opening <b>Event Viewer &gt; Windows Logs &gt; Application</b> and filtering the results for <i>LunaClientEventProvider</i>.</p> <div style="border: 1px solid black; padding: 5px; margin: 10px 0;"> <p><b>NOTE</b> To display Windows Logs in the Event Viewer as a non-administrator user you must register the <b>LunaClientEventProvider.dll</b>. Failure to register the <b>LunaClientEventProvider.dll</b> will result in the logs displaying to the console.</p> </div> <p><b>Linux:</b> Linux operating systems print application error logs to <b>/var/log/message</b>. Access the logs by opening <b>/var/log/message</b> and searching the results for <i>lunacm</i>.</p> <p><b>Ubuntu:</b> Ubuntu operating systems print application error logs to <b>/var/log/syslog</b>. Access the logs by opening <b>/var/log/syslog</b> and searching the results for <i>lunacm</i>.</p>
AuthTokenConfigURI	<p>The identifier for the authentication service which issues the tokens required to validate the client's identity to the Luna Cloud HSM service. Your client host must have an internet connection to reach this resource. Do not edit the default value unless instructed to by customer support.</p>
AuthTokenClientId	<p>The client identity required by the authentication service to issue a token. Do not edit the default value unless instructed to by customer support.</p>
AuthTokenClientSecret	<p>The client passphrase required by the authentication service to issue a token. Do not edit the default value unless instructed to by customer support.</p>

Section/Setting	Description
CurlLogsEnabled	<p>Enables libcurl logging. This variable applies to <a href="#">Luna HSM Client 10.3.0</a> and newer.</p> <p><b>Valid Values:</b></p> <ul style="list-style-type: none"> <li>&gt; <b>False:</b> Libcurl logging is disabled.</li> <li>&gt; <b>True</b>(default): Libcurl logging is enabled.</li> </ul> <div style="border: 1px solid #ccc; padding: 10px; margin: 10px 0;"> <p><b>NOTE</b> If using <a href="#">Luna HSM Client 10.4.0</a> or newer you <b>must</b> have AppLogLevel=info defined in your Chrystoki.conf\crystoki.ini to retrieve curl logs. See "<a href="#">AppLogLevel</a>" on the <a href="#">previous page</a> for more information.</p> </div> <p>Curl Logs are printed to the Event Viewer on Windows 10 and to the system and console on Linux.</p> <p><b>Windows:</b> Windows operating systems print application error logs to the Event Viewer. Access the logs by opening <b>Event Viewer &gt; Windows Logs &gt; Application</b> and filtering the results for <i>LunaClientEventProvider</i>.</p> <div style="border: 1px solid #ccc; padding: 10px; margin: 10px 0;"> <p><b>NOTE</b> To display Windows Logs in the Event Viewer as a non-administrator user you must register the <b>LunaClientEventProvider.dll</b>. Failure to register the <b>LunaClientEventProvider.dll</b> will result in the logs displaying to the console.</p> </div> <p><b>Linux:</b> Linux operating systems print application error logs to <b>/var/log/message</b>. Access the logs by opening <b>/var/log/message</b> and searching the results for <i>lunacm</i>.</p> <p><b>Ubuntu:</b> Ubuntu operating systems print application error logs to <b>/var/log/syslog</b>. Access the logs by opening <b>/var/log/syslog</b> and searching the results for <i>lunacm</i>.</p>
ClientConnectIntervalMs	<p>Interval in milliseconds between client connection attempts.</p> <p><b>Default: 1000</b></p>
ClientConnectRetryCount	<p>Maximum connection attempts between a client and a server.</p> <p><b>Default: 900</b></p>
ClientEofRetryCount	<p>Maximum command retries.</p> <p><b>Default: 15</b></p>
ClientPoolSize	<p>Number of threads in the thread pool available for client operations.</p> <p><b>Default: 32</b></p>

Section/Setting	Description
ClientTimeoutSec	<p>Time in seconds that a client waits for a response. This timeout applies to each retry attempt individually.</p> <p><b>Default: 600</b></p> <div><p><b>NOTE</b> This entry does not appear in the default configuration file, but the default value applies to this timeout. You can manually add the entry if you wish to edit the timeout.</p></div>

Section/Setting	Description
PartitionData00	<p>The partition serial number, load balancer IP address or hostname, and load balancer port.</p> <p>Executing <code>setenv</code>, when configuring the Luna HSM Client, removes PartitionData00 and replaces it with values for <code>ServerName</code> and <code>ServerPort</code>.</p> <p>The following format is used:</p> <p>PartitionData00=&lt;partition_serial_number&gt;, &lt;service_ip_address/hostname&gt;, &lt;service_port&gt;;</p> <div data-bbox="842 569 1406 667"> <p><b>NOTE</b> PartitionData00 is deprecated and included in the bundle to support legacy use cases. This may be removed in a future update.</p> </div> <div data-bbox="880 726 1386 1194"> <p><b>CAUTION!</b> The Luna Cloud HSM service failover to the redundant datacenter uses a change to DNS to direct client traffic to a secondary datacenter. The client configuration file includes the FQDN for the Luna Cloud HSM service datacenter in the <code>REST = PartitionData00</code> section or the <code>REST = ServerName</code> section after executing <code>setenv</code> (<code>eu.hsm.dpondemand.io</code> or <code>na.hsm.dpondemand.io</code>). In the event of a failover the DNS record for FQDN is updated to point to the secondary datacenter.</p> <p>Ensure that the client is configured to use the domain name for the datacenter and to not configure any filtering based on the IP addresses. Failure to use the domain name and filtering IP addresses could result in the client being unable to failover to the secondary datacenter.</p> </div> <div data-bbox="842 1503 1415 1734"> <p><b>NOTE</b> Using Luna Cloud HSM 10.7.2 or higher, users are no longer required to run <code>setenv</code> to configure the client to connect to the Cloud HSM Service. However, <code>setenv</code> may still be used to configure the client for hybrid use cases or integrations where setting the <code>ChrystokiConfigurationPath</code> is required.</p> </div>

Section/Setting	Description
RestClient	Indicates that cvclient and associated tools are acting as REST clients. <b>Default: 1</b>
ServerName	The name of the Luna Cloud HSM server.
ServerPort	The port used for Luna Cloud HSM server traffic.
<b>XTC</b>	<b>NOTE</b> This section configures a connection to a Luna Cloud HSM and applies only to a Luna Cloud HSM. This section is not created automatically for clients obtained from the Thales Support Portal. See <a href="#">"Adding a Luna Cloud HSM Service" on page 46</a> for detailed instructions on adding a Luna Cloud HSM service client to a Luna HSM Client. This section governs Luna Cloud HSM service functionality only and is not related to the Luna REST API. Requires <a href="#">Luna HSM Client 10.2.0</a> or newer.
Enabled	Indicates that XTC (Transferable Token Channel) is enabled. This channel must be enabled for the client to communicate with a Luna Cloud HSM service. <b>Valid Values:</b> <ul style="list-style-type: none"> <li>&gt; <b>0</b>: XTC is disabled.</li> <li>&gt; <b>1</b> (default): XTC is enabled.</li> </ul>
TimeoutSec	Time (in seconds) before a cryptographic request expires. Timestamps are included in XTC headers, and the HSM rejects messages which have expired. <b>Valid Values: 1-600</b>
<b>GemEngine</b>	<b>NOTE</b> This section is not created automatically.

Section/Setting	Description
DisableCheckFinalize	<p>Determines how the gem engine behaves for finalizing the cryptoki library. If an application has forking processes, then this causes the connection with the HSM to be shared between the parent and the child process which must be addressed for Linux/UNIX.</p> <p><b>Valid Values:</b></p> <ul style="list-style-type: none"> <li>&gt; <b>0</b> (default): Perform pre-fork checking -- when crypto calls are made in the parent process, the cryptoki library is finalized after each crypto call. However, in the child process, the library is initialized and the connection to the HSM is maintained after crypto calls. The parent and child will have different connections to the HSM.</li> <li>&gt; <b>1</b>: Perform post-fork checking -- the engine initializes the cryptoki library and maintains the connection to the HSM until the application terminates.</li> </ul> <p>If your application (own or 3rd party) is using OpenSSL and has forking processes, set this value to 0. Otherwise, setting the option to 1 will improve performance.</p> <p>Not used for Windows.</p>

\* If you intend to invoke a large number N for an M of N keyset (maximum is 16 splits), including also a backup set, you will need to increase the various PED timeout values well beyond the default values, in order to have enough time to comfortably complete the task. As a rough example, increase the PED's timeout for creating a keyset by a factor of 10. Altogether, the combined value works out to:

```
CommandTimeOutPedSet >= ( DefaultTimeOut + PEDTimeout1 + PEDTimeout2 + PEDTimeout3 )
```

So, for example, in the Luna section of the .conf file (similar for the .ini file in Windows):

```
Luna =
{ DefaultTimeOut = 500000; PEDTimeout1 = 100000; PEDTimeout2 = 2000000; PEDTimeout3 = 20000;
KeypairGenTimeOut = 2700000; CloningCommandTimeOut = 300000; CommandTimeOutPedSet = 2620000; }
```

The longest such activity would be creating a 16-key split of a new-format orange PED Key (RPK), with duplicates, which might take a little more than half an hour at a comfortable pace with no interruptions. This is considered an extreme edge-case. Your situation will probably require settings somewhere between the defaults and the values suggested above.

\*\*\*

**NOTE** From HSM firmware version 7.8.4 onward, Application IDs (APPId) are *encrypted*, with the following effects:

- Whenever firmware is upgraded from a non-APPID encrypted version (before firmware 7.8.4) to an encrypted APPID firmware version, the access ID shown in the logs will change.
- After the new firmware starts, the *encrypted* value of the same access ID for that application (for example, LUNACM) is now shown.
- The access ID shown also changes after every reset/restart of firmware version 7.8.4 onward because a new APPID encryption key (AEK) is created each time firmware starts up. The AEK is used by the crypto library of the APP to encrypt the access ID.
- Also whenever an Application is started it creates a new random access ID each time (unless fixed to a value [set AppId= under the Misc section] in the Configuration file ).

## Dynamic UserID Loading for Luna Cloud HSM Services

The UC Dynamic Loading feature is introduced in [Luna HSM Client 10.5.0](#) for Luna Cloud HSM services. This allows each User Account and Authentication (UAA) user to have the ability to have one or more partition(s) associated with them. The DPoD tenant role can now configure multiple UAA Users and manage them in one place instead of managing each one separately. This will also allow customers to add multiple UserID's (combination of unique authtokenclientsecret, authtokenclientid and URI) without the need to restart the application after the addition of a new UserID.

The ability to load multiple partitions to the same UserID without impacting service to other users is also supported. If an attempt is made to add the same partition ID to a different user that will be ignored and a warning log will be generated.

When a new configuration is added, running the "slot list" command will display the new partition ID for that user.

**NOTE** The maximum amount of users to be added using the "MaxUserIDCount" variable is defaulted at 100. Multiple partitions for the same user will **NOT** have a sequential slot ID.

### In Linux:

```
export AuthTokenConfigURI2=*****
export AuthTokenClientID2=*****
export AuthTokenClientSecret2=*****

export AuthTokenConfigURI3=*****
export AuthTokenClientID3=*****
export AuthTokenClientSecret3=*****
```

### In Windows:

```
set var=AuthTokenConfigURI2=*****
set var=AuthTokenClientID2=*****
set var=AuthTokenClientSecret2=*****

set var=AuthTokenConfigURI3=*****
set var=AuthTokenClientID3=*****
set var=AuthTokenClientSecret3=*****
```

## Updating the Luna HSM Client Software

---

To update the Luna HSM Client software, first uninstall any previous version of the Client. Then, run the new installer the same way you performed the original installation (refer to ["Luna HSM Client Software Installation" on page 20](#)).

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

**TIP** Thales recommends verifying the integrity of the Luna HSM Client packages, by calculating their SHA256 hash values and comparing with the hash values posted on the Support Portal, before installing them on your client machines.

You can use the sha256sum tool on Linux machines to calculate the SHA256 hash values.

## CHAPTER 3: Secure Transport Mode

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

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

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

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

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

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

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

### When STM is enabled on the HSM

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

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

### STM verification email

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

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

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

For information about the various tamper events, see ["Tamper Events" on page 144](#).

## 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 128](#)). If this is a new or zeroized HSM, skip to the next step.

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

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

```
lunacm:> stm recover -randomuserstring <XXXX-XXXX-XXXX-XXXX>
```

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

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

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

Enter **proceed** to recover from STM.

### If the verification strings do not match

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

## Placing an HSM In Secure Transport Mode

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

### To place an HSM into Secure Transport Mode

1. Log in as the HSM SO (see "[Logging In as HSM Security Officer](#)" on page 128).
2. Back up the contents of all application partitions.  
See [Partition Backup and Restore](#) for details.
3. Enter the following command to place the HSM into STM:  
lunacm:> **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.

**TIP Why do my STM verification codes not match?**

Be careful when resuming use of an HSM after transport. A single failed SO login attempt changes the state of the HSM firmware, because it increments the counter that tracks the number of login attempts remaining. The HSM uses the changed state when it calculates the verification code.

That will cause a mismatch when you compare STM values.

Entering an invalid PIN or Password is not covered by warranty, and is not cause for RMA.

Before assuming that an attack has occurred, please review the logs.

The above is also why you must deactivate partitions on a multi-factor quorum authenticated (PED) HSM before invoking STM and powering off. If the HSM has partitions that are Activated, and it is powered off for more than two hours, the partitions become deactivated, which makes a change in the firmware (activated state to deactivated state), again changing the calculated verification string.

# CHAPTER 4: Multifactor Quorum Authentication

The Luna USB HSM 7 can be initialized to use multifactor quorum authentication for all roles on the HSM. The authentication secrets are stored on USB iKeys, and are presented by inserting them directly into the Luna USB HSM 7. This means that the iKeys and direct access to the Luna USB HSM 7 are the only method of accessing the HSM's administrative functions. This prevents key-logging exploits on workstations connected to the client HSM, because authentication takes place entirely within the device itself. No password is entered via computer keyboard.

This section contains the following information about Luna USB HSM 7 multifactor quorum authentication:

- > ["Multifactor Quorum Authentication Architecture" below](#)
  - ["Comparing Password and Multifactor Quorum Authentication" on the next page](#)
- > ["iKeys" on the next page](#)
  - ["iKey Types and Roles" on page 84](#)
  - ["Shared iKey Secrets" on page 85](#)
  - ["Domain iKeys" on page 86](#)
  - ["iKey PINs" on page 86](#)
  - ["M of N Split Secrets \(Quorum\)" on page 86](#)
- > ["iKey Management Using Luna USB HSM 7" on page 87](#)

## Multifactor Quorum Authentication Architecture

The multifactor quorum authentication architecture consists of the following components:

- > Luna USB HSM 7: Role secrets stored on iKeys are presented directly to the Luna USB HSM 7 by connecting them to the USB-C input.
- > **Authentication secrets:** Cryptographic secrets generated by the HSM and stored on iKeys. 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.
- > **iKeys:** physical USB-connected devices that contain authentication secrets, created by the HSM (see ["iKeys" on the next page](#)). iKeys have the following custom authentication features:
  - **Shared Secrets:** iKeys of the same type can be reused or shared among HSMs or partitions, allowing domain sharing (necessary for backup configurations) and other custom configurations. See ["Shared iKey Secrets" on page 85](#).
  - **iKey PINs:** optional PINs associated with specific iKeys, set by the owner of the iKey at the time of creation. iKey PINs offer an extra layer of security for iKeys which could be lost or stolen. See ["iKey PINs" on page 86](#).

- **M of N Split Key Scheme:** optional configuration which allows a role to split its authentication secret across multiple iKeys, 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 86.

## Comparing Password and Multifactor Quorum Authentication

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

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

## iKeys

The iKey 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 USB HSM 7 does not hold the authentication secrets. They reside only on the portable iKeys.




iKeys are created when an HSM, partition, or role is initialized. Each iKey can contain only one authentication secret at a time, but it can be overwritten with a new authentication secret. See ["iKey Management Using Luna USB HSM 7" on page 87](#).




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

## iKey Types and Roles

Once initialized for multifactor quorum authentication, the Luna USB HSM 7 uses iKeys for all credentials. You can apply the appropriate labels included with your iKeys, according to the table below, as you create them.

The iKey colors correspond with the HSM roles described in ["HSM Roles" on page 127](#) and [Partition Roles](#). The following table describes the keys associated with the various roles:

Lifecycle	iKey	Secret	Function
HSM Administration	<b>Blue</b>	HSM Security Officer (HSM SO) secret	Authenticates the HSM SO role. The HSM SO manages provisioning functions and security policies for the HSM. <b>Mandatory</b>
	<b>Red</b> 	HSM Domain or Key Cloning Vector	Cryptographically defines the set of HSMs that can participate in cloning for backup. See <a href="#">"Domain iKeys" on page 86</a> . <b>Mandatory</b>
HSM Auditing	<b>White</b> 	Auditor (AU) secret	Authenticates the Auditor role, responsible for audit log management. This role has no access to other HSM services. <b>Optional</b>
Partition Administration	<b>Blue</b>	Partition Security Officer (PO) secret	Authenticates the Partition SO role. The PO manages provisioning activities and security policies for the partition. <b>NOTE:</b> If you want the HSM SO to also perform Partition SO duties, you can use the same blue key to initialize both roles. <b>Mandatory</b>
	<b>Red</b> 	Partition Domain or Key Cloning Vector	Cryptographically defines the set of partitions that can participate in cloning for backup or high-availability. See <a href="#">"Domain iKeys" on page 86</a> . <b>Mandatory</b>

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

**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 iKeys.

## Shared iKey Secrets

The Luna USB HSM 7 identifies the type of authentication secret on an inserted iKey, 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 iKey(s) to authenticate multiple HSMs or partitions. This is useful for:

- > 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 iKeys" on the next page](#))
- > allowing a read-write Crypto Officer role and a read-only Crypto User role to be managed by the same user

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

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

## Domain iKeys

A red domain iKey holds the key-cloning vector (the domain identifier) that allows key cloning between HSMs and partitions, and is therefore the iKey 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 the cloning domain.

**NOTE** An HSM or partition can be a member of only one domain, decided at initialization. A domain can only be changed by re-initializing the HSM or partition.

## iKey PINs

The Luna USB HSM 7 allows the holder of a iKey to set a numeric PIN, 4-48 characters long, to be associated with that iKey. This PIN must then be entered on the touchscreen for all future authentication. The PIN provides two-factor authentication and ensures security in case an iKey is lost or stolen. If you forget your PIN, it is the same as losing the iKey entirely; you cannot authenticate the role.

PINs can be set only at the time of key creation, and can be changed only by changing the secret on the iKey. Duplicate keys are true copies with the same PIN, intended as backups for one person (see ["Duplicating an Existing iKey Using Luna USB HSM 7" on page 93](#)). Duplicates of the iKey all have the same PIN.

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

**CAUTION!** Forgetting a PIN is equivalent to losing the key entirely; you can no longer authenticate the role, domain, or RPV. See ["Consequences of Losing iKeys" on page 91](#).

## M of N Split Secrets (Quorum)

The Luna USB HSM 7 can split an authentication secret among multiple iKeys (up to 16), and require a minimum number of the split keys (a quorum of key-holders) to authenticate the role. This provides a customizable layer of security by requiring multiple trusted people (sometimes called the quorum) to be present for authentication to the role.

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 splits of that role secret is five persons, and from among them, a quorum of three must be available to achieve authentication (any three in this 3 of 5 scenario, but cannot be the same key presented more than once during an authentication attempt).

In this scenario, the HSM SO authentication secret is split among five blue iKeys, and at least three of those keys must be presented to the Luna USB HSM 7 to log in as HSM SO.

This feature can be used to customize the level of security and oversight for all actions requiring multifactor quorum authentication. You can elect to apply 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 recommended only when you want multiple people to access the role, each with their own unique iKey PIN.

**NOTE** Using an M of N split secret can greatly increase the number of iKeys you require. Ensure that you have enough blank or rewritable iKeys on hand before you begin initializing 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 iKey (see [Activation and Auto-activation on Multifactor Quorum-Authenticated Partitions](#)). In this case, if the HSM is rebooted for maintenance or loses power due to an outage, the cached authentication secret is erased and the role must be reactivated (by logging in the role via LunaCM and presenting the requisite M number, or quorum, of iKeys) before normal operations can resume.

## iKey Management Using Luna USB HSM 7

---

Once you have connected your Luna USB HSM 7 to a workstation and installed Luna HSM Client, you can proceed with initializing roles on the HSM using multifactor quorum authentication. The procedures in this section will guide you through the touchscreen prompts at each stage of iKey creation, authentication, and other iKey operations with the Luna USB HSM 7.

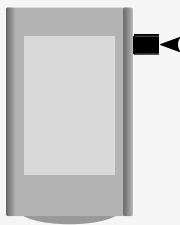
- > ["Creating iKey Using Luna USB HSM 7" below](#)
- > ["Authenticating a Role Using Luna USB HSM 7" on page 89](#)
- > ["Consequences of Losing iKeys" on page 91](#)
- > ["Identifying an iKey Secret Using Luna USB HSM 7" on page 93](#)
- > ["Duplicating an Existing iKey Using Luna USB HSM 7" on page 93](#)
- > ["Changing an iKey Credential" on page 94](#)

### Creating iKey Using Luna USB HSM 7

When you initialize an HSM, partition, or role, the Luna USB HSM 7 issues a series of prompts for you to follow to create your iKeys. iKey actions have a timeout setting (default: 120 seconds); ensure that you have everything you need before issuing an initialization command. The requirements for the operation depend on the iKey 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 iKey or keyset, the owners of those keys must be present with their iKey and PINs ready.
- > If you plan to use an M of N authentication scheme (quorum, or split-secret), all the parties involved must be present and ready to create their authentication split. It is advisable for each iKey holder to create backup duplicates, so you must have a sufficient number of blank or rewritable iKeys ready before you begin.
- > If you plan to make backup duplicates of iKeys, you must have a sufficient number of blank or rewritable iKeys ready.
- > If you plan to use PINs, ensure that they can be privately entered on the Luna USB HSM 7 and memorized, or written down and securely stored.

**NOTE** Whenever the Luna USB HSM 7 prompts you to insert an iKey, use the USB-C adapter in the USB port on the right side of the Luna USB HSM 7:



### To initiate iKey creation

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

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

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

- **Orange Remote iKey:**

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

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

```
lunacm:> partition init
```

- **Black Crypto Officer iKey:**

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

- **Gray Limited Crypto Officer iKey**

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

- **Gray Crypto User iKey:**

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

- **White Audit User iKey:**

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

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

### Stage 1: Reusing Existing iKeys

If you want to use an iKey or quorum of iKeys with an existing authentication secret, have them ready to present to the HSM. Reasons for reusing iKeys may include:

- > You want to use the same iKey to authenticate multiple HSMs/partitions
- > You want to initialize a partition in an already-existing cloning domain (to allow cloning of cryptographic objects between partitions)

**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 iKey Secrets" on page 85](#) and ["Domain iKeys" on page 86](#) for more information.

The first touchscreen prompt asks if you want to create a new quorum of iKeys or reuse an existing quorum. Make your selection and follow the instructions on the touchscreen. If you are creating a new quorum, go to ["Stage 2: Defining M of N" below](#).

### Stage 2: Defining M of N

If you chose to create a new keyset, the Luna USB HSM 7 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 86](#) for more information. If you do not want to use M of N (authentication by one iKey), enter a value of **1** for both M and N.

For each iKey in the quorum, proceed to ["Stage 3: Setting a PIN" below](#).

### Stage 3: Setting a PIN

If you are creating a new iKey, you have the option of setting a PIN that must be entered by the key owner during authentication. PINs must be 4-48 digits long. Do not use 0 for the first digit. See ["iKey PINs" on page 86](#) for more information.

**CAUTION!** If you forget your PIN, it is the same as losing the iKey entirely; you cannot authenticate the role. See ["Consequences of Losing iKeys" on page 91](#).

You now have the opportunity to create a duplicate of the new iKey in ["Stage 4: Duplicating New iKey" below](#). If you decline to create a duplicate now, repeat this stage for each new iKey in the quorum.

### Stage 4: Duplicating New iKey

You now have the option to create duplicates of your newly-created iKey(s) in case of key loss or theft.

## Authenticating a Role Using Luna USB HSM 7

When connected, the Luna USB HSM 7 responds to authentication commands in LunaCM. Commands that require authentication include:

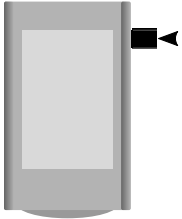
- > Role login commands (blue, black, gray, or white iKeys)
- > Backup/restore commands (red iKeys)
- > Remote PED connection commands (orange iKey)

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

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

Please attend to the PED.

Whenever the Luna USB HSM 7 prompts you to insert a iKey, use the USB port on the right side of the Luna USB HSM 7:



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

### To perform multifactor quorum authentication

1. The touchscreen prompts for the corresponding iKey. Insert the iKey (or the first M of N split-secret key) and follow the instructions on the touchscreen.

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

Please attend to the PED.

- If the key you inserted has an associated PIN, continue to step 2.
- If the key you inserted has no PIN, but it is an M of N split, skip to step 3.
- Otherwise, authentication is complete and the Luna USB HSM 7 returns control to the command interface.

Command Result : No Error

2. If a PIN is associated with the iKey, the touchscreen prompts for the PIN.

- If the key you inserted is an M of N split, continue to step 3.
- Otherwise, authentication is complete and the Luna USB HSM 7 returns control to the command interface.

Command Result : No Error

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

- If the key you inserted has an associated PIN, return to step 2.
- Repeat steps 2 and/or 3 until the requisite M number of keys have been presented. At this point, authentication is complete and the Luna USB HSM 7 returns control to the command interface.

Command Result : No Error

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

## Consequences of Losing iKeys

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

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

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

- > ["Blue HSM SO iKey" below](#)
- > ["Red HSM Domain iKey" below](#)
- > ["Blue Partition SO iKey" on the next page](#)
- > ["Red Partition Domain iKey" on the next page](#)
- > ["Black Crypto Officer iKey" on the next page](#)
- > ["Gray Crypto User iKey" on page 93](#)
- > ["White Audit User iKey" on page 93](#)

### Blue HSM SO iKey

If the HSM SO secret is lost, you can no longer perform administrative tasks on the HSM, including partition creation and client assignment. The contents of the HSM Admin partition are unrecoverable and you can no longer configure the HSM. Take the following steps:

1. Contact the Crypto Officer and have them immediately make a backup of their existing partition.
2. When all important cryptographic material is backed up, execute a factory reset of the HSM.
3. Initialize the HSM and create a new HSM SO secret.
4. Recreate the application partition.
5. The Partition SO must initialize the new partition using their original blue and red iKey(s), and initialize the Crypto Officer role (and Activation secret, if applicable). Supply the new black CO iKey to the Crypto Officer.
6. The Crypto Officer must change the login credentials from the new black CO iKey to their original black iKeys (and reset the Activation secret password, if applicable).
7. The Crypto Officer can now restore all partition contents from backup.
8. If you are using Remote PED, you must recreate the Remote PED Vector (RPV). You can re-use the original orange iKey.

### Red HSM Domain iKey

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

### Blue Partition SO iKey

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 iKey

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 iKey

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 iKey

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 iKey

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 an iKey Secret Using Luna USB HSM 7

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

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

You require:

- > Luna USB HSM 7 in Admin Mode
- > the key you want to identify

### To identify the type of secret stored on the iKey

1. Insert the iKey you want to identify.
2. Tap the **ADMIN** tab on the touchscreen to enter Admin mode.

The role secret type is identified on-screen.

## Duplicating an Existing iKey Using Luna USB HSM 7

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

- > Luna USB HSM 7 in Admin Mode
- > Enough blank or rewritable keys to make your copies

The iKey is duplicated exactly by this process. If there is a PIN assigned, the same PIN is assigned to the duplicate key. If the key is part of 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 86.

### To duplicate an existing iKey

1. Insert the iKey you want to duplicate. Have a blank or rewritable iKey ready.
2. Tap the **ADMIN** tab on the touchscreen to enter Admin mode.
3. Tap **Duplicate this iKey** and follow the instructions on the touchscreen.

### Changing an iKey Credential

It may be necessary to change the iKey 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 iKey
- > Personnel changes in your organization or changes to individual security clearances
- > Changes to your security scheme (implementing/revoking M of N, PINs, or shared secrets)

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

**CAUTION!** If you are changing an iKey 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 iKey credentials, you must always present the old keyset first; do not overwrite your old iKeys until you have no further need for them.

If you overwrite the original iKey with a new credential and the operation fails, it is possible for the iKey credential to be overwritten while the role remains tied to the old credential. If this happens, all login attempts with the overwritten iKey will fail. Ensure that you keep at least one backup copy of the old iKey credential until the role is successfully set to a new credential.

- > ["Blue HSM SO iKey" on page 91](#)
- > ["Red HSM Domain iKey" on page 91](#)
- > ["Orange Remote PED Vector iKey" on the next page](#)
- > ["Blue Partition SO iKey" on page 92](#)
- > ["Red Partition Domain iKey" on page 92](#)
- > ["Black Crypto Officer iKey" on page 92](#)
- > ["Gray Crypto User iKey" on the previous page](#)
- > ["White Audit User iKey" on the previous page](#)

### Blue HSM SO iKey

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

### To change the blue HSM SO iKey credential

1. In LunaCM, set the active slot to the Admin partition and log in as HSM SO.

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

2. Initiate the iKey change.

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

3. You are prompted to present the original blue key(s) and then to create a new HSM SO keyset. See ["Creating iKey Using Luna USB HSM 7" on page 87](#).

### Red HSM Domain iKey

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

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

### Orange Remote PED Vector iKey

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

#### To change the RPV/orange key credential

1. In LunaCM, set the active slot to the Admin partition and log in as HSM SO.

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

2. Initialize the RPV.

lunacm:> **ped vector init**

You are prompted to create a new Remote iKey.

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

### Blue Partition SO iKey

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

#### To change a blue Partition SO iKey credential

1. In LunaCM, log in as Partition SO.

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

2. Initiate the iKey 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 iKey

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 iKey

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

---

### To change a black Crypto Officer iKey credential

1. In LunaCM, log in as Crypto Officer.  
lunacm:> **role login -name co**
2. Initiate the iKey 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 iKey

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

---

### To change a gray Crypto User iKey credential

1. In LunaCM, log in as Crypto User.  
lunacm:> **role login -name cu**
2. Initiate the iKey change.  
lunacm:> **role changepw -name cu**
3. You are prompted to present the original gray key(s) and then to create a new Crypto User keyset.

### White Audit User Key

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

---

### To change the white Audit User iKey credential

1. In LunaCM, set the active slot to the Admin partition and log in as Auditor.  
lunacm:> **role login -name au**
2. Initiate the iKey change.  
lunacm:> **role changepw -name au**
3. You are prompted to present the original white key(s) and then to create a new Audit User keyset.

# CHAPTER 5: 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 106](#)
- > ["Logging In as Auditor" on page 113](#)
- > ["Configuring and Using Audit Logging" on page 109](#)
- > ["Audit Log Categories and HSM Events" on page 114](#)
- > ["Audit Log Troubleshooting" on page 121](#)

## Audit Logging Features

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

- > Log entries originate from the Luna USB HSM 7 (cryptographic module - the feature is implemented via HSM firmware (rather than in the library), for maximum security.
- > Log origin is assured.
- > Logs and individual records can be validated by any Luna USB HSM 7 that is a member of the same domain.
- > Audit Logging can be performed on password-authenticated and multifactor quorum-authenticated (both FIPS 140-3 level 3) configurations, but these configurations may not validate each other's logs - see the "same domain" requirement, above.

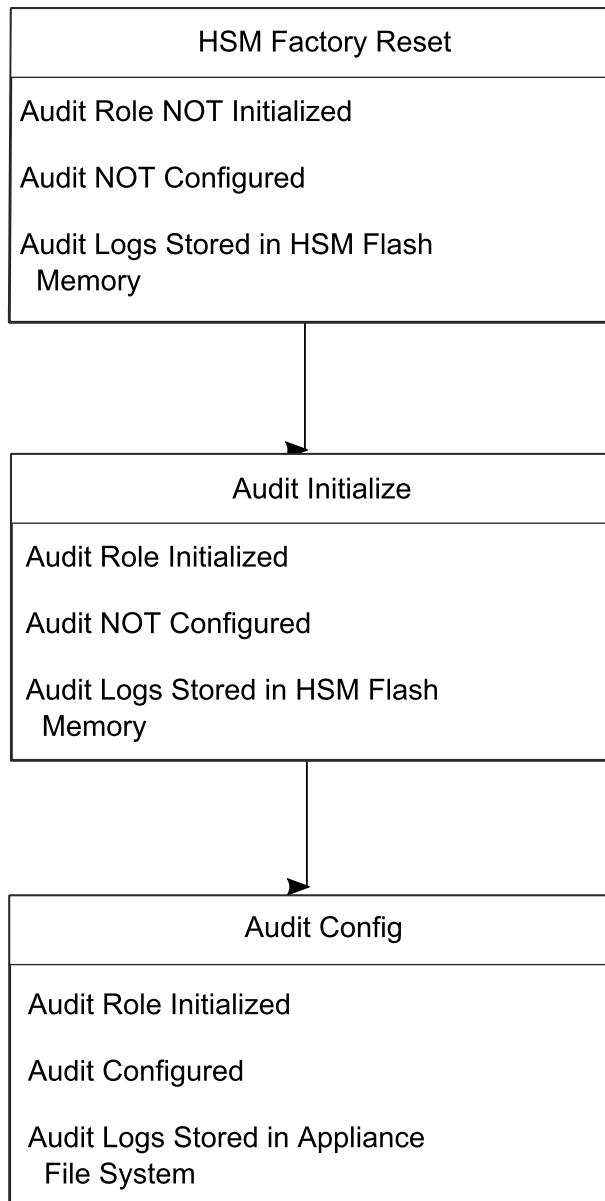
**NOTE** The "same domain" requirement still applies, but with the introduction of Extended Domain Management [ see [Universal Cloning](#) and [Domain Planning](#) ] (Partition Policy 44) in firmware version 7.8.0, you can change/add domains, such that the verifying HSM could be given the same domain as the original logging HSM.

Thus, from Luna HSM firmware version 7.8.0 onward, it is possible

- for a Multifactor Quorum HSM log to be validated by a Password-authenticated HSM or
- for a Password-authenticated HSM log to be validated by a Multifactor Quorum HSM.

- > Each entry includes the following:
  - When the event occurred
  - Who initiated the event (the authenticated entity)
  - What the event was
  - The result of the logging event (success, error, etc.)

- > Multiple categories of audit logging are supported, configured by the audit role.
- > Audit management is a separate role - the role creation does not require the presence or co-operation of the Luna USB HSM 7 SO.
- > The category of audit logging is configurable by (and only by) the audit role.
- > Audit log integrity is ensured against the following:
  - Truncation - erasing part of a log record
  - Modification - modifying a log record
  - Deletion - erasing of the entire log record
  - Addition - writing of a fake log record
- > The following critical events are logged unconditionally, regardless of the state of the audit role (initialized or not):
  - Tamper
  - Decommission
  - Zeroization
  - SO creation
  - Audit role creation

**Note:**

Logs are exported from the HSM's memory to the appliance's hard drive. Only an authenticated Auditor role is allowed to configure or initiate the export function. Therefore, an HSM in the Factory Reset state is **not** allowed to export log files from HSM memory to the appliance file system.

**Note:**

"audit log clear" clears logs only from the appliance file system. It does **not** affect logs stored in the HSM memory. Logs move out of HSM memory to the host file system, only when audit log rotation has been configured by the Auditor - so initialize and configure early to avoid log-entry build-up on the HSM.

**Types of events included in the logs**

The events that are included in the log is configurable by the audit role. The types of events that can be logged include the following:

- > log access attempts (logins)
- > log HSM management (init/reset/etc)
- > key management events (key create/delete)
- > asymmetric key usage (sig/ver)
- > first asymmetric key usage only (sig/ver)

- > symmetric key usage (enc/dec)
- > first symmetric key usage only (enc/dec)
- > log messages from CA\_LogExternal
- > log events relating to log configuration

Each of these events can be logged if they fail, succeed, or both.

### **Event log storage**

When the HSM logs an event, the log is stored on the HSM. The audit user cannot view these log entries. Before a log can be viewed, it must be rotated. Log rotation saves the log entries on the HSM to the local file system, where they can be viewed. Log records are HMACed using an audit log secret to ensure their authenticity. The audit log secret is unique to the HSM where the log was created, and is required to view the HSM event logs. The secret can be exported, allowing you to view and verify the logs on another HSM.

**TIP** Log entries are stored in the cryptographic module (HSM) until they are rotated off. Log entries are not rotated out of the cryptographic module *until* the audit user is initialized and audit logging is configured. By default, even if there is no audit user or configuration, the cryptographic module logs unconditional events within its own memory, like:

- > zeroize
- > decommission
- > hardware tamper
- > card removal
- > etc.

If the crypto module internal space ever fills completely with log records,

- > whether slowly from unconditional logs, or
- > quickly from more volatile high-volume event recording,

...the HSM / cryptographic module would *stop all operations* that were not `role init -name au` and `audit config`. The HSM would resume providing service only after the audit user cleared the logs.

To avoid that ever happening, configure audit logging to organize log parameters and handling, being sure to set sufficient frequency of rotation for the volume of record generation that you enable.

**Best practice** is to:

- > initialize the audit role as soon as the HSM is first powered on for production `role init -name au`
- > configure the log storage path on the external file system, along with the types of events to log, the rotation interval, etc. `audit config`
- > then, initialize the HSM Security Officer (this helps ensure that all messages, demanded by your auditing authority, are captured) `hsm init`
- > then, proceed with partition initialization and usage with your application(s)
- > then, *revisit* audit log configuration at regular intervals to tune the balance between
  - desired message types,
  - volume of audited actions normally performed (\*),
  - and so on
- > when you change behavior of the crypto module or change the types of events to audit, be sure to *revisit also* the rotation interval.

[\* Example, you might always want to record the generation of keys, but if usage of those keys is very high-volume (like in some signature use-cases), and thus would generate a high volume of log entries, it might be permissible, and prudent, to log only first-use of any key. Check with the relevant authority.]

## Event logging impacts HSM performance

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

## Audit limitations and Controlled tamper recovery state

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

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

## The Audit Role

A Luna USB HSM 7 Audit role allows complete separation of Audit responsibilities from the HSM Security Officer (HSM SO), the Crypto Officer(or User), and other HSM roles. If the Audit role is initialized, the HSM and Partition SOs are prevented from working with the log files, and auditors are unable to perform administrative tasks on the HSM. As a general rule, the Audit role should be created before the HSM Security Officer role, to ensure that all important HSM operations (including those that occur during initialization), are captured.

### Password-authenticated HSMs

For Luna USB HSM 7s with Password Authentication, the auditor role logs into the HSM to perform their activities using a password. After initializing the Audit role on a password-authenticated HSM, log in as the Auditor and set the domain (see [role setdomain](#)). This step is required before setting logging parameters or the log filepath, or importing/exporting audit logs.

### Multifactor Quorum-authenticated HSMs

For Luna USB HSM 7s with multifactor quorum authentication, the auditor role logs into the HSM to perform their activities using the Audit (white) iKey.

### Role Initialization

Creating the Audit role (and imprinting the white iKey for multifactor quorum-authenticated HSMs) does not require the presence or cooperation of the HSM SO.

### Audit Role Available Commands

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

```
lunacm:>audit
```

```
The following sub commands are available:
```

Command	Short	Description
verify	v	Verify a block of log messages

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

Syntax: audit <sub command>

Command Result : No Error

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

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

## Audit Log Secret

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

### Log Secret and Log Verification

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

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

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

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

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

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

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

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

## Audit Log Records

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

For the first log message ever returned from the HSM to the host there is no previous record and, therefore, no HMAC in flash. In this case, the previous HMAC is set to zero and the first HMAC is computed over the first log message concatenated with 32 zero-bytes. The first record in the log file then consists of the first log message plus 32 zero-bytes. The second record consists of the second message plus  $\text{HMAC}_1 = \text{HMAC}(\text{message}_1 || 0x0000)$ . 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 “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 time get**, 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 normal function of Audit logging is to export log entries constantly to the host 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

If you receive **CKR\_LOG\_FULL**, the log capacity has been reached, and all HSM operations will stop. This is to prevent the HSM from performing unlogged operations. In this condition, most HSM commands will not work; only commands that allow the Auditor to log in, clear the log storage, set the logging configuration, or reset the HSM to factory conditions are permitted.

See the later steps in ["Configuring Audit Logging" on page 110](#) for the procedure.

## Configuration Persists Unless Factory Reset is Performed

Audit logging configuration is not removed or reset upon HSM re-initialization or a tamper event. Factory reset or HSM decommission will remove the Audit user and configuration. Logs must be cleared by specific command. Therefore, if your security regime requires decommission at end-of-life, or prior to shipping an HSM, then explicit clearing of HSM logs should be part of that procedure.

This is by design, as part of separation of roles in the HSM. When the Audit role exists, the HSM SO cannot modify the logging configuration, and therefore cannot hide any activity from auditors.

## Audit Logging General Advice and Recommendations

---

The Security Audit Logging feature can produce a significant volume of data. It is expected, however, that Audit Officers will configure it properly for their specific operating environments. The data produced when the feature has been properly configured might be used for a number of reasons, such as:

- > Reconstructing a particular action or set of actions (forensics)
- > Tracing the actions of an application or individual user (accounting)
- > Holding a specific individual accountable for their actions (non-repudiation)

That last point represents the ultimate conclusion of any audit trail – to establish an irrefutable record of the chain of events leading up to a particular incident for the purpose of identifying and holding accountable the individual responsible. Not every organization will want to use security audit to meet the strict requirements of establishing such a chain of events. However, all security audit users will want to have an accurate representation of a particular sequence of events. To ensure that the audit log does contain an accurate representation of events and that it can be readily interpreted when it is reviewed, these basic guidelines should be followed after the audit logging feature has been properly configured:

- > Use a shell script to execute the `lunacm:> audit time sync` command at least once every 24 hours, provided the host has maintained its connection(s) to its configured NTP server(s).  
For newer firmware versions, that have HSM Policy **57 - Allow sync with host time**, you can initialize the time on the HSM, then set the policy on, to automatically sync the HSM with the local host every 24 hours.
- > Do not allow synchronization with the host's clock if the host has lost connectivity to NTP. This ensures that the HSM's internal clock is not set to a less accurate time than it has maintained internally. In general, the HSM's RTC will drift much less than the host's RTC and will, therefore, be significantly more accurate than the host in the absence of NTP.
- > Review logs at least daily and adjust configuration settings if necessary. It is important that any anomalies be identified as soon as possible and that the logging configuration that has been set is effective.
- > 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 logger daemon (PEDclient).**

> **pedclient mode stop**

> **pedclient mode start**

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

**TIP** Log entries are stored in the cryptographic module (HSM) until they are rotated off. Log entries are not rotated out of the cryptographic module *until* the audit user is initialized and audit logging is configured. By default, even if there is no audit user or configuration, the cryptographic module logs unconditional events within its own memory, like:

- > zeroize
- > decommission
- > hardware tamper
- > card removal
- > etc.

If the crypto module internal space ever fills completely with log records,

- > whether slowly from unconditional logs, or
- > quickly from more volatile high-volume event recording,

...the HSM / cryptographic module would *stop all operations* that were not `role init -name au` and `audit config`. The HSM would resume providing service only after the audit user cleared the logs.

To avoid that ever happening, configure audit logging to organize log parameters and handling, being sure to set sufficient frequency of rotation for the volume of record generation that you enable.

**Best practice** is to:

- > initialize the audit role as soon as the HSM is first powered on for production `role init -name au`
- > configure the log storage path on the external file system, along with the types of events to log, the rotation interval, etc. `audit config`
- > then, initialize the HSM Security Officer (this helps ensure that all messages, demanded by your auditing authority, are captured) `hsm init`
- > then, proceed with partition initialization and usage with your application(s)
- > then, *revisit* audit log configuration at regular intervals to tune the balance between
  - desired message types,
  - volume of audited actions normally performed (\*),
  - and so on
- > when you change behavior of the crypto module or change the types of events to audit, be sure to *revisit also* the rotation interval.

[\* Example, you might always want to record the generation of keys, but if usage of those keys is very high-volume (like in some signature use-cases), and thus would generate a high volume of log entries, it might be permissible, and prudent, to log only first-use of any key. Check with the relevant authority.]

## Configuring and Using Audit Logging

This section describes the procedures required to enable audit logging, configure it to specify what is logged and how often the logs are rotated, and how to copy, verify and read the audit logs. It contains the following information:

- > ["Configuring Audit Logging" below](#)
- > ["Exporting the Audit Logging Secret and Importing to a Verifying HSM" on the next page](#)
- > ["Audit Role Authentication Considerations" on page 113](#)

## Configuring Audit Logging

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

### To configure audit logging:

1. Configure the Luna USB HSM 7 host computer to use network time protocol (NTP).
2. Set the slot focus to the HSM administrative partition of the desired HSM:  
 lunacm:> **slot set -slot** <slotnum>
3. Initialize the Auditor role (you can also use the shortcut **au**). Specify a password if the HSM will be initialized to use password authentication. If you do not specify a password, multifactor quorum authentication will be used:  
 lunacm:> **role init -name Auditor [-password <password>]**  
 If you chose multifactor quorum authentication, you are referred to the touchscreen, which prompts for a white iKey.
4. Now that the Auditor role exists on the HSM, the auditing function must be configured. However, before you can configure you must log in as the Auditor user (you can also use the shortcut **au**):  
 lunacm:> **role login -name au**
  - On password-authenticated HSMs, you are prompted to enter the password for the Auditor user.
  - On multifactor quorum-authenticated HSMs, you are referred to the touchscreen, which prompts for the white iKey for the Auditor user.
5. Set the domain for the Audit role:  
 lunacm:> **role setdomain**
6. Synchronize the HSM's clock with the host time (which should also be synchronized with the NTP server) so that all subsequent log records will have a valid and accurate timestamp.  
 lunacm:> **audit time sync**
7. Set the filepath where log files are to be saved. You must complete this step before you can start event logging.  
 lunacm:> **audit config path** <filepath>  
 If you previously configured logging on the HSM and then made changes to your configuration that made that path invalid (such as deleting the path outside of LunaCM or reinstalling the HSM in a different host system), set a valid log path by running **audit config path** before restarting event logging. If the log path is set incorrectly, logs will be stored in the HSM's limited memory and not exported to the file system. Event logs may be lost if the HSM's memory runs out.
8. Configure audit logging to specify what you want to log. You can specify the level of audit appropriate for needs of the organization's policy and the nature of the application(s) using the HSM:  
 lunacm:> **audit config evmask** <event\_value>

**NOTE** Before you configure audit logging, we suggest using **audit config ?** to see all the available options in the configuration process.

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

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

As a further example, the command **audit config evmask all** will log everything the HSM does. This might be useful in some circumstances, but will quickly fill up log files.

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

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

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

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

lunacm:> **audit config size** <size>

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

**CAUTION!** This step is very important. If you do not configure the log rotation correctly, logs are stored on the HSM and have nowhere to go. If the logs fill up all available space on the HSM, most operations will fail with CKR\_LOG\_FULL, and cryptographic services will be interrupted.

See **audit config** for additional examples.

## Exporting the Audit Logging Secret and Importing to a Verifying HSM

You can export the audit log secret from one HSM and import it to another to allow the first HSM's logs to be viewed and verified on the second. The HSMs must share the same authentication method and Audit cloning domain (password string or red iKey). You can verify logs from a Luna PCIe HSM 7 using a Luna Network HSM 7, and vice-versa.

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

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

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

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

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

3. Transfer the logging secret to the HSM that will verify the logs. If you are verifying the logs with another locally-installed Luna USB HSM 7, skip this step.

- If you are planning to verify logs with a Luna USB HSM 7, use **pscp** or **sftp** to transfer the logging secret to the appliance. Provide the audit user's credentials when prompted.

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

- If you are planning to verify logs with a Luna USB HSM 7 installed in a different host computer, you can use **sftp**, **pscp**, or other secure means to transfer the logging secret.

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

4. Log in to the verifying HSM appliance as the **audit** user. For this example, we will assume that you have already initialized the HSM audit user role, using the same domain/secret as is associated with the source HSM.

- If you are using a Luna Network HSM 7, connect via SSH and log in to LunaSH as the **audit** user:

```
lunash:> audit login
```

- If you are using a Luna PCIe HSM 7 or Luna USB HSM 7, open LunaCM and log in using the Auditor role:

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

5. Import the audit logging secret to the HSM.

- Luna Network HSM 7 (LunaSH):

```
lunash:> audit secret import -serialtarget <target_HSM_SN> -serialsource <source_HSM_SN> -file <log_secret_file>
```

- Luna PCIe HSM 7 or Luna USB HSM 7 (LunaCM):

```
lunacm:> audit import file <log_secret_file>
```

6. You can now verify audit log files from the source HSM.

- Luna Network HSM 7 (LunaSH):

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

- Luna PCIe HSM 7 or Luna USB HSM 7 (LunaCM):

```
lunacm:> audit verify file <audit_log_filename>.log
```

You might need to provide the full path to the file, depending upon your current environment settings.

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

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

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

## Audit Role Authentication Considerations

- > The audit role iKey or password is a critical property to manage the audit logs. If that authentication secret is lost, the HSM must be factory reset (that is, zeroize the HSM) in order to initialize the audit role again.
- > Multiple bad logins produce different results for the HSM SO and for the audit role, as follows:
  - After 3 bad SO logins, the `LUNA_RET_SO_LOGIN_FAILURE_THRESHOLD` error is returned and the HSM is zeroized.
  - After 3 bad audit logins, the `LUNA_RET_AUDIT_LOGIN_FAILURE_THRESHOLD` error is returned, but the HSM is unaffected. If a subsequent login attempt is executed within 30 seconds, the `LUNA_RET_AUDIT_LOGIN_TIMEOUT_IN_PROGRESS` error is returned. If you wait for more than 30 seconds and try login again with the correct password, the login is successful.

## Logging In as Auditor

Before you can change the audit logging configuration, archive audit logs, or verify audit logs from another HSM, you must log in to the Luna USB HSM 7's Admin partition as Auditor (AU), or relevant commands will fail.

### To log in as Auditor

1. Launch LunaCM on the Luna USB HSM 7 host workstation.
2. Set the active slot to the HSM Admin partition.

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

3. Log in as Auditor.

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

You are prompted for the Auditor credential.

## Failed Auditor Login Attempts

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

**NOTE** The system must actually receive some erroneous/false information before it logs a failed attempt; if you merely forget to insert the iKey, or insert the wrong color key, that is not counted as a failed attempt. You must insert an incorrect iKey of the correct type, or enter an incorrect PIN or challenge secret, to fail a login attempt.

## Audit Log Categories and HSM Events

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

### Partition Role IDs

If you are using a Luna USB HSM 7 with Luna HSM Firmware 7.7.0 or newer and [Luna HSM Client 10.3.0](#) or newer, the HSM event log reports events with the following IDs assigned to each partition role:

#### Administrative Partition Role IDs

Partition Role	Role ID
Administrator	0
HSM Security Officer	1
Auditor	8

#### Application Partition Role IDs

Partition Role	Role ID
Partition Security Officer	1
Crypto Officer	0
Limited Crypto Officer	9
Crypto User	5

### HSM Access

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

HSM Event	Description
LUNA_LOGOUT_OTHER	C_LogoutOther. 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
LUNA_LOAD_CUSTOM_MODULE	CA_LoadModule
LUNA_LOAD_ENCRYPTED_CUSTOM_MODULE	CA_LoadEncryptedModule
LUNA_UNLOAD_CUSTOM_MODULE	CA_UnloadModule
LUNA_EXECUTE_CUSTOM_COMMAND	CA_PerformModuleCall
LUNA_HA_LOGIN	CA_HAGetLoginChallenge, CA_HAAnswerLoginChallenge, CA_HALogin, CA_HAAnswerMofNChallenge, HAActivateMofN

## Log External

HSM Event	Description
LUNA_LOG_EXTERNAL	CA_LogExternal

## HSM Management

HSM Event	Description
LUNA_ZEROIZE	CA_FactoryReset This event is logged unconditionally.
LUNA_INIT_TOKEN	C_InitToken This event is logged unconditionally.
LUNA_SET_PIN	C_SetPIN
LUNA_INIT_PIN	C_InitPIN
LUNA_CREATE_CONTAINER	CA_CreateContainer
LUNA_DELETE_CONTAINER	CA_DeleteContainer, CA_DeleteContainerWithHandle
LUNA_SEED_RANDOM	C_SeedRandom
LUNA_EXTRACT_CONTEXTS	C_GetOperationState
LUNA_INSERT_CONTEXTS	C_SetOperationState
LUNA_SELF_TEST	C_PerformSelfTest
LUNA_LOAD_CERT	CA_SetTokenCertificateSignature
LUNA_HA_INIT	CA_HAInit
LUNA_SET_HSM_POLICY	CA_SetHSMPolicy
LUNA_SET_DESTRUCTIVE_HSM_POLICY	CA_SetDestructiveHSMPolicy
LUNA_SET_CONTAINER_POLICY	CA_SetContainerPolicy
LUNA_SET_CAPABILITY	Internal, for capability update
LUNA_CREATE_LOGIN_CHALLENGE	CA_CreateLoginChallenge

HSM Event	Description
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
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

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

## Per-Key Authorization

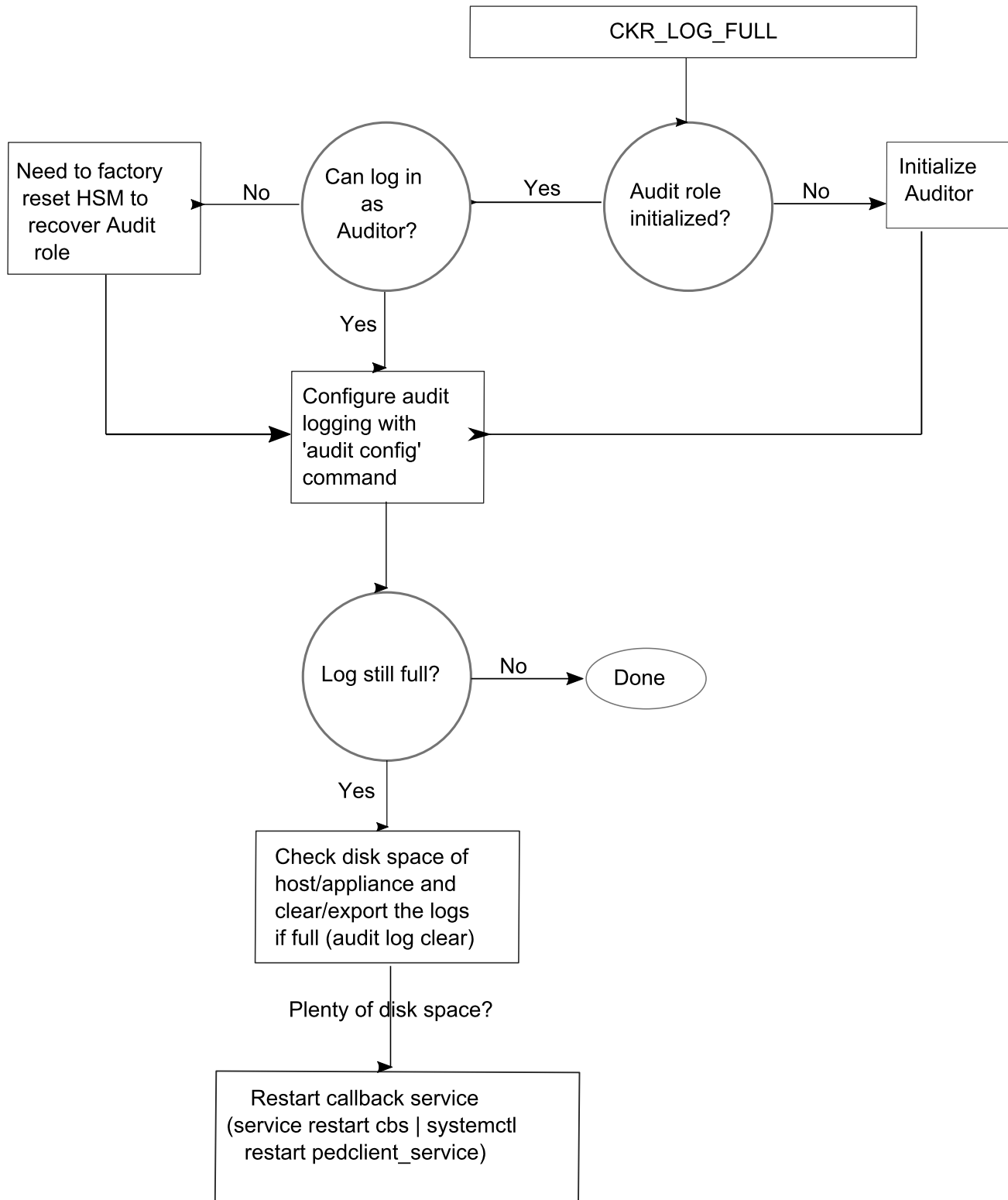
HSM Event	Description
LUNA_AUTHORIZE_KEY	<a href="#">CA_AuthorizeKey</a>
LUNA_SET_AUTHORIZATION_DATA	<a href="#">CA_SetAuthorizationData</a>
LUNA_RESET_AUTHORIZATION_DATA	<a href="#">CA_ResetAuthorizationData</a>
LUNA_ASSIGN_KEY	<a href="#">CA_AssignKey</a>
LUNA_INCREMENT_FAILED_AUTH_COUNT	<a href="#">CA_IncrementFailedAuthCount</a>

## Audit Log Management

HSM Event	Description
LUNA_LOG_SET_TIME	CA_TimeSync
LUNA_LOG_GET_TIME	CA_GetTime
LUNA_LOG_SET_CONFIG	CA_LogSetConfig This event must be allowed to proceed even if the result should be logged but cannot (for example, due to a log full condition).
LUNA_LOG_GET_CONFIG	CA_LogGetConfig This event must be allowed to proceed even if the result should be logged but cannot (for example, due to a log full condition).
LUNA_LOG_VERIFY	CA_LogVerify
LUNA_CREATE_AUDIT_CONTAINER **	CA_InitAudit The event is logged unconditionally.
LUNA_LOG_IMPORT_SECRET	CA_LogImportSecret
LUNA_LOG_EXPORT_SECRET	CA_LogExportSecret

## Audit Log Troubleshooting

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



## Cryptographic Operations Blocked During Remote PED Operations When Audit Logging Is Enabled

With audit logging enabled on the HSM, crypto operations are blocked on all application partitions during Remote PED operations. During this time, requests sent to HA member partitions on this HSM will not fail over to other members. When the Remote PED operation is complete, all crypto operations resume normally. If your application has its own timeout programmed, it may incorrectly conclude that the entire HA group has failed.

Using [Luna HSM Client 10.7.2](#) or newer, you can configure the ["ProbeTimeout" on page 62](#) setting in the **Chrystoki.conf/crystoki.ini** file to trigger an HA failover after a specified time. This allows operations to continue normally during Remote PED operations.

# CHAPTER 6: Initializing the Luna USB HSM 7

Initialization prepares a new Luna USB HSM 7 for use, or an existing HSM for reuse. You must initialize the HSM before you can generate and store objects, or perform cryptographic operations.

- > On a new or factory-reset Luna USB HSM 7, initialization sets the HSM Security Officer credentials (password string or USB iKey), the HSM label, and the cloning domain (password string or USB iKey) 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 HSM SO credentials and cloning domain (password strings or USB iKeys). You have the option to change or retain the existing label. This is sometimes referred to as a 'soft' initialization. See ["Re-initializing the Luna USB HSM 7" on page 126](#).

**NOTE** To ensure accurate auditing, perform initialization only after you have set the system time parameters (time, date, time zone, use of 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.

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

During the initialization procedure, you select password or multifactor quorum (iKey) authentication as your preferred authentication method. This cannot be changed later without destroying all cryptographic objects on the HSM. Ensure that you use the same method that the rest of your HSM deployment uses.

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

<b>HSM Label</b>	<p>The label is a string that uniquely identifies this HSM.</p> <p>The HSM label created during initialization must be 1-32 characters in length. If you specify a longer label, it will automatically be truncated to 32 characters. The following characters are allowed:</p> <pre>abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789 !@#\$%^&amp;*() -_ =+[]{} /;:'",.&lt;&gt;?`~</pre> <p>Spaces are allowed; enclose the label in double quotes if it includes spaces. Including both spaces and quotation marks in a label may cause unexpected labeling behavior.</p> <p>For more information, refer to <a href="#">"Name, Label, and Password Requirements" on page 129</a>.</p>
<b>HSM SO credentials</b>	<p>If you select multifactor quorum authentication (<b>-iped</b> option), you create a new HSM SO (blue) iKey (set) or re-use an existing key(set) from an HSM you want to share credentials with. If you are using multifactor quorum authentication, ensure that you have an iKey strategy before beginning. See <a href="#">"Multifactor Quorum Authentication" on page 82</a>.</p> <p>If you select password authentication (<b>-ipwd</b> option), you specify the HSM SO password. Employ standard password-security practices.</p> <div data-bbox="427 884 1394 1119" style="border: 1px solid #ccc; padding: 10px; margin: 10px 0;"> <p><b>NOTE</b> To <i>change</i> the authentication type of a Luna USB HSM 7 between Password auth and Multifactor Quorum auth, or the reverse, (with the <code>-ipwd</code> option or the <code>-iped</code> option of the <code>hsm init</code> command) requires a factory reset first (<a href="#">hsm factoryreset</a>).</p> <p>The factory reset is <i>not</i> needed if you are initializing the HSM to the same mode of authentication as is currently configured.</p> </div> <p>Passwords and activation challenge secrets must be 8-255 characters in length. Spaces are allowed; to specify a password with spaces using command-line options, enclose the password in double quotation marks. The space character may not be used as the first character in a password.</p> <p>The following characters are allowed:</p> <pre>!#\$%&amp;'()*+,-./0123456789:;=? @ABCDEFGHIJKLMNOPQRSTUVWXYZ[]^_`abcdefghijklmnopqrstuvwxyz{ }~</pre> <p>This character set is enforced when using <a href="#">Luna HSM Client 10.8.0</a> or newer, and recommended for all previous versions. Previously-set passwords and challenge secrets are unaffected, but the new character set is enforced when these passwords are changed.</p>

### Cloning domain for the HSM Admin partition

The cloning domain is a shared identifier that makes cloning possible among a group of HSM partitions. On the Luna 7 HSM Admin partition, it must be set, but has no practical function.

**NOTE** This is distinct from the domain on an application partition, which is a critical component required for key cloning, backup/restore, and high availability groups. Refer to [Domain Planning](#) for more information.

If you select multifactor quorum authentication (**-iped** option), you create a new Domain (red) iKey(set) or re-use an existing key(set) from an HSM you want to be able to clone with.

If you select password authentication (**-ipwd** option), you create a new domain string or re-use an existing string from an HSM you want to be able to clone with.

The domain string must be 1-128 characters in length. The following characters are allowed:

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

The following characters are problematic or invalid and must not be used in a domain string:

"& ; < > ? \ ` |

Spaces are allowed, as long as the leading character is not a space; to specify a domain string with spaces using the **-domain** option, enclose the string in double quotation marks.

For password-authenticated HSMs, the domain string should match the complexity of the partition password.

## Prerequisites

Before you begin, ensure that you are familiar with the concepts in the following sections

- > ["Multifactor Quorum Authentication" on page 82](#) (if you plan to use this authentication method)
- > ["HSM Roles" on page 127](#)

### To initialize a new or factory-reset HSM

1. Open a LunaCM session and set the active slot to the HSM Admin partition.
2. If Secure Transport Mode is set, you must unlock the HSM before proceeding. New Luna USB HSM 7s are shipped from the factory in Secure Transport Mode (STM). STM allows you to verify that an HSM has not been tampered while out of your possession, such as when it is shipped to another location, or placed into storage. See ["Secure Transport Mode" on page 78](#) for more information.  
  
To recover your HSM from Secure Transport Mode, follow the procedure in ["Recovering an HSM From Secure Transport Mode" on page 79](#).
3. If you are initializing the HSM to use multifactor quorum authentication, ensure that you have sufficient iKeys available.
4. Initialize the HSM, specifying a label for your Luna USB HSM 7 and your preferred method of authentication, password (**-ipwd**) or multifactor quorum (**-iped**):  
  
`lunacm:> hsm init -label <label> { -ipwd | -iped }`
5. Respond to the prompts to complete the initialization process:
  - If you selected password authentication, you are prompted to set the HSM SO password and the HSM Admin partition cloning domain string.

- If you selected multifactor quorum authentication, you receive the prompt "**Attend to the PED**". These operations are completed using the Luna USB HSM 7 touchscreen. Follow the instructions on the touchscreen to complete the initialization procedure. You can create MofN quorum keysets and duplicate keys as required. See "[Creating iKey Using Luna USB HSM 7](#)" on [page 87](#) for more information.

## Re-initializing the Luna USB HSM 7

On an initialized Luna USB HSM 7, re-initialization clears all existing partitions and objects, but retains the HSM 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 initialization. If you do not want to do a soft init, and also change the SO credentials and cloning domain, you reset the HSM to factory conditions using **hsm factoryreset**, and then perform the procedure described in "[Initializing a New or Factory-reset HSM](#)" on [page 123](#).

**CAUTION!** Ensure you have backups for any partitions and objects you want to keep, before re-initializing the HSM.

### To re-initialize the HSM (soft init)

1. Open a LunaCM session and set the slot to the HSM Admin partition.
2. Log in as the HSM SO.
3. If Secure Transport Mode is set, you must unlock the HSM before proceeding. See "[Recovering an HSM From Secure Transport Mode](#)" on [page 79](#).
4. If you are initializing a multifactor quorum-authenticated HSM, have the appropriate iKeys ready.
5. Re-initialize the HSM, specifying a label for your Luna USB HSM 7:

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

# CHAPTER 7: 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 client system, the HSM and the application partition
- > the actions each user is allowed to perform when logged in (the user's role)

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

Luna USB HSM 7 divides roles on the HSM according to an enhanced version of the PKCS#11 standard. Configuration, administration, and auditing of the HSM itself is the responsibility of the roles described below. Cryptographic functions take place on the application partition, which has a different set of independent roles (see [Partition Roles](#)).

Personnel holding the HSM roles described below access HSM functions by logging in to the Admin partition on the HSM using LunaCM. They must therefore have the appropriate Administrator access to the workstation hosting the Luna USB HSM 7.

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 Luna USB HSM 7" on page 123](#))
- > Setting and changing global HSM policies (see ["HSM Capabilities and Policies" on page 131](#))
- > Creating/deleting the application partition (see ["Application Partitions" on page 141](#))

### 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](#)

## Auditor (AU)

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

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

## Managing the Auditor Role

Refer to ["Configuring and Using Audit Logging" on page 109](#) for procedures involving the Auditor role. See also:

- > ["Logging In as Auditor" on page 113](#)
- > ["Changing a Role Credential" below](#)

## Administrator (AD)

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

## Logging In as HSM Security Officer

Before you can create an application partition or perform other administrative functions on the HSM, you must log in to the Luna USB HSM 7's Admin partition as HSM Security Officer (SO), or administrative commands will fail.

### To log in as HSM SO

1. Launch LunaCM on the Luna USB HSM 7 client workstation.
2. Set the active slot to the HSM Admin partition.
3. Log in as HSM SO.

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

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

You are prompted for the HSM SO credential.

## Failed HSM SO Login Attempts

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

**NOTE** The system must actually receive some erroneous/false information before it logs a failed attempt; if you merely forget to insert the iKey, or insert the wrong color key, that is not counted as a failed attempt. You must insert an incorrect iKey of the correct type, or enter an incorrect PIN or challenge secret, to fail a login attempt.

## Changing a Role Credential

From time to time, you may need to change the credential for a role. The credential might have been compromised, or your organization's security policy may mandate password changes after a specific time interval. The following procedure allows you to change the credential for a role (HSM SO, Auditor, Partition SO, Crypto Officer, Crypto User). You must first log in using the role's current credential.

**NOTE** If **partition policy 21: Force user PIN change after set/reset** is set to **1** (default), this procedure is required after initializing or resetting the CO or CU role and/or creating a challenge secret.

## To change a role credential

1. In LunaCM, log in using the role's current credential (see [Logging In to the Application Partition](#)).

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

2. Change the credential for the logged-in role. If you are using a password-authenticated HSM, specify a new password. If you are using a multifactor quorum-authenticated HSM, ensure that you have a blank or rewritable iKey available. Refer to ["Creating iKey Using Luna USB HSM 7" on page 87](#).

Passwords and activation challenge secrets must be 8-255 characters in length. Spaces are allowed; to specify a password with spaces using command-line options, enclose the password in double quotation marks. The space character may not be used as the first character in a password. The following characters are allowed:

```
!#$% '()*+,-./0123456789:;=? @ABCDEFGHIJKLMNopQRSTUVWXYZ[]^_abcdefghijklmnopqrstuvwxyz{|}~
```

This character set is enforced when using [Luna HSM Client 10.8.0](#) or newer, and recommended for all previous versions. Previously-set passwords and challenge secrets are unaffected, but the new character set is enforced when these passwords are changed.

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

3. To change the CO or CU challenge secret for an activated multifactor quorum-authenticated partition, specify the **-oldpw** and/or **-newpw** options.

```
lunacm:> role changepw -name <role> -oldpw <oldpassword> -newpw <newpassword>
```

## Name, Label, and Password Requirements

This page describes length and character requirements for setting labels, domains, passwords, and challenge secrets on the Luna USB HSM 7. This information can also be found in relevant sections throughout the documentation. Refer to the applicable section below:

- > ["HSM Labels" below](#)
- > ["Cloning Domains" on the next page](#)
- > ["Partition Labels" on the next page](#)
- > ["Role Passwords or Challenge Secrets" on the next page](#)

### HSM Labels

The HSM label created during initialization must be 1-32 characters in length. If you specify a longer label, it will automatically be truncated to 32 characters. The following characters are allowed:

```
abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789 !@#$%^&*()-_+=[]{}|/;/:'",.<>?`~
```

Spaces are allowed; enclose the label in double quotes if it includes spaces. Including both spaces and quotation marks in a label may cause unexpected labeling behavior.

## Cloning Domains

The domain string must be 1-128 characters in length. The following characters are allowed:

abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789 !@#\$%^\*\_+[]{}()/:',.~

The following characters are problematic or invalid and must not be used in a domain string: "&;<>?\`|

Spaces are allowed, as long as the leading character is not a space; to specify a domain string with spaces using the **-domain** option, enclose the string in double quotation marks.

For password-authenticated HSMs, the domain string should match the complexity of the partition password.

## Partition Labels

In LunaCM, the partition label created during initialization must be 1-32 characters in length. If you specify a longer label, it will automatically be truncated to 32 characters. The following characters are allowed:

abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789 !@#\$%^&\*()-\_+=[]{} \ | / ; : ' , . < > ` ~

Spaces are allowed; enclose the label in double quotation marks if it includes spaces.

## Role Passwords or Challenge Secrets

Passwords and activation challenge secrets must be 8-255 characters in length. Spaces are allowed; to specify a password with spaces using command-line options, enclose the password in double quotation marks. The space character may not be used as the first character in a password.

The following characters are allowed:

!#\$% ' ( ) \* + , - . / 0 1 2 3 4 5 6 7 8 9 : = ? @ A B C D E F G H I J K L M N O P Q R S T U V W X Y Z [ ] ^ \_ a b c d e f g h i j k l m n o p q r s t u v w x y z { } ~

This character set is enforced when using [Luna HSM Client 10.8.0](#) or newer, and recommended for all previous versions. Previously-set passwords and challenge secrets are unaffected, but the new character set is enforced when these passwords are changed.

## CHAPTER 8: HSM Capabilities and Policies

The Luna USB HSM 7 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 time of manufacture. 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 application partitions by the Partition Security Officer.

The table below describes all Luna USB HSM 7 capabilities, their corresponding policies, and the results of changing their settings. This section contains the following procedures:

- > ["Setting HSM Policies Manually" on page 138](#)
- > ["Setting HSM Policies Using a Template" on page 138](#)

To zeroize the HSM and revert policies to their default values, see ["Zeroizing or Resetting the HSM to Factory Conditions" on page 186](#).

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

### Destructive Policies

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

#	HSM Capability	HSM Policy
0	<b>Enable PIN-based authentication</b> Always <b>1</b> . The HSM can authenticate users with keyboard-entered passwords.	<b>PIN-based authentication</b> Displays <b>1</b> if you chose password authentication at the time of HSM initialization.
1	<b>Enable PED-based authentication</b> Always <b>1</b> . The HSM can authenticate users with secrets stored on physical iKeys (multifactor quorum authentication) inserted into the Luna USB HSM 7. The Crypto Officer and Crypto User roles may also be configured with a secondary, keyboard-entered challenge secret.	<b>PED-based authentication</b> Displays <b>1</b> if you chose multifactor quorum authentication at the time of HSM initialization.
2	<b>Performance level</b> This value is standard on all Luna USB HSM 7s.	N/A

#	HSM Capability	HSM Policy
4	<b>Enable domestic mechanisms &amp; key sizes</b> Always 1. All Luna USB HSM 7s are capable of full-strength cryptography with no US export restrictions.	N/A
6	<b>Enable masking</b> Always 1.	<b>Allow Masking</b>
7	<b>Enable cloning</b> Always 1. All current Luna USB HSM 7s have the ability to clone cryptographic objects from one partition to another.	<b>Allow cloning</b> <i>Destructive</i> <ul style="list-style-type: none"> <li>&gt; <b>1</b> (default): The HSM may clone cryptographic objects from one partition to another sharing the same cloning domain. This is required to back up partitions. The Partition SO can enable/disable cloning on individual partitions.</li> <li>&gt; <b>0</b>: The application partition may not clone cryptographic objects. The Partition SO cannot change this.</li> </ul>
9	<b>Enable full (non-backup) functionality</b> Always 1. The Luna USB HSM 7 is capable of full cryptographic functions.	N/A
12	<b>Enable non-FIPS algorithms</b> Always 1. The HSM can use all cryptographic algorithms described in <a href="#">Supported Mechanisms</a> .	<b>Allow non-FIPS algorithms</b> <i>Destructive</i> <ul style="list-style-type: none"> <li>&gt; <b>1</b> (default): The HSM may use all available cryptographic algorithms, meaning all the FIPS-approved algorithms as well as non-FIPS algorithms.</li> <li>&gt; <b>0</b>: Only algorithms sanctioned by the FIPS 140 standard are permitted. Some of these algorithms will have certain operations restricted; refer to your firmware version in <a href="#">Supported Mechanisms</a> for more information.</li> </ul>

#	HSM Capability	HSM Policy
15	<b>Enable SO reset of partition PIN</b> Always <b>1</b> . This capability enables: <ul style="list-style-type: none"> <li>&gt; the Partition SO to reset the password or iKey secret of the Crypto Officer.</li> <li>&gt; the Crypto Officer to reset the password or iKey secret of the Crypto User.</li> </ul>	<b>SO can reset partition PIN</b> <i>Destructive</i> <ul style="list-style-type: none"> <li>&gt; <b>1</b>: Partition SO may reset the password or iKey secret of a Crypto Officer who has been locked out after too many failed login attempts.</li> <li>&gt; <b>0</b> (default): The CO lockout is permanent and the partition contents are no longer accessible. The partition must be re-initialized, and key material restored from a backup device.</li> </ul> See <a href="#">Resetting the Crypto Officer or Crypto User Credential</a> .
16	<b>Enable network replication</b> Always <b>1</b> . This capability enables cloning of cryptographic objects over a network. This is required for partition backup to a remote Luna Backup HSM.	<b>Allow network replication</b> <ul style="list-style-type: none"> <li>&gt; <b>1</b> (default): Cloning of cryptographic objects is permitted over a network. Remote backup is allowed.</li> <li>&gt; <b>0</b>: Cloning over a network is not permitted. Partition backup is possible to a locally-connected Luna Backup HSM only.</li> </ul>
17	<b>Enable Korean Algorithms</b> Always <b>0</b> . The Korea-specific algorithm set is not currently available for Luna USB HSM 7.	N/A
19	<b>Manufacturing Token</b> Always <b>0</b> . For Thales internal use only.	N/A
21	<b>Enable forcing user PIN change</b> Always <b>1</b> . This capability forces the Crypto Officer or Crypto User to change the initial role credential created by the Partition SO.	<b>Force user PIN change after set/reset</b> <ul style="list-style-type: none"> <li>&gt; <b>1</b> (default): After the Partition SO initializes or resets the Crypto Officer credential, the CO must change the credential before any other actions are permitted. This also applies when the CO initializes/resets the Crypto User role. This policy is intended to enforce the separation of roles on the partition.</li> <li>&gt; <b>0</b>: The CO/CU may continue to use the credential assigned by the Partition SO.</li> </ul> See <a href="#">"Changing a Role Credential" on page 128</a> .

#	HSM Capability	HSM Policy
22	<b>Enable offboard storage</b> Always <b>1</b> .	<b>Allow offboard storage</b> <i>Destructive</i> Deprecated policy. On previous HSMs, this policy allowed or disallowed the use of the portable SIM key. Default: <b>1</b>
23	<b>Enable partition groups</b> Always <b>0</b> - deprecated capability.	N/A
25	<b>Enable Remote PED usage</b> Always <b>1</b> .	<b>Allow Remote PED usage</b> <ul style="list-style-type: none"> <li>&gt; <b>1</b> (default): When initialized for multifactor quorum authentication, the HSM may authenticate roles using a remotely-located Luna PED server.</li> <li>&gt; <b>0</b>: The HSM can authenticate roles by connecting iKeys directly to the Luna USB HSM 7 only.</li> </ul>
27	<b>HSM non-volatile storage space</b> Displays the maximum non-volatile storage space (in bytes) on the HSM.	N/A
30	<b>Enable Unmasking</b> Always <b>1</b> . This capability enables migration from legacy Luna HSMs that used SIM.	<b>Allow unmasking</b> <ul style="list-style-type: none"> <li>&gt; <b>1</b> (default): Cryptographic objects may be migrated from legacy Luna HSMs that used SIM.</li> <li>&gt; <b>0</b>: Migration from legacy HSMs using SIM is not possible.</li> </ul>
33	<b>Maximum number of partitions</b> Always <b>1</b> . Displays the maximum number of application partitions that can be created on the Luna USB HSM 7.	<b>Current maximum number of partitions</b> N/A
35	<b>Enable Single Domain</b> Always <b>0</b> . Not applicable to Luna USB HSM 7.	N/A
36	<b>Enable Unified PED Key</b> Always <b>0</b> . Not applicable to Luna USB HSM 7.	N/A

#	HSM Capability	HSM Policy
37	<b>Enable MofN</b> Always <b>1</b> .	<b>Allow MofN</b> <ul style="list-style-type: none"> <li>&gt; <b>1</b> (default): During iKey creation, you have the option to require a quorum to authenticate the role, by splitting the role secret among multiple iKeys. See <a href="#">"M of N Split Secrets (Quorum)" on page 86</a>.</li> <li>&gt; <b>0</b>: Users do not have the option to split role secrets (M and N are automatically set to <b>1</b>).</li> </ul>
38	<b>Enable small form factor backup/restore</b> Always <b>0</b> . Not applicable to Luna USB HSM 7.	N/A
40	<b>Enable decommission on tamper</b> Always <b>0</b> . Not applicable to Luna USB HSM 7.	N/A
42	<b>Enable partition re-initialize</b> Always <b>0</b> . Not applicable to Luna USB HSM 7.	N/A
43	<b>Enable low level math acceleration</b> Always <b>1</b> . This capability enables acceleration of cryptographic functionality for maximum HSM performance.	N/A
46	<b>Allow Disabling Decommission</b> Always <b>0</b> . Not applicable to Luna USB HSM 7.	N/A
48	<b>Enable Controlled Tamper Recovery</b> Always <b>0</b> . Not applicable to Luna USB HSM 7.	N/A
49	<b>Enable Partition Utilization Metrics</b> Always <b>1</b> . This capability enables the HSM SO to view (or export to a named file) counters that record how many times specific cryptographic operations have been performed in the application partition since the last counter-reset event.	<b>Allow Partition Utilization Metrics</b> <ul style="list-style-type: none"> <li>&gt; <b>1</b>: The HSM SO can view Partition Utilization Metrics.</li> <li>&gt; <b>0</b> (default): Partition Utilization Metrics are not available.</li> </ul> See <a href="#">"Partition Utilization Metrics" on page 153</a> for more information.
50	<b>Enable Functionality Modules</b> Always <b>0</b> . Not applicable to Luna USB HSM 7.	N/A
51	<b>Enable SMFS Auto Activation</b> Always <b>0</b> . Not applicable to Luna USB HSM 7.	N/A

#	HSM Capability	HSM Policy
52	<b>Allow Restricting FM Privilege Level</b> Always <b>0</b> . Not applicable to Luna USB HSM 7.	N/A
53	<b>Allow Encrypting of Keys from FM to HSM</b> Always <b>0</b> . Not applicable to Luna USB HSM 7.	N/A
55	<b>Enable Restricted Restore</b> Always <b>0</b> . Not applicable to Luna USB HSM 7.	N/A

#	HSM Capability	HSM Policy
56	<p><b>Enable User Defined ECC Curves</b></p> <p>Always 1. This capability allows the HSM SO to restrict or allow the use of user-defined ECC curves.</p> <p>The state of the associated policy is preserved through firmware update.</p> <p>Requires <a href="#">Luna USB HSM 7 Firmware 7.7.3</a> or newer.</p>	<p><b>Allow User Defined ECC Curves</b></p> <p><i>Destructive</i></p> <ul style="list-style-type: none"> <li>&gt; : User-defined ECC curves can be used, without restriction.</li> <li>&gt; (default): Named curves (that we have verified) can still be used, as can user-defined ECC curves where the named-curve parameters are provided. User-defined ECC curves that cannot map to built-in named curves during key-pair generation, public key creation, private key unwrapping, cloning or SKS, and key derivation, return the error ECC_CURVE_NOT_ALLOWED.</li> </ul> <p>Named-curve samples are provided when you include the SDK option while installing the Client. The files must be unmodified.</p> <p>/usr/safenet/lunaclient/samples/ecc_examples</p> <ul style="list-style-type: none"> <li>&gt; bpP160r1.txt</li> <li>&gt; bpP512t1.txt</li> <li>&gt; x962_char2_163v1.txt</li> <li>&gt; bpP192r1.txt</li> <li>&gt; secp384r1.txt</li> <li>&gt; x962_char2_359V1.txt</li> <li>&gt; bpP224r1.txt</li> <li>&gt; bpP384R1.txt</li> <li>&gt; sm2p256v1.txt</li> </ul> <div style="border: 1px solid black; padding: 10px; margin-top: 10px;"> <p><b>NOTE</b> For FIPS compliance, NIST requires us to make security claims with respect to the curves that we support.</p> <p>It is impossible to test and report on all possible user-defined ECC curves. Therefore, commonly-used, named curves are explicitly tested, documented to comply with FIPS requirements, and allowed in FIPS 140 approved configuration.</p> </div>

## 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 131](#) 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 Luna USB HSM 7" on page 123](#)).
- > If you are changing a destructive policy and you have partitions existing on the HSM, back up any important cryptographic objects (see [Partition Backup and Restore](#)).

### To manually set or change an HSM policy

1. Launch LunaCM and set the active slot to the HSM Admin partition.

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

2. [Optional] Display the existing HSM policy settings.

```
lunacm:> hsm showpolicies
```

3. Log in as HSM SO (see ["Logging In as HSM Security Officer" on page 128](#)).

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

4. Change the policy setting by specifying the policy number and the desired value (**0**, **1**, or a number in the accepted range for that policy).

```
lunacm:> hsm changehsmpolicy -policy <policy_ID> -value <value>
```

If you are changing a destructive policy, you are prompted to enter **proceed** to continue the operation.

## Setting HSM Policies Using a Template

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

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

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 ["Zeroizing or Resetting the HSM to Factory Conditions" on page 186](#).

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

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

- > ["Creating an HSM Policy Template" 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. Launch LunaCM and set the active slot to the Admin partition. If you are creating a template from an initialized HSM, you must log in as HSM SO.

```
lunacm:> slot set slot <admin_slotnum>
```

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

2. Create the HSM policy template file with an original filename. Specify the path to the location where you wish to save the template. No file extension is required. If a template file with the same name exists in the specified directory, it is overwritten.

```
lunacm:> hsm showpolicies -exporttemplate <filepath/filename>
```

```
lunacm:>hsm showpolicies -exporttemplate /usr/safenet/lunaclient/templates/HSMPT
```

```
HSM policies for HSM: myPCIeHSM written to /usr/safenet/lunaclient/templates/HSMPT
```

```
Command Result : No Error
```

3. Customize the template file with a standard text editor (see ["Editing an HSM Policy Template" below](#)).

## Editing an HSM Policy Template

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

### HSM Policy Template Example

This example shows the contents of an HSM policy template created using the factory default policy settings. Use a standard text editor to change the policy values (0=OFF, 1=ON, or the desired value 0-255). You cannot edit the destructiveness of HSM policies. See ["HSM Capabilities and Policies" on page 131](#) 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.

```
# HSM Policy template FW Version 7.7.2
# Sourced from HSM: myLunaUSB, SN: 556677
# Field format - Policy ID:Policy Description:Policy Value
```

```
6:"Allow masking":1
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
25:"Allow remote PED usage":1
30:"Allow unmasking":1
33:"Current maximum number of partitions":1
37:"Allow MofN":1
43:"Allow low level math acceleration":1
49:"Allow Partition Utilization Metrics":0
56:"Allow User Defined ECC Curves":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 35: Enable Single Domain** is always **Disallowed**, so you cannot set the corresponding HSM policy to **1**. If you attempt to initialize an HSM with a template containing invalid policy values, an error is returned and initialization fails.

## Applying an HSM Policy Template

The following procedure describes how to initialize the HSM using a policy template.

### To apply a policy template to a new HSM

1. Ensure that the template file is saved on the workstation hosting the destination HSM.
2. Launch LunaCM and initialize the destination HSM using the policy template file. If the template file is not in the same directory as LunaCM, include the correct filepath.

```
lunacm:> hsm init -label <label> -applytemplate <filepath/filename>
```

3. Verify that the template has been applied correctly by checking the partition's policy settings.

```
lunacm:> hsm showpolicies
```

# CHAPTER 9: Application Partitions

The Luna USB HSM 7 has two partitions:

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

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

## Creating the Application Partition

The HSM Security Officer (SO) is responsible for creating the application partition.

### Prerequisites

- > The HSM must be initialized (see ["Initializing the Luna USB HSM 7" on page 123](#)).
- > You require the HSM SO credential (password or blue iKey).

#### To create the application partition on the Luna USB HSM 7

1. Log in as HSM SO (see ["Logging In as HSM Security Officer" on page 128](#)).  
lunacm:> **role login -name so**
2. Create the application partition, specifying a slot number to associate with it. You can optionally specify a V1 partition using the **-version** option, or a V0 partition is created by default. You can also convert V0 to V1 after initialization (see [V0 and V1 Partitions](#)).  
lunacm:> **partition create -slot <slotnum> [-version 1]**
3. [Optional] Confirm that the partition was created.  
lunacm:> **slot list**

## Deleting the Application Partition

The HSM SO can delete the partition at any time, destroying all partition roles and stored cryptographic objects.

### To delete the application partition

1. Log in as HSM SO (see "[Logging In as HSM Security Officer](#)" on page 128).

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

2. Delete the application partition by specifying the slot number.

lunacm:> **partition delete** -slot <slot>

# CHAPTER 10: Security in Operation

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

- > ["Physical Security and Tamper Events" below](#)
- > ["Tamper Events" on the next page](#)
- > ["Security Effects of Administrative Actions" on page 145](#)

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

## Physical Security and Tamper Events

The Luna USB HSM 7 (the cryptographic module) contains a single battery to keep the time clock up to date.

By design, that battery will last longer than the life expectancy of the device. The following notes pertain:

- > Should the battery fail, then the time must be set before using the device.
- > The presence or absence of a working battery has no impact on the key materials.
- > Key materials are accessible only when
  - the HSM is powered on -- there is no way to extract key material from a powered-off Luna USB HSM 7,
  - the user has been successfully authenticated -- there is no way to extract key material from a Luna USB HSM 7 without the appropriate user authentication (either by password or by multi-factor quorum [PED] ).
- > Tamper detection is enabled when the unit is powered on.
- > Physical intrusion is prevented by an epoxy layer applied on components where the key materials reside.
- > Both temperature and voltage are monitored, and the cryptographic module shuts down while any environmental conditions are outside of normal allowed operating ranges:
  - Temperature -- Environmental Failure Protection (EFP) temperature events are detected by an internal temperature sensor.

Under Temperature	Over Temperature
Soft Tamper	Soft Tamper
0°C ± 2°C	+70°C ± 2°C

- Voltage -- the module monitors the 5V power rail

Under Voltage	Over Voltage
Halt	Soft Tamper
3.9V ± 0.11V	5.71V ± 0.145V

## Tamper Events

Luna USB HSM 7 detects hardware anomalies (such as card over-temperature) and registers them as tamper events.

Tamper event	Response
Over/under temperature	<p>Halt the HSM. Deactivate activated partitions.</p> <p>Decommission the HSM if <b>policy 40: Decommission on Tamper</b> is enabled.</p> <p>Warnings are logged for mild over/under temperature events. Warnings are self-clearing if the condition is resolved.</p>
Over/under voltage	<p>Halt the HSM. Deactivate activated partitions.</p> <p>Decommission the HSM if <b>policy 40: Decommission on Tamper</b> is enabled.</p> <p>Warnings are logged for mild over/under voltage events. Warnings are self-clearing if the condition is resolved.</p>

## Recovering from a Tamper Event

If you are using activation on your multifactor quorum-authenticated partitions, it is disabled when a tamper is detected, or if any uncleared tamper conditions are detected on reboot. See [Activation on Multifactor Quorum-Authenticated Partitions](#) and [Partition Capabilities and Policies](#) for more information.

### To recover from a tamper

1. View the output of `lunacm:> slot list` (displayed by default on login). The reason for the tamper is indicated by the **HSM Status** field. You can also use `lunacm:> hsm tampershow` to display the last tamper event.

**NOTE** The `slot list` and `hsm tampershow` commands only show the last tamper event, even if several tampers have occurred.

2. Resolve the issue(s) that caused the tamper event.
3. If the tamper message indicates that a reset is required, exit LunaCM and use the `lunareset` utility to reset the HSM.

`lunareset <device>`

4. Verify that all tampers have been cleared:

`lunacm:> hsm tampershow`

5. If the **Policy 22: Allow Activation** and/or **Policy 23: Allow AutoActivation** are enabled on your multifactor quorum-authenticated partitions, the CO and CU (if enabled) must log in to reactivate those roles:

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

## Security Effects of Administrative Actions

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

### Overt Security Actions

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

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

Those are discussed in their own sections.

### Actions with Security- and Content-Affecting Outcomes

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

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

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

#### Factory Reset HSM

<b>Domain</b>	Destroyed
<b>HSM SO Role</b>	Destroyed
<b>Partition SO Role</b>	Destroyed
<b>Auditor Role</b>	Destroyed
<b>Partition Roles</b>	Destroyed

<b>HSM or Partition/Contents</b>	HSM/Destroyed
<b>HSM Policies</b>	Reset
<b>RPV</b>	Destroyed
<b>Messaging</b>	You are about to factory reset the HSM. All contents of the HSM will be destroyed. HSM policies will be reset and the remote PED vector will be erased.

### Zeroize HSM

<b>Domain</b>	Destroyed
<b>HSM SO Role</b>	Destroyed
<b>Partition SO Role</b>	Destroyed
<b>Auditor Role</b>	Unchanged
<b>Partition Roles</b>	Destroyed
<b>HSM or Partition/Contents</b>	HSM/Destroyed
<b>HSM Policies</b>	Unchanged
<b>RPV</b>	Unchanged
<b>Messaging</b>	You are about to zeroize the HSM. All contents of the HSM will be destroyed. HSM policies, remote PED vector and Auditor left unchanged.

### Change Destructive HSM Policy

<b>Domain</b>	Unchanged
<b>HSM SO Role</b>	Unchanged
<b>Partition SO Role</b>	Destroyed
<b>Auditor Role</b>	Unchanged
<b>Partition Roles</b>	Destroyed
<b>HSM or Partition/Contents</b>	HSM/Destroyed
<b>HSM Policies</b>	Unchanged except for new policy
<b>RPV</b>	Unchanged

<b>Messaging</b>	You are about to change a destructive HSM policy. All partitions of the HSM will be destroyed.
------------------	--

### HSM Initialize When Zeroized (hard init)

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

### HSM Initialize From Non-Zeroized State (soft init)

<b>Domain</b>	Unchanged
<b>HSM SO Role</b>	Unchanged
<b>Partition SO Role</b>	Destroyed
<b>Auditor Role</b>	Unchanged
<b>Partition Roles</b>	Destroyed
<b>HSM or Partition/Contents</b>	HSM/Destroyed
<b>HSM Policies</b>	Unchanged
<b>RPV</b>	Unchanged
<b>Messaging</b>	You are about to initialize the HSM that is already initialized. All partitions of the HSM will be destroyed. You are required to provide the current SO password.

**Partition Initialize When Zeroized (hard init)**

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

**Partition Initialize From Non-Zeroized State (soft init)**

<b>Domain</b>	Unchanged
<b>HSM SO Role</b>	Unchanged
<b>Partition SO Role</b>	Destroyed
<b>Auditor Role</b>	Unchanged
<b>Partition Roles</b>	Destroyed
<b>HSM or Partition/Contents</b>	Partition/Destroyed
<b>HSM Policies</b>	Unchanged
<b>RPV</b>	Unchanged
<b>Messaging</b>	You are about to initialize the partition that is already initialized. All contents of the partition will be destroyed. You are required to provide the current Partition SO password.

**Elsewhere**

Certain other actions can sometimes cause collateral changes to the HSM, like firmware update. They usually do not affect contents, unless a partition is full and the action changes the size of partitions or changes the amount of space-per-partition that is taken by overhead/infrastructure. These are discussed elsewhere.

# CHAPTER 11: 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 152](#)
- > ["Partition Utilization Metrics" on page 153](#)
- > ["Cryptographic Module and Token Return Codes" on page 154](#)
- > ["Library Codes" on page 172](#)
- > ["Vendor-Defined Return Codes" on page 176](#)

## HSM Status Values

Each HSM administrative slot shown in a LunaCM slot listing includes an HSM status. Here are the possible values and what they mean, and what is required to recover from each one.

Indicated Status of HSM	Meaning	Recovery
OK	The HSM is in a good state, working properly.	n/a
Zeroized	The HSM is in zeroized state. All objects and roles are unusable.	HSM initialization is required before the HSM can be used again. "Hard init" - HSM SO and domain are gone, no authentication required. (see Note1)
Decommissioned	The HSM has been decommissioned.	HSM initialization is required before the HSM can be used again. "Hard init" - HSM SO and domain are gone, no authentication required. (see Note1)
Transport Mode	The HSM is in Secure Transport Mode.	STM must be disabled before the HSM can be used.
Transport Mode, zeroized	The HSM is in Secure Transport Mode, and is also zeroized.	STM must be disabled, and then HSM initialization is required before the HSM can be used.

Indicated Status of HSM	Meaning	Recovery
Transport Mode, Decommissioned	The HSM is in Secure Transport Mode, and has been decommissioned.	STM must be disabled, and then HSM initialization is required before the HSM can be used.
Hardware Tamper	The HSM has been tampered. (MTK is destroyed and must be rebuilt from recovery vectors.)	Reboot the host or restart the HSM. 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. 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. 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 Luna USB HSM 7" on page 123](#) for more information.

# 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 'placeholder' slots that might later be filled by a physical Luna USB HSM 7 or a Luna Backup HSM.

In the Chrystoki.conf file (or the Windows crystoki.ini file), for Luna USB HSM 7, you can remove the empty slots by modifying the CardReader entry, like this:

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

For Luna Network HSM 7, which has its configuration file internal to the appliance, and not directly accessible for modification, you cannot change the default cryptographic slot allotments.

## Error: 'hsm update firmware' failed. (10A0B : LUNA\_RET\_OPERATION\_RESTRICTED) when attempting to perform hsm update firmware

You must ensure that STM is disabled before you run the firmware update.

Also, as with any update, you should backup any important HSM contents before proceeding.

## LUNA\_RET\_OPERATION\_RESTRICTED when attempting to perform a restore operation

Did you perform the backup before Functionality Modules (FMs) were enabled on the HSM? Enabling FMs allows injection of software into the HSM, which makes it inherently less secure than an HSM that has never had FMs enabled. The cloning operation (used to perform backup and restore) recognizes the state of the source and target devices, and can refuse to transfer objects from a more secure device to a less-secure device.

In general, to ensure that you will be able to backup and restore (with partition archive commands) or clone directly with clone commands or include partitions in HA groups (which also uses cloning), ensure that partition policies are set the same on the involved partitions.

## KR\_ECC\_POINT\_INVALID Error when decrypting a file encrypted from BSAFE through ECIES using ECC key with any of the curves from the x9\_t2 section

As indicated on the BSAFE web site, they support only the NIST-approved curves (prime, Binary, and Koblitz). That includes most/all the curves from test items 0 through 37 in CK Demo: the "secp", "X9\_62\_prime", and "sect" curves.

The X9.62 curves that are failing in this task are X9.62 binary/char2 curves which do not appear to be supported by BSAFE. So, you appear to be encountering a BSAFE limitation and not a Luna HSM problem.

## 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.

## Performance Monitoring

---

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

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

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

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

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

By watching trends and correlating with what your application is doing, you can:

- > Determine the kinds of loads you are placing on the HSM.
- > Seek efficiencies in how your applications are coded and configured.
- > Plan for expansion or upgrades of your existing HSM infrastructure.
- > Plan for upgrades of electrical capacity and HVAC capacity.

## Notes about Monitor/Counter Behavior

When performing certain operations the HSM reaches its maximum performance capability before the counter reaches 100%. This occurs because the counter measures the load on the HSM's CPU and the CPU is able to saturate the asymmetric engines and still have capacity to perform other actions.

Also, symmetric cryptographic operations cause the counter to quickly rise to 90% even though there is significant remaining capacity. This behavior occurs because, as the HSM receives more concurrent symmetric commands, its CPU is able to handle them more efficiently (by performing them in bulk) – thus achieving more throughput from the same number of CPU cycles.

See lunacm:> [hsm monitor](#).

## Partition Utilization Metrics

---

In order to ensure the quality of service (QoS) that you provide to applications that make use of HSM partitions, it is first necessary to know how the users and applications are making use of the HSM resources - that is, the distribution of demand.

For an HSM with a single application partition, it can be helpful to know what type of load is being imposed on the HSM and the enumeration and categorization of operations that are being performed. Application developers might have a good idea of the expected ratio of operations, but the operations team managing the application servers would like to know the real-world utilization, for their planning and management purposes.

### 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.
- > Using and Luna HSM Firmware 7.8.9 or newer, you can now choose whether "[Partition Utilization Metrics](#)" [above](#) can be viewed/exported and reset without needing login to the HSM. For continuity, the option defaults to requiring SO login, but that can be changed with a single command, to suit your security and auditing regimes. The existing QoS commands function as previously; only access to them is affected. This option is set using **HSM Policy 58: [Allow Unrestricted Metrics Access](#)**.

## 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 (zero) 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 using HSM-level policy **49: Allow Partition Utilization Metrics**. That policy is off (value 0) by default, as it is not required in all use-cases, and is most useful where multiple applications use the HSM.

**NOTE** The Utilization Metrics feature allows the HSM SO to know which operations are being performed on the HSM. This information is normally available only to the Auditor when audit logging is turned on. However, while the SO can see a record of cryptographic operations, there is no visibility as to which keys are being used.

Setting the policy on (value 1) enables utilization metrics for all partitions including the Admin partition. Changing the policy is not destructive in either direction (off-to-on or on-to-off).

The **hsm showUtilization** command allows you to view the current utilization counter values for all partitions, and overall counts for the entire HSM, without resetting the counters.

The **hsm resetUtilization** command allows you to reset to zero the current utilization counter values for all partitions.

### To access the Partition Utilization Metrics feature

1. Log in as HSM SO (see "Logging In as HSM Security Officer" on page 128).  
lunacm:> **role login -name so**
2. Enable HSM policy **49: Allow Partition Utilization Metrics**.  
lunacm:> **hsm changehsmpolicy -policy 49 -value 1**

### To view or save Partition Utilization Metrics without resetting

lunacm:> **hsm showUtilization -serial** <partition\_SN>

### To reset the Partition Utilization Metrics counters to zero

Metrics are reset whenever power is lost to the HSM or the HSM is reset, or the HSM is initialized. These events do not save the metrics.

To display the metrics since the last reset (making them available to be captured manually or by script) and then immediately reset the metrics:

lunacm:> **hsm resetUtilization**

## Cryptographic Module and Token Return Codes

The following table summarizes HSM error codes:

HSM Error	Hex Code	PKCS#11 or SFNT Defined CKR Error
LUNA_RET_OK	0x00000000	CKR_OK

HSM Error	Hex Code	PKCS#11 or SFNT Defined CKR Error
LUNA_RET_CANCEL	0x00010000	CKR_CANCEL
LUNA_RET_FLAGS_INVALID	0x00040000	CKR_FLAGS_INVALID, removed from v2.0
LUNA_RET_TOKEN_NOT_PRESENT	0x00E00000	CKR_TOKEN_NOT_PRESENT
LUNA_RET_FORMER_INVALID_ENTRY_TYPE	0x00300130	CKR_DEVICE_ERROR
LUNA_RET_SP_TX_ERROR	0x00300131	CKR_DEVICE_ERROR
LUNA_RET_SP_RX_ERROR	0x00300132	CKR_DEVICE_ERROR
LUNA_RET_PED_ID_INVALID	0x00300140	CKR_DEVICE_ERROR
LUNA_RET_PED_UNSUPPORTED_PROTOCOL	0x00300141	CKR_DEVICE_ERROR
LUNA_RET_PED_UNPLUGGED	0x00300142	CKR_PED_UNPLUGGED
LUNA_RET_PED_ERROR	0x00300144	CKR_DEVICE_ERROR
LUNA_RET_PED_UNSUPPORTED_CRYPTO_PROTOCOL	0x00300145	CKR_DEVICE_ERROR
LUNA_RET_PED_DEK_INVALID	0x00300146	CKR_DEVICE_ERROR
LUNA_RET_PED_CLIENT_NOT_RUNNING	0x00300147	CKR_PED_CLIENT_NOT_RUNNING
LUNA_RET_CL_ALIGNMENT_ERROR	0x00300200	CKR_DEVICE_ERROR
LUNA_RET_CL_QUEUE_LOCATION_ERROR	0x00300201	CKR_DEVICE_ERROR
LUNA_RET_CL_QUEUE_OVERLAP_ERROR	0x00300202	CKR_DEVICE_ERROR
LUNA_RET_CL_TRANSMISSION_ERROR	0x00300203	CKR_DEVICE_ERROR
LUNA_RET_CL_NO_TRANSMISSION	0x00300204	CKR_DEVICE_ERROR
LUNA_RET_CL_COMMAND_MALFORMED	0x00300205	CKR_DEVICE_ERROR
LUNA_RET_CL_MAILBOXES_NOT_AVAILABLE	0x00300206	CKR_DEVICE_ERROR
LUNA_RET_MM_NOT_ENOUGH_MEMORY	0x00310000	CKR_DEVICE_MEMORY †

HSM Error	Hex Code	PKCS#11 or SFNT Defined CKR Error
LUNA_RET_MM_INVALID_HANDLE	0x00310001	CKR_DEVICE_MEMORY †
LUNA_RET_MM_USAGE_ALREADY_SET	0x00310002	CKR_DEVICE_MEMORY †
LUNA_RET_MM_ACCESS_OUTSIDE_ALLOCATION_RANGE	0x00310003	CKR_DEVICE_MEMORY †
LUNA_RET_MM_INVALID_USAGE	0x00310004	CKR_DEVICE_MEMORY †
LUNA_RET_MM_ITERATOR_PAST_END	0x00310005	CKR_DEVICE_MEMORY †
LUNA_RET_MM_FATAL_ERROR	0x00310006	CKR_DEVICE_MEMORY †
LUNA_RET_MEMORY_ALLOCATION_FAILED	0x00310007	CKR_DEVICE_MEMORY †
LUNA_RET_TEMPLATE_INCOMPLETE	0x00D00000	CKR_TEMPLATE_INCOMPLETE
LUNA_RET_TEMPLATE_INCONSISTENT	0x00D10000	CKR_TEMPLATE_INCONSISTENT*
LUNA_RET_ATTRIBUTE_TYPE_INVALID	0x00120000	CKR_ATTRIBUTE_TYPE_INVALID
LUNA_RET_ATTRIBUTE_VALUE_INVALID	0x00130000	CKR_ATTRIBUTE_VALUE_INVALID
LUNA_RET_ATTRIBUTE_READ_ONLY	0x00100000	CKR_ATTRIBUTE_READ_ONLY
LUNA_RET_ATTRIBUTE_SENSITIVE	0x00110000	CKR_ATTRIBUTE_SENSITIVE
LUNA_RET_OBJECT_HANDLE_INVALID	0x00820000	CKR_OBJECT_HANDLE_INVALID
LUNA_RET_MAX_OBJECT_COUNT	0x00820001	CKR_MAX_OBJECT_COUNT_EXCEEDED
LUNA_RET_ATTRIBUTE_NOT_FOUND	0x00120010	CKR_ATTRIBUTE_TYPE_INVALID
LUNA_RET_CAN_NOT_CREATE_SECRET_KEY	0x00D10011	CKR_TEMPLATE_INCONSISTENT
LUNA_RET_CAN_NOT_CREATE_PRIVATE_KEY	0x00D10012	CKR_TEMPLATE_INCONSISTENT
LUNA_RET_SECRET_KEY_MUST_BE_SENSITIVE	0x00130013	CKR_ATTRIBUTE_VALUE_INVALID
LUNA_RET_SECRET_KEY_MUST_HAVE_SENSITIVE_ATTRIBUTE	0x00D00014	CKR_TEMPLATE_INCOMPLETE

HSM Error	Hex Code	PKCS#11 or SFNT Defined CKR Error
LUNA_RET_PRIVATE_KEY_MUST_BE_SENSITIVE	0x00130015	CKR_ATTRIBUTE_VALUE_INVALID
LUNA_RET_PRIVATE_KEY_MUST_HAVE_SENSITIVE_ATTRIBUTE	0x00D00016	CKR_TEMPLATE_INCOMPLETE
LUNA_RET_SIGNING_KEY_MUST_BE_LOCAL	0x00680001	CKR_KEY_FUNCTION_NOT_PERMITTED
LUNA_RET_MULTI_FUNCTION_KEYS_NOT_ALLOWED	0x00D10018	CKR_TEMPLATE_INCONSISTENT
LUNA_RET_CAN_NOT_CHANGE_KEY_FUNCTION	0x00100019	CKR_ATTRIBUTE_READ_ONLY
LUNA_RET_KEY_SIZE_RANGE	0x00620000	CKR_KEY_SIZE_RANGE
LUNA_RET_KEY_TYPE_INCONSISTENT	0x00630000	CKR_KEY_TYPE_INCONSISTENT
LUNA_RET_KEY_INVALID_FOR_OPERATION	0x00630001	CKR_KEY_TYPE_INCONSISTENT
LUNA_RET_KEY_PARITY	0x00630002	CKR_KEY_TYPE_INCONSISTENT
LUNA_RET_KEY_UNEXTRACTABLE	0x006a0000	CKR_KEY_UNEXTRACTABLE
LUNA_RET_KEY_EXTRACTABLE	0x006a0001	KR_KEY_UNEXTRACTABLE
LUNA_RET_KEY_INDIGESTIBLE	0x00670000	CKR_KEY_INDIGESTIBLE
LUNA_RET_KEY_NOT_WRAPPABLE	0x00690000	CKR_KEY_NOT_WRAPPABLE
LUNA_RET_KEY_NOT_UNWRAPPABLE	0x00690001	CKR_KEY_NOT_WRAPPABLE
LUNA_RET_ARGUMENTS_BAD	0x00070000	CKR_ARGUMENTS_BAD
LUNA_RET_INVALID_ENTRY_TYPE	0x00070001	CKR_INVALID_ENTRY_TYPE
LUNA_RET_DATA_INVALID	0x00200000	CKR_DATA_INVALID
LUNA_RET_SM_DATA_INVALID	0x00200002	CKR_DATA_INVALID
LUNA_RET_NO_RNG_SEED	0x00200015	CKR_DATA_INVALID
LUNA_RET_FUNCTION_NOT_SUPPORTED	0x00540000	CKR_FUNCTION_NOT_SUPPORTED
LUNA_RET_NO_OFFBOARD_STORAGE	0x00540001	CKR_FUNCTION_NOT_SUPPORTED

HSM Error	Hex Code	PKCS#11 or SFNT Defined CKR Error
LUNA_RET_CL_COMMAND_NON_BACKUP	0x00540002	CKR_FUNCTION_NOT_SUPPORTED
LUNA_RET_BUFFER_TOO_SMALL	0x01500000	CKR_BUFFER_TOO_SMALL
LUNA_RET_DATA_LEN_RANGE	0x00210000	CKR_DATA_LEN_RANGE
LUNA_RET_GENERAL_ERROR	0x00050000	CKR_GENERAL_ERROR
LUNA_RET_DEVICE_ERROR	0x00300000	CKR_DEVICE_ERROR
LUNA_RET_UNKNOWN_COMMAND	0x00300001	CKR_FUNCTION_NOT_SUPPORTED
LUNA_RET_TOKEN_LOCKED_OUT	0x00300002	CKR_PIN_LOCKED
LUNA_RET_RNG_ERROR	0x00300003	CKR_DEVICE_ERROR
LUNA_RET_DES_SELF_TEST_FAILURE	0x00300004	CKR_DEVICE_ERROR
LUNA_RET_CAST_SELF_TEST_FAILURE	0x00300005	CKR_DEVICE_ERROR
LUNA_RET_CAST3_SELF_TEST_FAILURE	0x00300006	CKR_DEVICE_ERROR
LUNA_RET_CAST5_SELF_TEST_FAILURE	0x00300007	CKR_DEVICE_ERROR
LUNA_RET_MD2_SELF_TEST_FAILURE	0x00300008	CKR_DEVICE_ERROR
LUNA_RET_MD5_SELF_TEST_FAILURE	0x00300009	CKR_DEVICE_ERROR
LUNA_RET_SHA_SELF_TEST_FAILURE	0x0030000a	CKR_DEVICE_ERROR
LUNA_RET_RSA_SELF_TEST_FAILURE	0x0030000b	CKR_DEVICE_ERROR
LUNA_RET_RC2_SELF_TEST_FAILURE	0x0030000c	CKR_DEVICE_ERROR
LUNA_RET_RC4_SELF_TEST_FAILURE	0x0030000d	CKR_DEVICE_ERROR
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

HSM Error	Hex Code	PKCS#11 or SFNT Defined CKR Error
LUNA_RET_SM_UNKNOWN_COMMAND	0x00300011	CKR_DEVICE_ERROR
LUNA_RET_UM_TSN_MISSING	0x00300012	CKR_DEVICE_ERROR
LUNA_RET_SM_TSV_MISSING	0x00300013	CKR_DEVICE_ERROR
LUNA_RET_SM_UNKNOWN_TOSM_STATE	0x00300014	CKR_DEVICE_ERROR
LUNA_RET_DSA_PARAM_GEN_FAILURE	0x00300015	CKR_DEVICE_ERROR
LUNA_RET_DSA_SELF_TEST_FAILURE	0x00300016	CKR_DEVICE_ERROR
LUNA_RET_SEED_SELF_TEST_FAILURE	0x00300017	CKR_DEVICE_ERROR
LUNA_RET_AES_SELF_TEST_FAILURE	0x00300018	CKR_DEVICE_ERROR
LUNA_RET_FUNCTION_NOT_SUPPORTED_BY_HARDWARE	0x00300019	CKR_DEVICE_ERROR
LUNA_RET_HAS160_SELF_TEST_FAILURE	0x0030001a	CKR_DEVICE_ERROR
LUNA_RET_KCDSA_PARAM_GEN_FAILURE	0x0030001b	CKR_DEVICE_ERROR
LUNA_RET_KCDSA_SELF_TEST_FAILURE	0x0030001c	CKR_DEVICE_ERROR
LUNA_RET_HSM_INTERNAL_BUFFER_TOO_SMALL	0x0030001d	CKR_DEVICE_ERROR
LUNA_RET_COUNTER_WRAPAROUND	0x0030001e	CKR_DEVICE_ERROR
LUNA_RET_TIMEOUT	0x0030001f	CKR_TIMEOUT
LUNA_RET_NOT_READY	0x00300020	CKR_DEVICE_ERROR
LUNA_RET_RETRY	0x00300021	CKR_DEVICE_ERROR
LUNA_RET_SHA1_RSA_SELF_TEST_FAILURE	0x00300022	CKR_DEVICE_ERROR
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

HSM Error	Hex Code	PKCS#11 or SFNT Defined CKR Error
LUNA_RET_TOKEN_LOCKED_OUT_CL	0x00300100	CKR_DEVICE_ERROR
LUNA_RET_TOKEN_LOCKED_OUT_MM	0x00300101	CKR_DEVICE_ERROR
LUNA_RET_TOKEN_LOCKED_OUT_UM	0x00300102	CKR_DEVICE_ERROR
LUNA_RET_TOKEN_LOCKED_OUT_SM	0x00300103	CKR_DEVICE_ERROR
LUNA_RET_TOKEN_LOCKED_OUT_RN	0x00300104	CKR_DEVICE_ERROR
LUNA_RET_TOKEN_LOCKED_OUT_CA	0x00300105	CKR_DEVICE_ERROR
LUNA_RET_TOKEN_LOCKED_OUT_PM	0x00300106	CKR_DEVICE_ERROR
LUNA_RET_TOKEN_LOCKED_OUT_OH	0x00300107	CKR_DEVICE_ERROR
LUNA_RET_TOKEN_LOCKED_OUT_CCM	0x00300108	CKR_DEVICE_ERROR
LUNA_RET_TOKEN_LOCKED_OUT_SHA_DIGEST	0x00300109	CKR_DEVICE_ERROR
LUNA_RET_SM_ACCESS_REALLOC_ERROR	0x00310101	CKR_DEVICE_ERROR
LUNA_RET_SM_SESSION_REALLOC_ERROR	0x00310102	CKR_DEVICE_ERROR
LUNA_RET_SM_MEMORY_ALLOCATION_ERROR	0x00310103	CKR_DEVICE_ERROR
LUNA_RET_ENCRYPTED_DATA_INVALID	0x00400000	CKR_ENCRYPTED_DATA_INVALID
LUNA_RET_ENCRYPTED_DATA_LEN_RANGE	0x00410000	CKR_ENCRYPTED_DATA_LEN_RANGE
LUNA_RET_FUNCTION_CANCELED	0x00500000	CKR_FUNCTION_CANCELED
LUNA_RET_KEY_HANDLE_INVALID	0x00600000	CKR_KEY_HANDLE_INVALID
LUNA_RET_MECHANISM_INVALID	0x00700000	CKR_MECHANISM_INVALID
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

HSM Error	Hex Code	PKCS#11 or SFNT Defined CKR Error
LUNA_RET_UM_PIN_INCORRECT_CONTAINER_ZEROIZED	0x00a00001	CKR_PIN_INCORRECT
LUNA_RET_UM_PIN_INCORRECT_CONTAINER_LOCKED	0x00a00002	CKR_PIN_INCORRECT
LUNA_RET_UM_PIN_LEN_RANGE	0x00a20000	CKR_PIN_LEN_RANGE
LUNA_RET_SM_PIN_EXPIRED	0x00a30000	CKR_PIN_EXPIRED
LUNA_RET_SM_EXCLUSIVE_SESSION_EXISTS	0x00b20000	CKR_SESSION_EXCLUSIVE_EXISTS
LUNA_RET_SM_SESSION_HANDLE_INVALID	0x00b30000	CKR_SESSION_HANDLE_INVALID
LUNA_RET_SIGNATURE_INVALID	0x00c00000	CKR_SIGNATURE_INVALID
LUNA_RET_SIGNATURE_LEN_RANGE	0x00c10000	CKR_SIGNATURE_LEN_RANGE
LUNA_RET_UNWRAPPING_KEY_HANDLE_INVALID	0x00f00000	CKR_UNWRAPPING_KEY_HANDLE_INVALID
LUNA_RET_UNWRAPPING_KEY_SIZE_RANGE	0x00f10000	CKR_UNWRAPPING_KEY_SIZE_RANGE
LUNA_RET_UNWRAPPING_KEY_TYPE_INCONSISTENT	0x00f20000	CKR_UNWRAPPING_KEY_TYPE_INCONSISTENT
LUNA_RET_USER_ALREADY_LOGGED_IN	0x01000000	CKR_USER_ALREADY_LOGGED_IN
LUNA_RET_SM_OTHER_USER_LOGGED_IN	0x01000001	CKR_USER_ALREADY_LOGGED_IN
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

HSM Error	Hex Code	PKCS#11 or SFNT Defined CKR Error
LUNA_RET_WRAPPING_KEY_HANDLE_INVALID	0x01130000	CKR_WRAPPING_KEY_HANDLE_INVALID
LUNA_RET_WRAPPING_KEY_SIZE_RANGE	0x01140000	CKR_WRAPPING_KEY_SIZE_RANGE
LUNA_RET_WRAPPING_KEY_TYPE_INCONSISTENT	0x01150000	CKR_WRAPPING_KEY_TYPE_INCONSISTENT
LUNA_RET_CERT_VERSION_NOT_SUPPORTED	0x00300300	CKR_DEVICE_ERROR
LUNA_RET_SIM_AUTHFORM_INVALID	0x0020011e	CKR_SIM_AUTHFORM_INVALID
LUNA_RET_CCM_TOO_LARGE	0x00210001	CKR_DATA_LEN_RANGE
LUNA_RET_TEST_VS_BSAFE_FAILED	0x00300820	CKR_DEVICE_ERROR
LUNA_RET_SFNT3120_ERROR	0x00300821	CKR_DEVICE_ERROR
LUNA_RET_SFNT3120_SELFTEST_FAILED	0x00300822	CKR_DEVICE_ERROR
LUNA_RET_SFNT3120_CRC	0x00300823	CKR_DEVICE_ERROR
LUNA_RET_SFNT3120_ALG_NO_SOFTWARE_SUPPORT	0x00300824	CKR_DEVICE_ERROR
LUNA_RET_ISES_ERROR	0x00300880	CKR_DEVICE_ERROR
LUNA_RET_ISES_INIT_FAILED	0x00300881	CKR_DEVICE_ERROR
LUNA_RET_ISES_LNAU_TEST_FAILED	0x00300882	CKR_DEVICE_ERROR
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

HSM Error	Hex Code	PKCS#11 or SFNT Defined CKR Error
LUNA_RET_RM_NO_MEMORY	0x00310a02	CKR_DEVICE_MEMORY
LUNA_RET_RM_BAD_HSM_PARAMS	0x00300a03	CKR_DEVICE_ERROR
LUNA_RET_RM_POLICY_ELEMENT_DESTRUCTIVE	0x00200a04	CKR_DATA_INVALID
LUNA_RET_RM_POLICY_ELEMENT_NOT_DESTRUCTIVE	0x00200a05	CKR_DATA_INVALID
LUNA_RET_RM_CONFIG_CHANGE_ILLEGAL	0x00010a06	CKR_CANCEL
LUNA_RET_RM_CONFIG_CHANGE_FAILS_DEPENDENCIES	0x00010a07	CKR_CANCEL
LUNA_RET_LICENSE_ID_UNKNOWN	0x00200a08	CKR_DATA_INVALID
LUNA_RET_LICENSE_CAPACITY_EXCEEDED	0x00010a09	CKR_LICENSE_CAPACITY_EXCEEDED
LUNA_RET_RM_POLICY_WRITE_RESTRICTED	0x00010a0a	CKR_CANCEL
LUNA_RET_OPERATION_RESTRICTED	0x00010a0b	CKR_OPERATION_NOT_ALLOWED
LUNA_RET_CANNOT_PERFORM_OPERATION_TWICE	0x00010a0c	CKR_CANCEL
LUNA_RET_BAD_PPID	0x00200a0d	CKR_DATA_INVALID
LUNA_RET_BAD_FW_VERSION	0x00200a0e	CKR_DATA_INVALID
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

HSM Error	Hex Code	PKCS#11 or SFNT Defined CKR Error
LUNA_RET_OH_OBJECT_TYPE_INVALID	0x00300c01	CKR_DEVICE_ERROR
LUNA_RET_OH_OBJECT_ALREADY_EXISTS	0x00010c02	CKR_CANCEL
LUNA_RET_OH_OBJECT_OWNER_DOES_NOT_EXIST	0x00200c03	CKR_DATA_INVALID
LUNA_RET_STORAGE_TYPE_INCONSISTENT	0x00200c04	CKR_DATA_INVALID
LUNA_RET_CONTAINER_CAN_NOT_HAVE_MEMBERS	0x00200c05	CKR_DATA_INVALID
LUNA_RET_SAVED_STATE_INVALID	0x01600000	CKR_SAVED_STATE_INVALID
LUNA_RET_STATE_UNSAVEABLE	0x01800000	CKR_STATE_UNSAVEABLE
LUNA_RET_ERROR	0x80000000	CKR_GENERAL_ERROR
LUNA_RET_CONTAINER_HANDLE_INVALID	0x80000001	CKR_CONTAINER_HANDLE_INVALID
LUNA_RET_INVALID_PADDING_TYPE	0x80000002	CKR_DATA_INVALID
LUNA_RET_NOT_FOUND	0x80000007	CKR_FUNCTION_FAILED
LUNA_RET_TOO_MANY_CONTAINERS	0x80000008	CKR_TOO_MANY_CONTAINERS
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

HSM Error	Hex Code	PKCS#11 or SFNT Defined CKR Error
LUNA_RET_KCV_PARAMETER_COULD_NOT_BE_ADDED	0x80000101	CKR_DEVICE_MEMORY
LUNA_RET_INVALID_CERTIFICATE_DATA	0x80000102	CKR_CERTIFICATE_DATA_INVALID
LUNA_RET_INVALID_CERTIFICATE_TYPE	0x80000103	CKR_CERTIFICATE_DATA_INVALID
LUNA_RET_INVALID_CERTIFICATE_VERSION	0x80000104	CKR_CERTIFICATE_DATA_INVALID
LUNA_RET_INVALID_MODULUS_SIZE	0x80000105	CKR_ATTRIBUTE_VALUE_INVALID
LUNA_RET_WRAPPING_ERROR	0x80000107	CKR_WRAPPING_ERROR
LUNA_RET_UNWRAPPING_ERROR	0x80000108	CKR_UNWRAPPING_ERROR
LUNA_RET_INVALID_PRIVATE_KEY_TYPE	0x80000109	CKR_DATA_INVALID
LUNA_RET_TSN_MISMATCH	0x8000010a	CKR_DATA_INVALID
LUNA_RET_KCV_PARAMETER_MISSING	0x8000010b	CKR_CLONING_PARAMETER_MISSING
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

HSM Error	Hex Code	PKCS#11 or SFNT Defined CKR Error
LUNA_RET_DAK_MISSING	0x80000117	CKR_DAK_MISSING
LUNA_RET_BAD_DAK	0x80000118	CKR_BAD_DAK
LUNA_RET_HOK_MISSING	0x80000119	CKR_CERTIFICATE_DATA_MISSING
LUNA_RET_CITS_DAK_MISSING	0x8000011a	CKR_CITS_DAK_MISSING
LUNA_RET_SIM_AUTHORIZATION_FAILED	0x8000011b	CKR_SIM_AUTHORIZATION_FAILED
LUNA_RET_SIM_VERSION_UNSUPPORTED	0x8000011c	CKR_SIM_VERSION_UNSUPPORTED
LUNA_RET_SIM_CORRUPT_DATA	0x8000011d	CKR_SIM_CORRUPT_DATA
LUNA_RET_ECC_MIC_MISSING	0x8000011e	CKR_CERTIFICATE_DATA_MISSING
LUNA_RET_ECC_HOK_MISSING	0x8000011f	CKR_CERTIFICATE_DATA_MISSING
LUNA_RET_ECC_HOC_MISSING	0x80000120	CKR_CERTIFICATE_DATA_MISSING
LUNA_RET_ECC_DAK_MISSING	0x80000121	CKR_CERTIFICATE_DATA_MISSING
LUNA_RET_ECC_DAC_MISSING	0x80000122	CKR_CERTIFICATE_DATA_MISSING
LUNA_RET_ROOT_CERT_MISSING	0x80000123	CKR_CERTIFICATE_DATA_MISSING
LUNA_RET_HOC_MISSING	0x80000124	CKR_CERTIFICATE_DATA_MISSING
LUNA_RET_INVALID_CERTIFICATE_FUNCTION	0x80000125	CKR_CERTIFICATE_DATA_INVALID
LUNA_RET_N_TOO_LARGE	0x80000200	CKR_ARGUMENTS_BAD
LUNA_RET_N_TOO_SMALL	0x80000201	CKR_ARGUMENTS_BAD
LUNA_RET_M_TOO_LARGE	0x80000202	CKR_ARGUMENTS_BAD
LUNA_RET_M_TOO_SMALL	0x80000203	CKR_ARGUMENTS_BAD
LUNA_RET_WEIGHT_TOO_LARGE	0x80000204	CKR_ARGUMENTS_BAD
LUNA_RET_WEIGHT_TOO_SMALL	0x80000205	CKR_ARGUMENTS_BAD
LUNA_RET_TOTAL_WEIGHT_INVALID	0x80000206	CKR_ARGUMENTS_BAD

HSM Error	Hex Code	PKCS#11 or SFNT Defined CKR Error
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
LUNA_RET_VECTOR_OF_DIFFERENT_SET	0x8000021a	CKR_ARGUMENTS_BAD
LUNA_RET_VECTOR_DUPLICATE	0x8000021b	CKR_ARGUMENTS_BAD
LUNA_RET_VECTOR_TYPE_INVALID	0x8000021c	CKR_ARGUMENTS_BAD
LUNA_RET_MISSING_COMMAND_PARAMETER	0x8000021d	CKR_ARGUMENTS_BAD
LUNA_RET_M_OF_N_CLONING_IS_NOT_ALLOWED	0x8000021e	CKR_FUNCTION_NOT_SUPPORTED

HSM Error	Hex Code	PKCS#11 or SFNT Defined CKR Error
LUNA_RET_M_OF_N_IS_NOT_REQUIRED	0x8000021f	CKR_OPERATION_NOT_INITIALIZED
LUNA_RET_M_OF_N_IS_NOT_INITIALIZED	0x80000220	CKR_OPERATION_NOT_INITIALIZED
LUNA_RET_M_OF_N_SECRET_INVALID	0x80000221	CKR_GENERAL_ERROR
LUNA_RET_CCM_NOT_PRESENT	0x80000300	CKR_FUNCTION_NOT_SUPPORTED
LUNA_RET_CCM_NOT_SUPPORTED	0x80000301	CKR_FUNCTION_NOT_SUPPORTED
LUNA_RET_CCM_UNREMOVABLE	0x80000302	CKR_DATA_INVALID
LUNA_RET_CCM_CERT_INVALID	0x80000303	CKR_DATA_INVALID
LUNA_RET_CCM_SIGN_INVALID	0x80000304	CKR_DATA_INVALID
LUNA_RET_CCM_UPDATE_DENIED	0x80000305	CKR_DATA_INVALID
LUNA_RET_CCM_FWUPDATE_DENIED	0x80000306	CKR_DATA_INVALID
LUNA_RET_SM_ACCESS_ID_INVALID	0x80000400	CKR_DATA_INVALID
LUNA_RET_SM_ACCESS_ALREADY_EXISTS	0x80000401	CKR_DATA_INVALID
LUNA_RET_SM_MULTIPLE_ACCESS_DISABLED	0x80000402	CKR_FUNCTION_NOT_SUPPORTED
LUNA_RET_SM_UNKNOWN_ACCESS_TYPE	0x80000403	CKR_ARGUMENTS_BAD
LUNA_RET_SM_BAD_ACCESS_HANDLE	0x80000404	CKR_DATA_INVALID
LUNA_RET_SM_BAD_CONTEXT_NUMBER	0x80000405	CKR_DATA_INVALID
LUNA_RET_SM_UNKNOWN_SESSION_TYPE	0x80000406	CKR_DATA_INVALID
LUNA_RET_SM_CONTEXT_ALREADY_ALLOCATED	0x80000407	CKR_DATA_INVALID
LUNA_RET_SM_CONTEXT_NOT_ALLOCATED	0x80000408	CKR_DEVICE_MEMORY
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

HSM Error	Hex Code	PKCS#11 or SFNT Defined CKR Error
LUNA_RET_MTK_ZEROIZED	0x80000531	CKR_MTK_ZEROIZED
LUNA_RET_MTK_STATE_INVALID	0x80000532	CKR_MTK_STATE_INVALID
LUNA_RET_MTK_SPLIT_INVALID	0x80000533	CKR_MTK_SPLIT_INVALID
LUNA_RET_INVALID_IP_PACKET	0x80000600	CKR_DEVICE_ERROR
LUNA_RET_INVALID_BOARD_TYPE	0x80000700	CKR_DEVICE_ERROR
LUNA_RET_ECC_NOT_SUPPORTED	0x80000601	CKR_FUNCTION_NOT_SUPPORTED
LUNA_RET_ECC_BUFFER_OVERFLOW	0x80000602	CKR_DEVICE_ERROR
LUNA_RET_ECC_POINT_INVALID	0x80000603	CKR_ECC_POINT_INVALID**
LUNA_RET_ECC_SELF_TEST_FAILURE	0x80000604	CKR_DEVICE_ERROR
LUNA_RET_ECC_UNKNOWN_CURVE	0x80000605	CKR_ECC_UNKNOWN_CURVE
LUNA_RET_HA_NOT_SUPPORTED	0x80000900	CKR_FUNCTION_NOT_SUPPORTED
LUNA_RET_HA_USER_NOT_INITIALIZED	0x80000901	CKR_OPERATION_NOT_INITIALIZED
LUNA_RET_HSM_STORAGE_FULL	0x80000902	CKR_HSM_STORAGE_FULL
LUNA_RET_CONTAINER_OBJECT_STORAGE_FULL	0x80000903	CKR_CONTAINER_OBJECT_STORAGE_FULL
LUNA_RET_KEY_NOT_ACTIVE	0x80000904	CKR_KEY_NOT_ACTIVE
LUNA_RET_CB_NOT_SUPPORTED	0x80000a01	CKR_FUNCTION_NOT_SUPPORTED
LUNA_RET_CB_PARAM_INVALID	0x80000a02	CKR_CALLBACK_ERROR
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

HSM Error	Hex Code	PKCS#11 or SFNT Defined CKR Error
LUNA_RET_CB_SYS_ERROR	0x80000a07	CKR_CALLBACK_ERROR
LUNA_RET_CB_HIOS_HANDLE_INVALID	0x80000a10	CKR_CALLBACK_ERROR
LUNA_RET_CB_HIOS_ID_INVALID	0x80000a11	CKR_CALLBACK_ERROR
LUNA_RET_CB_HIOS_CLOSED	0x80000a12	CKR_CALLBACK_ERROR
LUNA_RET_CB_HIOS_CANCELED	0x80000a13	CKR_CALLBACK_ERROR
LUNA_RET_CB_HIOS_IO_ERROR	0x80000a14	CKR_CALLBACK_ERROR
LUNA_RET_CB_HIOS_SEND_TIMEOUT	0x80000a15	CKR_CALLBACK_ERROR
LUNA_RET_CB_HIOS_RECV_TIMEOUT	0x80000a16	CKR_CALLBACK_ERROR
LUNA_RET_CB_HIOS_STATE_INVALID	0x80000a17	CKR_CALLBACK_ERROR
LUNA_RET_CB_HIOS_OUTPUT_BUFFER_TOO_SMALL	0x80000a18	CKR_CALLBACK_ERROR
LUNA_RET_CB_HIOS_INPUT_BUFFER_TOO_SMALL	0x80000a19	CKR_CALLBACK_ERROR
LUNA_RET_CB_HANDLE_INVALID	0x80000a20	CKR_CALLBACK_ERROR
LUNA_RET_CB_ID_INVALID	0x80000a21	CKR_CALLBACK_ERROR
LUNA_RET_CB_REMOTE_ABORT	0x80000a22	CKR_CALLBACK_ERROR
LUNA_RET_CB_REMOTE_CLOSED	0x80000a23	CKR_CALLBACK_ERROR
LUNA_RET_CB_REMOTE_ABANDONED	0x80000a24	CKR_CALLBACK_ERROR
LUNA_RET_CB_MUST_READ	0x80000a25	CKR_CALLBACK_ERROR
LUNA_RET_CB_MUST_WRITE	0x80000a26	CKR_CALLBACK_ERROR
LUNA_RET_CB_INVALID_CALL_FOR_THE_STATE	0x80000a27	CKR_CALLBACK_ERROR
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

HSM Error	Hex Code	PKCS#11 or SFNT Defined CKR Error
LUNA_RET_LOG_FILE_WRITE_ERROR	0x80000d01	CKR_LOG_FILE_WRITE_ERROR
LUNA_RET_LOG_BAD_FILE_NAME	0x80000d02	CKR_LOG_BAD_FILE_NAME
LUNA_RET_LOG_FULL	0x80000d03	CKR_LOG_FULL
LUNA_RET_LOG_NO_KCV	0x80000d04	CKR_LOG_NO_KCV
LUNA_RET_LOG_BAD_RECORD_HMAC	0x80000d05	CKR_LOG_BAD_RECORD_HMAC
LUNA_RET_LOG_BAD_TIME	0x80000d06	CKR_LOG_BAD_TIME
LUNA_RET_LOG_AUDIT_NOT_INITIALIZED	0x80000d07	CKR_LOG_AUDIT_NOT_INITIALIZED
LUNA_RET_LOG_RESYNC_NEEDED	0x80000d08	CKR_LOG_RESYNC_NEEDED
LUNA_RET_AUDIT_LOGIN_TIMEOUT_IN_PROGRESS	0x80000d09	CKR_AUDIT_LOGIN_TIMEOUT_IN_PROGRESS
LUNA_RET_AUDIT_LOGIN_FAILURE_THRESHOLD	0x80000d0a	CKR_AUDIT_LOGIN_FAILURE_THRESHOLD
LUNA_RET_XTC_ERROR	0x80001600	CKR_XTC_ERROR
LUNA_RET_CONTEXT_INVALID	0x80001601	CKR_CONTEXT_INVALID
LUNA_RET_SESSION_COUNT	0x80001603	CKR_MAX_SESSION_COUNT
LUNA_RET_BUSY	0x80001604	CKR_BUSY

\* This error (CKR\_TEMPLATE\_INCONSISTENT) might be encountered when using CKDemo in a new client with firmware older than version 6.22.0. Try CKDemo option 98, sub-option 16. If it is set to "enhanced roles", try selecting it to set it to "legacy Luna roles". The setting is a toggle, and flips every time you select it.

\*\* This error, or "unable to read public key", might be encountered when using BSAFE to encrypt data with ECC public key using curves from the Brainpool suite. As indicated on the BSAFE website (May 2012) they do not appear to support Brainpool curves. Therefore, your own applications should not attempt that combination, and you should avoid attempting to specify Brainpool curves with BSAFE ECC when using the Luna CKDemo utility.

† These errors (0x00310000 through 0x00310007) are all considered as the same generic CKR\_DEVICE\_MEMORY error *by a host application*. They are visible using Luna HSM Firmware 7.8.1 or newer. Your application is responsible for closing crypto sessions and releasing resources when they are no longer being used. Failure to do so allows accumulating orphan sessions to eventually consume all available HSM memory. The HSM has no way to know that any given session is no longer needed, unless your application explicitly closes the session. If a solution/application mixes Java and C/C++ operations, those might not agree on when sessions are to close.

**Workaround:** If you are seeing device memory errors in the logs, consider:

- 1. Stopping your application (so that it does not continue attempting cryptographic operations against the HSM)
- 2. Restarting the HSM to clear any orphan sessions or processes (use `hsm restart` to restart the HSM)
- 3. Restarting your application.

**NOTE** This is a temporary measure to clear the effects of application behavior that should be corrected, or the problem can recur. Contact your application vendor to report the memory issue.

## Library Codes

Hex value	Decimal value	Return code/error description
0	0	OKAY, NO ERROR
0xC0000000	3221225472	PROGRAMMING ERROR: RETURN CODE
0xC0000001	3221225473	OUT OF MEMORY
0xC0000002	3221225474	NON-SPECIFIC ERROR
0xC0000003	3221225475	UNEXPECTED NULL POINTER
0xC0000004	3221225476	PROGRAMMING ERROR: LOGIC
0xC0000005	3221225477	OPERATION WOULD BLOCK IF ATTEMPTED
0xC0000006	3221225478	BUFFER IS TOO SMALL
0xC0000100	3221225728	OPERATION CANCEL
0xC0000101	3221225729	INVALID SLOT IDENTIFIER
0xC0000102	3221225730	INVALID DATA
0xC0000103	3221225731	INVALID PIN
0xC0000104	3221225732	NO TOKEN PRESENT
0xC0000105	3221225733	FUNCTION IS NOT SUPPORTED
0xC0000106	3221225734	NON-CRYPTOKI ELEMENT CLONE
0xC0000107	3221225735	INVALID BUFFER SIZE FOR CHALLENGE

Hex value	Decimal value	Return code/error description
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
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

Hex value	Decimal value	Return code/error description
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
0xC0000700	3221227264	SSL ERROR
0xC0000701	3221227265	SSL CTX ERROR
0xC0000702	3221227266	SSL CIPHER LIST ERROR
0xC0000703	3221227267	SSL CERT VERIFICATION LOCATION ERROR

Hex value	Decimal value	Return code/error description
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
0xC0001001	3221229569	PARTITION NOT ACTIVATED
0xc0002000	3221233664	FAILED TO CREATE THREAD
0xc0002001	3221233665	CALLBACK ERROR
0xc0002002	3221233666	UNKNOWN CALLBACK COMMAND

Hex value	Decimal value	Return code/error description
0xc0002003	3221233667	SHUTTING DOWN
0xc0002004	3221233668	REMOTE SIDE DISCONNECTED
0xc0002005	3221233669	SOCKET CLOSED
0xC0002006	3221233670	INVALID COMMAND
0xC0002007	3221233671	UNKNOWN COMMAND
0xC0002008	3221233672	UNKNOWN COMMAND VERSION
0xC0002009	3221233673	FILE LOCK FAILED
0xC0002010	3221233680	FILE LOCK ERROR
0xc0002011	3221233681	FAILED TO CREATE PROCESS
0xc0002012	3221233682	USB PED NOT FOUND
0xc0002013	3221233683	USB PED NOT RESPONDING
0xc0002014	3221233684	USB PED OPERATION CANCELLED
0xc0002015	3221233685	USB PED TOO MANY CONNECTED
0xc0002016	3221233686	USB PED OUT OF SYNC
0xC0001100	3221229824	UNABLE TO CONNECT

## Vendor-Defined Return Codes

Code	Name
0x80000004	CKR_RC_ERROR
0x80000005	CKR_CONTAINER_HANDLE_INVALID
0x80000006	CKR_TOO_MANY_CONTAINERS

Code	Name
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
0x8000001c	CKR_SO_LOGIN_FAILURE_THRESHOLD

Code	Name
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

Code	Name
0x80000049	CKR_STC_CIPHER_SUITE_REJECTED
0x8000004a	CKR_STC_DH_KEY_NOT_FROM_SAME_GROUP
0x8000004b	CKR_STC_COMPUTE_DH_KEY_ERROR
0x8000004c	CKR_STC_FIRST_PHASE_KDF_ERROR
0x8000004d	CKR_STC_SECOND_PHASE_KDF_ERROR
0x8000004e	CKR_STC_KEY_CONFIRMATION_FAILED
0x8000004f	CKR_STC_NO_SESSION_KEY
0x80000050	CKR_STC_RESPONSE_BAD_MAC
0x80000051	CKR_STC_NOT_ENABLED
0x80000052	CKR_STC_CLIENT_HANDLE_INVALID
0x80000053	CKR_STC_SESSION_INVALID
0x80000054	CKR_STC_CONTAINER_INVALID
0x80000055	CKR_STC_SEQUENCE_NUM_INVALID
0x80000056	CKR_STC_NO_CHANNEL
0x80000057	CKR_STC_RESPONSE_DECRYPT_ERROR
0x80000058	CKR_STC_RESPONSE_REPLAYED
0x80000059	CKR_STC_REKEY_CHANNEL_MISMATCH
0x8000005a	CKR_STC_RSA_ENCRYPT_ERROR
0x8000005b	CKR_STC_RSA_SIGN_ERROR
0x8000005c	CKR_STC_RSA_DECRYPT_ERROR
0x8000005d	CKR_STC_RESPONSE_UNEXPECTED_KEY
0x8000005e	CKR_STC_UNEXPECTED_NONCE_PAYLOAD_SIZE

Code	Name
0x8000005f	CKR_STC_UNEXPECTED_DH_DATA_SIZE
0x80000060	CKR_STC_OPEN_CIPHER_MISMATCH
0x80000061	CKR_STC_OPEN_DHNIST_PUBKEY_ERROR
0x80000062	CKR_STC_OPEN_KEY_MATERIAL_GEN_FAIL
0x80000063	CKR_STC_OPEN_RESP_GEN_FAIL
0x80000064	CKR_STC_ACTIVATE_MACTAG_U_VERIFY_FAIL
0x80000065	CKR_STC_ACTIVATE_MACTAG_V_GEN_FAIL
0x80000066	CKR_STC_ACTIVATE_RESP_GEN_FAIL
0x80000067	CKR_CHALLENGE_INCORRECT
0x80000068	CKR_ACCESS_ID_INVALID
0x80000069	CKR_ACCESS_ID_ALREADY_EXISTS
0x8000006a	CKR_KEY_NOT_KEKABLE
0x8000006b	CKR_MECHANISM_INVALID_FOR_FP
0x8000006c	CKR_OPERATION_INVALID_FOR_FP
0x8000006d	CKR_SESSION_HANDLE_INVALID_FOR_FP
0x8000006e	CKR_CMD_NOT_ALLOWED_HSM_IN_TRANSPORT
0x8000006f	CKR_OBJECT_ALREADY_EXISTS
0x80000070	CKR_PARTITION_ROLE_DESC_VERSION_INVALID
0x80000071	CKR_PARTITION_ROLE_POLICY_VERSION_INVALID
0x80000072	CKR_PARTITION_ROLE_POLICY_SET_VERSION_INVALID
0x80000073	CKR_REKEK_KEY
0x80000074	CKR_KEK_RETRY_FAILURE

Code	Name
0x80000075	CKR_RNG_RESEED_TOO_EARLY
0x80000076	CKR_HSM_TAMPERED
0x80000077	CKR_CONFIG_CHANGE_ILLEGAL
0x80000078	CKR_SESSION_CONTEXT_NOT_ALLOCATED
0x80000079	CKR_SESSION_CONTEXT_ALREADY_ALLOCATED
0x8000007a	CKR_INVALID_BL_ITB_AUTH_HEADER
0x80000114	CKR_OBJECT_READ_ONLY
0x80000136	CKR_KEY_NOT_ACTIVE
0x80000400	CKR_ACCESS_ID_INVALID
0x80001600	CKR_XTC_ERROR
0x80001601	CKR_CONTEXT_INVALID
0x80001603	CKR_MAX_SESSION_COUNT
0x80001604	CKR_BUSY
0x80001606	CKR_SERVICE_UNAVAILABLE

# CHAPTER 12: HSM Updates

Thales releases periodic updates to the Luna USB HSM 7 firmware, as well as updated versions of the Luna HSM Client software. If you have recently purchased a new Luna USB HSM 7 and your organization requires FIPS certification, you can download and install a FIPS-validated version of the HSM firmware. You can download these updates as they become available from the Thales Customer Support Portal: <https://supportportal.thalesgroup.com>.

The [Customer Release Notes](#) (CRN) contain important information on updates.

The following chapter provides tested update paths and procedures for installing update packages, as well as a list of the version dependencies for certain features. It contains the following sections:

- > ["Updating the Luna USB HSM 7 Firmware" below](#)
- > ["Updating the Luna HSM Client Software" on page 77](#)
- > [Updating the Luna Backup HSM 7 Firmware](#)
- > [Updating the Luna Backup HSM G5 Firmware](#)
- > ["Rolling Back the Luna HSM Firmware" on the next page](#)

## Updating the Luna USB HSM 7 Firmware

To update the firmware on a Luna USB HSM 7, download the desired firmware version from the Thales Support Portal. Use LunaCM on the host workstation to apply the update. You require:

- > Luna USB HSM 7 firmware update file (<filename>.**fuf**)
- > the firmware update authentication code file (<filename>.**txt**)

### To update the Luna USB HSM 7 firmware

1. Copy the firmware file (<filename>.**fuf**) and the authentication code file (<filename>.**txt**) to the Luna HSM Client root directory.
  - Windows: C:\Program Files\SafeNet\LunaClient
  - Linux/AIX: /usr/safenet/lunaclient/bin
  - Solaris: /opt/safenet/lunaclient/bin

**NOTE** On some Windows configurations, you might not have authority to copy or unzip files directly into **C:\Program Files\...** If this is the case, put the files in a known location that you can reference in a LunaCM command.

2. Launch LunaCM.
3. If more than one HSM is installed, set the active slot to the Admin partition of the HSM you wish to update.

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

4. Log in as HSM SO.

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

5. Apply the new firmware update by specifying the update file and the authentication code file. If the files are not located in the Luna HSM Client root directory, specify the full filepaths.

```
lunacm:> hsm updatefw -fuf <filename>.fuf -authcode <filename>.txt
```

## Changing the Firmware Upgrade Permissions (Linux only)

By default, the root user and any user who is part of the **hsmusers** group can perform a firmware update. You can use this procedure to restrict firmware update operations to root only (that is, disable firmware update for members of the **hsmusers** group).

---

### To restrict firmware update operations to the root user only

1. Open the the `/etc/modprobe.d/k7.conf` file for editing:

```
sudoedit /etc/modprobe.d/k7.conf
```

2. Change the **k7\_rootonly\_reset** option from **0** to **1**. Save the file and exit the editor.

3. Stop any processes that are using the K7 driver. Typically this means stopping the **pedclient** service, and the **luna-snmp** service, if you are using SNMP.

```
sudo systemctl stop pedclient_service
```

```
sudo systemctl stop luna-snmp
```

4. Reload the driver:

```
sudo systemctl reload k7
```

---

## Rolling Back the Luna HSM Firmware

When updating the HSM firmware, the Luna USB HSM 7 saves the previously-installed firmware version on the HSM. If required, you can roll back to this previously-installed version. Rollback allows you to try firmware without permanently committing to the new version.

Rollback does not create a new rollback target; a single rollback target is preserved when a firmware update is performed. After a rollback operation, no further rollback is possible until the next firmware update saves the pre-update version as the new rollback target.

**CAUTION!** 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.

---

### To roll back the Luna HSM firmware to the previous version

1. Check the previous firmware version that is available on the HSM.

lunacm:> **hsm showinfo**

2. Back up any important cryptographic objects currently stored on the HSM (see [Partition Backup and Restore](#)).

3. At the LunaCM prompt, login as HSM SO.

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

4. Roll back the HSM firmware.

lunacm:> **hsm rollbackfw**

LunaCM performs an automatic restart following the rollback procedure.

5. Re-initialize the HSM and restore your partition from backup.

# CHAPTER 13: 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:

- > ["Comparing Zeroize and Factory Reset" below](#)
- > ["HSM Zeroization" on the next page](#)
- > ["Resetting the Luna USB HSM 7 to Factory Condition" on page 188](#)
- > ["Stored Data Integrity" on page 188](#)

## Comparing Zeroize and Factory Reset

You can clear the contents of your Luna HSM, or the HSM may be cleared in response to an event. How this affects the contents and configuration of your HSM depends on whether the user partitions were deleted or whether the HSM was zeroized or factory reset as detailed below:

Action	Command/Event	Description
Erase User Partitions	> Enable or disable a destructive HSM policy	Destroy/erase the user partition, but do not zeroize the HSM. To bring the HSM back into service, you need to: <ol style="list-style-type: none"><li>1. Recreate the partition</li><li>2. Reinitialize the partition roles</li></ol>
Zeroize	> Too many bad login attempts on the HSM SO account > <code>lunacm:&gt; <b>hsm zeroize</b></code>	Deletes all partitions and their contents, but retains the HSM configuration (audit role and configuration, policy settings). To bring the HSM back into service, you need to: <ol style="list-style-type: none"><li>1. Reinitialize the HSM</li><li>2. Recreate the partition</li><li>3. Reinitialize the partition roles</li></ol>

Action	Command/Event	Description
Factory Reset	lunacm:> <b>hsm factoryreset</b>	Deletes the application partition and its 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.

## 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
- > set a "destructive" HSM policy

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 USB HSM 7 to Factory Condition

These instructions will allow you to restore your Luna USB HSM 7 to its original factory configuration. The HSM is zeroized, all partitions erased, and HSM policies are returned to their default settings.

### To reset the HSM to factory condition

1. Set the active slot to the admin partition.

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

2. Reset the HSM to factory settings.

```
lunacm:> hsm factoryreset
```

## 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 `lunacm:>hsm restart` should recover the HSM without losing data in permanent storage.

If the HSM firmware halts because data in the permanent flash storage is corrupted, the HSM is recovered by using the newly enhanced **hsm factoryReset** command which deletes all the partitions, zeroizes all the objects, and resets the policies.

Since **hsm factoryReset** is destructive, it is important to keep a regular backup of HSM objects in case the HSM ever goes into a state that requires factory reset.

Running the **hsm factoryReset** command, while the HSM is in normal working state, has the same behavior as before Luna HSM Firmware 7.7.0.

Running the **hsm factoryReset** command, while the HSM is in a halt state (where the normal "factoryReset" fails), invokes the recovery process, which takes several minutes (6+ minutes) to complete. It is important to wait for the **hsm factoryReset** command to complete without interruption.

For an example of the output, see [hsm factoryreset](#).