

Thales Luna Network HSM 7.7.1

PARTITION ADMINISTRATION GUIDE



Document Information

Last Updated	2021-10-28 10:56:06 GMT-04:00
---------------------	-------------------------------

Trademarks, Copyrights, and Third-Party Software

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

Disclaimer

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

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

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

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

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

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

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

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

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

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

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

Regulatory Compliance

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

USA, FCC

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

Canada

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

Europe

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

CONTENTS

Document Information	2
Preface: About the Partition Administration Guide	13
Customer Release Notes	14
Audience	14
Document Conventions	14
Support Contacts	16
Chapter 1: Luna HSM Client Software Installation	17
Windows Luna HSM Client Installation	18
Required Client Software	18
Prerequisites	18
Installing the Luna HSM Client Software	19
Modifying the Installed Windows Luna HSM Client Software	22
Java	23
Luna CSP and KSP	23
USB-powered PED	24
Modifying the Number of Luna Backup HSM Slots	24
Uninstalling the Luna HSM Client Software	25
After Installation	27
Troubleshooting	27
Scripted/Unattended Windows Installation/Uninstallation	28
Command line options overview	28
Installing all components and features	30
Installing the Luna HSM Client for the Luna Network HSM	31
Installing the Luna HSM Client for the Luna PCIe HSM	31
Installing the Luna HSM Client for the Luna USB HSM	31
Installing the Luna HSM Client for the Luna Backup HSM	32
Installing the Luna HSM Client for Remote PED	32
Installation Location	32
Logging	33
Uninstalling the Luna HSM Client	33
Linux Luna HSM Client Installation	34
Where to install, and SELinux	35
Installing the Client Software	35
Installing the Minimal Client Software	39
Controlling User Access to Your Attached HSMs and Partitions	39
Uninstalling the Client Software or Removing Components	40
Java	40
Scripted or Unattended Installation	41
Interrupting the Installation	42

Modifying the Number of Luna Backup HSM Slots	42
Effects of Kernel Upgrades	43
Troubleshooting	43
Luna Minimal Client Install for Linux - Overview	43
Included in the Minimal Client	45
Installation Prerequisites	47
Preparing the Configuration File for Use with Luna Minimal Client and Docker	47
Installing Luna Minimal Client on Linux Using Docker	48
To install the Luna Minimal Client software on a Linux 64-bit Docker instance:	48
Functionality Modules (FMs) with Luna Minimal Client	52
Thales Data Protection on Demand Luna Cloud HSM Service with Luna Minimal Client	52
From Linux Minimal Client Create a Docker Container to Access a DPOD Luna Cloud HSM Service	52
Create a Luna HSM Client Docker image for use with Functionality Modules	53
Solaris Luna HSM Client Installation	57
Prerequisites	57
Installing the Client Software	58
Uninstalling the Luna HSM Client Software	60
Java	60
Scripted or Unattended Installation	60
Interrupting the installation - [Ctrl] [C]	61
AIX Luna HSM Client Installation	63
Prerequisites	63
Installing the Client Software	63
Uninstalling the Luna HSM Client Software	66
Installing Java	66
Scripted or Unattended Installation	66
Interrupting the Installation	67
Adding a Luna Cloud HSM Service	68
Configuration File Summary	70
Updating the Luna HSM Client Software	85
Chapter 2: Client-Partition Connections	86
Comparing NTLS and STC	86
Client to HSM Security Best Practices	91
Security around Password-authenticated systems	92
Creating an NTLS Connection Using Self-Signed Certificates	92
Multi-Step NTLS Connection Procedure	93
One-Step NTLS Connection Procedure	95
Creating an NTLS Connection Using a Self-Signed Appliance Certificate and a Client Certificate Signed by a Trusted Certificate Authority	96
Registering the Appliance Certificate on the Client	97
Authenticating a Client Using a Trusted CA	98
Registering the Client Certificate and CA Certificate Chain on the Appliance	99
Creating an NTLS Connection Using Certificates Signed by a Trusted Certificate Authority	99
Authenticating the Appliance Using a Trusted CA	100
Authenticating a Client Using a Trusted CA	101
Registering a Client to the Appliance	102

Using a Combination of Self-Signed and CA-Signed Certificates	103
Assigning or Revoking NTLS Client Access to a Partition	103
Creating an STC Connection	104
Preparing the HSM/Partition to Use STC	105
Connecting an Initialized STC Partition to Multiple Clients	109
Converting Initialized NTLS Partitions to STC	113
Using the STC Admin Channel	115
Configuring STC Identities and Settings	117
Restoring Broken NTLS or STC Connections	121
Restoring NTLS/STC Connections after Regenerating the Server and/or Client Certificates	121
Restoring Connections After HSM Zeroization	122
Restoring STC Connections After Partition Zeroization	122
Updating Luna Network HSM with STC Partitions to 7.7.0 or Newer	123
Cryptography is enhanced (requires firmware 7.7.0)	123
What are "pre-firmware 7.7.0", and V0, and V1 partitions?	126
What is the origin of each partition type	127
Partition Policy considerations	128
General HSM behavior	128
Cloning	129
SMK (SKS Master Key)	129
Behavior at partition level	130
Structure of partition	131
Objects in a partition	131
Memory	131
Behavior at key level	132
PPT (partition policy template)	132
Per-key Authorization	133
Multi-factor authentication (PED-auth)	133
Client software interaction	134
HA (client mediated)	134
HA Indirect Login	135
Functionality Modules (FMs)	135
Partition Roles	135
Backup/Restore	136
STC (Secure Trusted Channel)	137
Converting pre-7.7.0 partitions to V0, or V0 partitions to V1	137
If your application partition is a member of an HA group...	137
If your application partitions have been using STC...	137
To convert from pre-7.7.0 to V0	138
To convert from V0 to V1	138
To convert from V1 to V0	138
Scalable Key Storage (SKS)	139
What is Scalable Key Storage?	139
When to use SKS (Use Cases)	141
When would it be appropriate to use SKS?	141

Security consideration	142
SKS model	142
The SKS model - how it works	142
Characteristics and Implementation Notes	144
Characteristics of the SKS Implementation	144
Functional Notes	145
SMK Locations in a Partition	145
High Availability and SKS	146
Preparing and Administering SKS Partitions	146
Checklist	147
Provisioning SKS	147
Replicating the SMK to another SKS Partition	147
Preparing to use SKS	148
Using SKS	149
Using SKS - options	149
API	149
ckdemo example	150
Java Sample	151
High Availability	151
SKS Backup and Restore	153
Constraints on SKS Backup and Restore	154
Backup the SKS Master Key (SMK)	154
Restore an SKS Master Key (SMK)	155
Backup objects	157
Troubleshooting SKS Backup and Restore	157
SMK Rollover	158
Migrating Scalable Key Storage (SKS)	159
Per-Key Authorization (PKA)	164
Example Use Case	164
New Role and Handling	165
No New Administrative Commands	165
Dependencies and Interactions with Other Features	165
Chapter 6: Key Cloning	166
Overview and Key Concepts	166
Domain Planning	167
What is a security domain or cloning domain?	167
Only one domain per partition - no copying across domains	168
No common domains across Password-authenticated and PED-authenticated HSMs	168
Characteristics of Cloning Domains	169
Cloning Objects to Another Application Partition	170
Cloning Keys Between Luna 6, Luna 7, and Luna Cloud HSM	171
Chapter 7: PED Authentication	176
PED Authentication Architecture	176
Comparing Password and PED Authentication	177
PED Keys	178

PED Key Types and Roles	178
Shared PED Key Secrets	180
M of N Split Secrets (Quorum)	182
PED-Authenticated HSMs with Firmware 7.7.0 (and newer)	183
New-series PED Behavior Notes	183
Updating or Rolling-back PED-auth HSM Firmware	184
Luna PED Received Items	184
Luna PED Hardware Functions	186
Physical Features	186
Keypad Functions	187
Modes of Operation	188
PED with Newer CPU (AC Power Block Now Optional)	189
Local PED Setup	190
Secure Local PED	191
About Remote PED	191
Remote PED Architecture	192
PEDserver-PEDclient Communications	196
Initializing the Remote PED Vector and Creating an Orange Remote PED Key	197
Installing PEDserver and Setting Up the Remote Luna PED	200
Opening a Remote PED Connection	202
Ending or Switching the Remote PED Connection	210
Remote PED Troubleshooting	211
Migrating the Orange Remote PED Key For Luna 7.7.0 or Newer	215
Migrating the Orange RPK(s) Using a Local PED Connection	217
Updating Luna PED Firmware (for older-version PED that requires a power-block)	218
Updating Luna PED Firmware (for USB-powered PED)	221
Preparing for the Upgrade	222
Upgrading the Luna PED Firmware to Version 2.9.0 (or newer)	223
PED Key Management	224
Creating PED Keys	224
Performing PED Authentication	229
Consequences of Losing PED Keys	231
Identifying a PED Key Secret	233
Duplicating Existing PED Keys	234
Changing a PED Key Secret	235
PEDserver and PEDclient	238
The PEDserver Utility	238
The PEDclient Utility	238
pedserver	239
pedserver -appliance	240
pedserver -appliance delete	241
pedserver -appliance list	242
pedserver -appliance register	243
pedserver mode	244
pedserver -mode config	245
pedserver -mode connect	247
pedserver -mode disconnect	248

pedserver -mode show	249
pedserver -mode start	251
pedserver -mode stop	253
pedserver -regen	255
pedclient	255
pedclient -mode assignid	257
pedclient -mode config	258
pedclient -mode deleteid	260
pedclient -mode releaseid	261
pedclient -mode setid	262
pedclient -mode show	263
pedclient -mode start	264
pedclient -mode stop	266
pedclient -mode testid	267
Chapter 8: Initializing an Application Partition	268
Chapter 9: Partition Capabilities and Policies	272
Setting Partition Policies Manually	283
Setting Partition Policies Using a Template	284
Creating a Partition Policy Template	284
Editing a Partition Policy Template	285
Applying a Partition Policy Template	286
Configuring the Partition for Cloning or Export of Private/Secret Keys	287
Cloning Mode	288
Key Export Mode	289
No Backup Mode	289
Chapter 10: Partition Roles	291
Changing a Partition Role Credential	297
Activation and Auto-activation on Multi-factor- (PED-) Authenticated Partitions	299
Enabling Activation on a Partition	300
Activating a Role	300
Security of Your Partition Challenge	303
Name, Label, and Password Requirements	304
Custom Appliance User Accounts	304
Custom Appliance Roles	304
Appliance User Passwords	304
HSM Labels	305
Cloning Domains	305
Partition Names	305
Partition Labels	305
HSM/Partition Role Passwords or Challenge Secrets	305
Chapter 11: Verifying the HSM's Authenticity	307
Public Key Confirmations	307
Verifying the HSM's Authenticity	308

Chapter 12: Migrating Keys to Your New HSM	310
Supported Luna HSMs	310
Migration methods	310
Preconditions	311
Roles required for migration	311
Luna Network HSM (5.x or 6.x) to Luna Network HSM (7.x)	311
Cloning	314
Cloning Using an HA Group	316
Luna USB HSM (5.x or 6.x) to Luna Network HSM (7.x)	318
Backup and Restore	318
Cloning	320
Luna PCIe HSM (5.x or 6.x) to Luna Network HSM (7.x)	322
Backup and Restore	323
Cloning	325
Luna PCIe HSM or Luna USB HSM (5.x or 6.x) to Luna PCIe HSM (7.x)	327
Backup and Restore	327
Cloning	330
Cloning Using an HA Group	332
Moving from Pre-7.7.0 to Firmware 7.7.0 or Newer	334
Chapter 13: High-Availability Groups	336
Client-driven High Availability	336
Planning Your HA Group Deployment	346
HSM and Partition Prerequisites	346
Sample Configurations	347
Setting Up an HA Group	350
Verifying an HA Group	354
Setting an HA Group Member to Standby	356
Configuring HA Auto-Recovery	358
Enabling/Disabling HA Only Mode	358
HA Logging	359
Configuring HA Logging	359
HA Log Messages	361
Adding/Removing an HA Group Member	363
Manually Recovering a Failed HA Group Member	366
Manually Recovering a Failed HA Group Member	366
Replacing an HA Group Member	367
Deleting an HA Group	370
HA Troubleshooting	370
Administration Tasks on HA Groups	370
Unique Object IDs (OUID)	370
Client-Side Limitations	372
Client-Side Failures	372
Failures Between the HSM Appliance and Client	372
Avoid direct access to individual HA group members when securing with STC	372
Effect of PED Operations	373
Updating Luna Network HSM HA Group Members to Luna 7.7.0 or Newer	373

Updating Luna Network HSM HA Group Members to Luna 7.7+ V0 partitions	375
General guidelines for updating or converting of HA member partitions	376
Avoid direct access to individual HA group members when securing with STC	377
Chapter 14: Backup and Restore Using a Luna Backup HSM (G5)	379
Backup and Restore Best Practices	379
Planning Your Backup HSM Deployment	380
Partition to Partition	380
Backup HSM Connected to the Appliance	381
Backup HSM Connected to the Client Workstation	381
Backup HSM Installed Using Remote Backup Service (RBS)	382
About the Luna Backup HSM (G5)	383
Physical Features	384
Luna Backup HSM (G5) Functionality	384
Storage and Maintenance	385
Luna Backup HSM (G5) Required Items	386
Installing the Backup HSM	387
Installing or Replacing the Luna Backup HSM (G5) Battery	388
Backup HSM Secure Transport and Tamper Recovery	390
Creating a Secure Recovery Key	391
Setting Secure Transport Mode	392
Recovering From a Tamper Event or Secure Transport Mode	392
Disabling Secure Recovery	393
Initializing the Backup HSM Remote PED Vector	393
Updating the Luna Backup HSM (G5) Firmware	395
Resetting the Backup HSM to Factory Conditions	397
Backup/Restore Using an Appliance-Connected Luna Backup HSM (G5)	397
Initializing the Backup HSM	398
Backing Up an Application Partition	399
Restoring an Application Partition from Backup	400
Backup/Restore Using a Client-Connected Luna Backup HSM (G5)	401
Initializing the Backup HSM	402
Backing Up an Application Partition	403
Restoring an Application Partition from Backup	404
Configuring a Remote Luna Backup HSM (G5) Server	406
Installing/Configuring the Remote Backup Service	406
Chapter 15: Backup and Restore Using a Luna Backup HSM (G7)	408
Overview and Key Concepts	408
Overview	409
Credentials Required to Perform Backup and Restore Operations	409
Client Software Required to Perform Backup and Restore Operations From a Client Workstation	410
PED Authentication with the Luna Backup HSM (G7)	410
Backup and Restore Best Practices	411
Luna Backup HSM (G7) Hardware Installation	412
Luna Backup HSM Received Items	412
Installing the Luna Backup HSM Hardware	414

Initializing a Client-Connected Luna Backup HSM (G7)	414
Initializing a PED-Authenticated HSM	415
Initializing a Password-Authenticated HSM	418
Backing Up to a Client-Connected Luna Backup HSM (G7)	419
Backing Up a Multi-factor- (PED-) Authenticated Partition	419
Backing Up a Password-Authenticated Partition	424
Restoring From a Client-Connected Luna Backup HSM (G7)	426
Restoring a Multi-factor- (PED-) Authenticated Partition	426
Restoring a Password-Authenticated Partition	429
Initializing an Appliance-Connected Luna Backup HSM (G7)	431
Recovering the Luna Backup HSM (G7) from Secure Transport Mode	431
Initializing a PED-Authenticated HSM	432
Initializing a Password-Authenticated HSM	434
Backing Up to an Appliance-Connected Luna Backup HSM (G7)	435
Backing Up a PED-Authenticated Partition	436
Backing Up a Password-Authenticated Partition	440
Restoring From an Appliance-Connected Luna Backup HSM (G7)	442
Restoring a PED-Authenticated Partition	443
Restoring a Password-Authenticated Partition	446
Backup and Restore to a Remote Backup Service (RBS)-Connected Luna Backup HSM (G7)	447
Installing and Configuring the Remote Backup Service	448
Updating the Luna Backup HSM (G7) Firmware	449
Updating the Client-Connected Luna Backup HSM (G7) Firmware	450
Updating the Appliance-Connected Luna Backup HSM (G7) Firmware	451
Rolling Back the Luna Backup HSM (G7) Firmware	452
Chapter 16: Slot Numbering and Behavior	453
Order of Occurrence for Different Luna HSMs	453
Settings Affecting Slot Order	454
Effects of Settings on Slot List	454
Effects of New Firmware on Slot Login State	455

PREFACE: About the Partition Administration Guide

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

- > ["Luna HSM Client Software Installation" on page 17](#)
- > ["Client-Partition Connections" on page 86](#)
- > ["What are "pre-firmware 7.7.0", and V0, and V1 partitions?" on page 126](#)
- > ["Converting pre-7.7.0 partitions to V0, or V0 partitions to V1" on page 137](#)
- > ["Key Cloning" on page 166](#)
- > ["Scalable Key Storage \(SKS\)" on page 139](#)
- > ["Per-Key Authorization \(PKA\)" on page 164](#)
- > ["PED Authentication" on page 176](#)
- > ["Initializing an Application Partition" on page 268](#)
- > ["Partition Capabilities and Policies" on page 272](#)
- > ["Partition Roles" on page 291](#)
- > ["Verifying the HSM's Authenticity" on page 307](#)
- > ["Migrating Keys to Your New HSM" on page 310](#)
- > ["High-Availability Groups" on page 336](#)
- > ["Backup and Restore Using a Luna Backup HSM \(G5\) " on page 379](#)
- > ["Backup and Restore Using a Luna Backup HSM \(G7\)" on page 408](#)
- > ["Configuring a Remote Luna Backup HSM \(G5\) Server" on page 406](#)
- > ["Slot Numbering and Behavior" on page 453](#)

The preface includes the following information about this document:

- > [Customer Release Notes](#)
- > ["Audience" on the next page](#)
- > ["Document Conventions" on the next page](#)
- > ["Support Contacts" on page 16](#)

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

Customer Release Notes

The customer release notes (CRN) provide important information about this release that is not included in the customer documentation. Read the CRN to fully understand the capabilities, limitations, and known issues for this release. You can view or download the latest version of the CRN from the Technical Support Customer Portal at <https://supportportal.thalesgroup.com>.

Audience

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

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

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

Document Conventions

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

Notes

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

NOTE Take note. Contains important or helpful information.

Cautions

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

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

Warnings

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

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

Command syntax and typeface conventions

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

Support Contacts

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

Customer Support Portal

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

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

Telephone

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

CHAPTER 1: Luna HSM Client Software Installation

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

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

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

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

Choose the instructions for your operating system:

- > ["Windows Luna HSM Client Installation" on the next page](#)
 - ["Scripted/Unattended Windows Installation/Uninstallation" on page 28](#)
- > ["Linux Luna HSM Client Installation" on page 34](#)
 - ["Luna Minimal Client Install for Linux - Overview" on page 43](#)
 - ["Installing Luna Minimal Client on Linux Using Docker" on page 48](#)
 - ["From Linux Minimal Client Create a Docker Container to Access a DPOD Luna Cloud HSM Service" on page 52](#)
 - ["Create a Luna HSM Client Docker image for use with Functionality Modules" on page 53](#)
- > ["AIX Luna HSM Client Installation" on page 63](#)
- > ["Solaris Luna HSM Client Installation" on page 57](#)
- > ["Adding a Luna Cloud HSM Service" on page 68](#)
- > ["Configuration File Summary" on page 70](#)
- > ["Updating the Luna HSM Client Software" on page 85](#)

Windows Luna HSM Client Installation

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

- > "Required Client Software" below
- > "Prerequisites" below
- > "Installing the Luna HSM Client Software" on the next page
- > "Modifying the Installed Windows Luna HSM Client Software" on page 22
- > "Java" on page 23
- > "Luna CSP and KSP" on page 23
- > "Modifying the Number of Luna Backup HSM Slots" on page 24
- > "Uninstalling the Luna HSM Client Software" on page 25
- > "After Installation" on page 27
- > "Troubleshooting" on page 27
- > "Scripted/Unattended Windows Installation/Uninstallation" on page 28

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

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

Prerequisites

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

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

Installing the Luna HSM Client Software

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

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

For compatibility of our HSMs with Windows CAPI we have Luna CSP, and for the newer Windows CNG we have Luna KSP. See "[Luna CSP and KSP](#)" on [page 23](#) for more information.

Interactive (prompted, this page) and non-interactive (no prompts "[Scripted/Unattended Windows Installation/Uninstallation](#)" on [page 28](#)) installation options are available.

CAUTION! Deprecation of Windows Server 2012 R2 and Luna PCIe HSM 6.x

Luna HSM Client 10.3.0 is the last client version to support Windows Server 2012 R2, which accepts the Luna PCIe HSM 6.x driver.

If you intend to use Luna PCIe 6.x HSM (alone or with Luna PCIe 7.x), options include:

- to continue with Windows, remain at Windows Server 2012 R2, and remain at Luna HSM Client 10.3.0, or
- to use newer Windows and future client versions, move any Luna PCIe 7.x HSMs to a separate server, or
- switch to Linux, if your application permits, which continues to support the Luna PCIe 6.x driver and allows version 7.x and 6.x to coexist in one server.

Luna Network HSM (LNH) does not make use of client-side drivers, so you can use newer clients with LNH 6.x and with LNH 7.x, Cloud HSM, etc.

To install the Luna HSM Client software

1. Log into Windows as "Administrator", or as a user with administrator privileges (see "[Troubleshooting](#)" on [page 27](#)).
2. Uninstall any previous versions of the Client software before you proceed (see "[Uninstalling the Luna HSM Client Software](#)" on [page 25](#)).

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

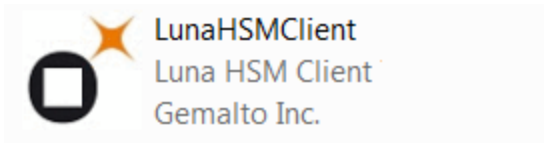
3. Download the Luna HSM Client from the Thales Support Portal at <https://supportportal.thalesgroup.com> and

TIP We recommend verifying the integrity of the Universal 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.

4. Extract the .zip to an appropriate folder.

5. In the extracted directory, locate the folder for your Windows architecture and double click **LunaHSMClient.exe**.



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

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



NOTE Dependencies and considerations when installing:

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

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

- a. Agree to the terms of the License Agreement to proceed with installation. To view the agreement text, click the link in the dialog. The installer loads a PDF version if a PDF reader is available; otherwise it launches a text editor and a plain-text version of the agreement.
 - b. If Windows presents a security notice asking if you wish to install the device driver from 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, Luna USB HSM, or Luna Backup HSMs).
7. When the installation completes, the button options are Uninstall, Modify, or Quit; click **Quit** to finish.



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

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.

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

To modify the installed Luna HSM Client software

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



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



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

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

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

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

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

Java

If you install the Luna Java Security Provider (JSP), refer to [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.

USB-powered PED

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

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

To use the new USB-powered PED

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

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

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

BOOT V.1.1.0-1

CORE V.3.0.0-1

Loading PED...

Entering...

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

Modifying the Number of 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 70.

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:

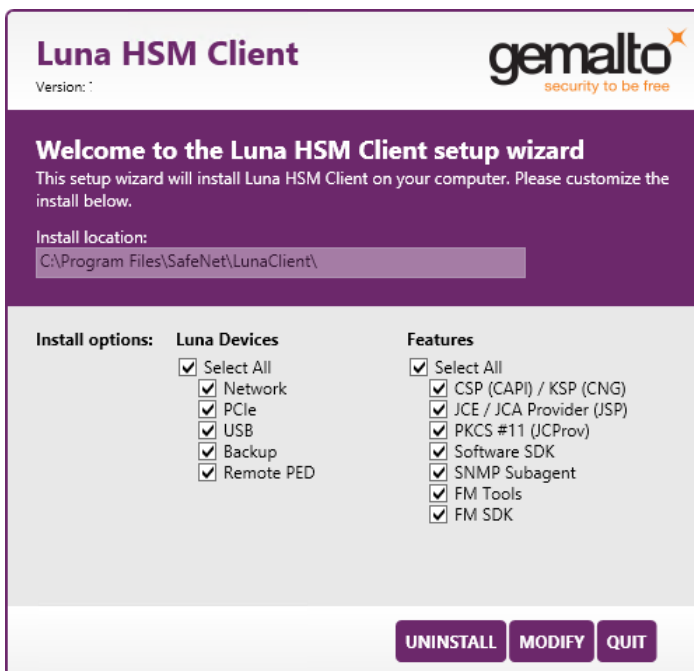
- For Luna Backup HSM (G5):
LunaG5Slots = <value>;
- For Luna Backup HSM (G7):
LunaG7Slots = <value>;

Uninstalling the Luna HSM Client Software

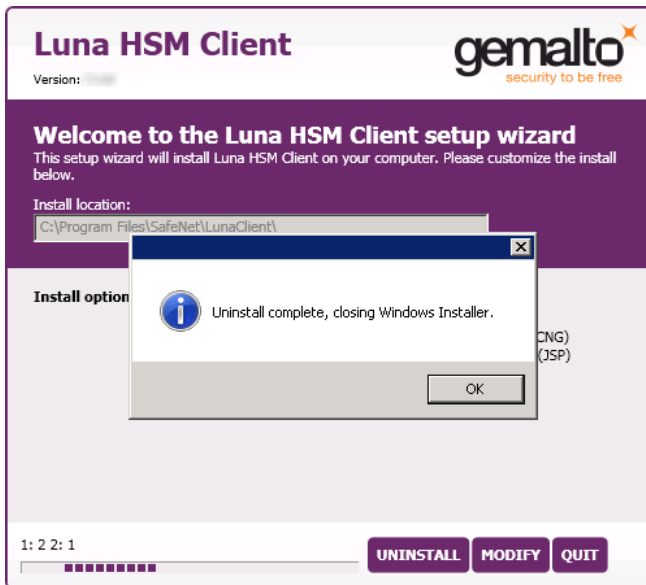
You need to uninstall Luna HSM Client before installing a new version. If you wish to modify the installation (perhaps to add a component or product that you did not previously install), you must uninstall the current installation and re-install with the desired options. If you have a Luna Backup HSM connected to the client workstation, either disconnect it or stop the PEDclient service ("[pedclient -mode stop](#)" on page 266) 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.

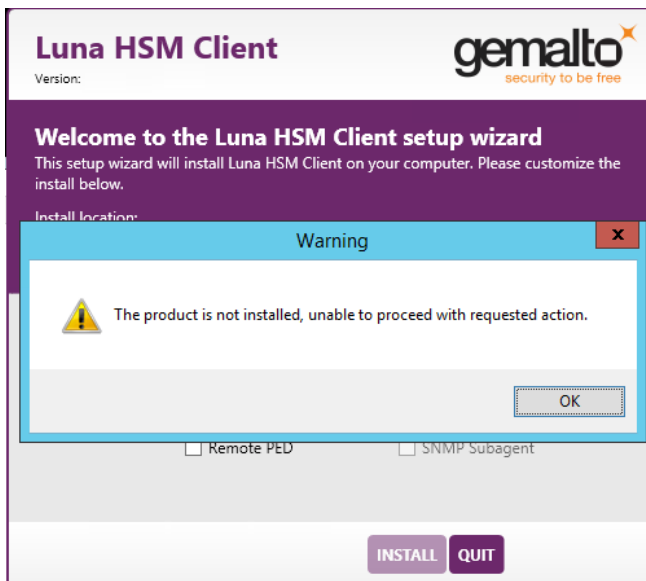


- When the uninstallation is complete, click **OK** to dismiss the operating system's confirmation dialog.

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.

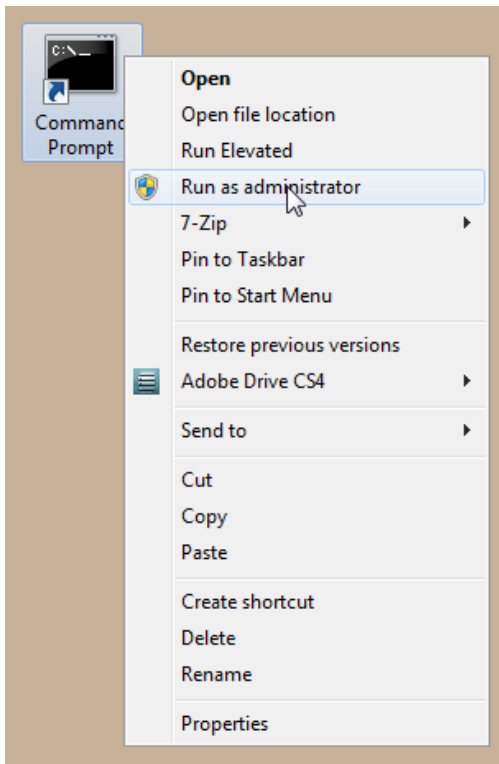
After Installation

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 ["Scripted/Unattended Windows Installation/Uninstallation" on the next page](#) for instructions on how to install the client software from the command line.

Scripted/Unattended Windows Installation/Uninstallation

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

- > ["Command line options overview" below](#)
- > ["Installing the Luna HSM Client for the Luna Network HSM" on page 31](#)
- > ["Installing the Luna HSM Client for the Luna PCIe HSM" on page 31](#)
- > ["Installing the Luna HSM Client for the Luna USB HSM" on page 31](#)
- > ["Installing the Luna HSM Client for the Luna Backup HSM" on page 32](#)
- > ["Installing the Luna HSM Client for Remote PED" on page 32](#)
- > ["Installation Location " on page 32](#)
- > ["Logging" on page 33](#)
- > ["Uninstalling the Luna HSM Client" on page 33](#)

If you want to perform an interactive installation, using the graphical, interactive installer, see ["Windows Luna HSM Client Installation" on page 18](#)

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

Command line options overview

The following command-line options are available:

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

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

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

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

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

The device names are not case-sensitive.

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

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

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

Feature identifier value	Can be installed with these Luna devices	Description
SNMP	PCIe, USB, Backup	SNMP subagent

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

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

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

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

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

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

Installing all components and features

Subsequent sections detail how to install the Luna HSM Client software, drivers (if necessary), and optional features (like Java support and the SDK), for individual HSMs. This section describes how to install everything at once, so that all 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 (Network HSM (no driver), PCIe HSM, Backup HSM, Remote PED), as well as all the features (CSP/KSP, JSP, JCProv, C++ SDK, SNMP Subagent)

LunaHSMClient.exe /install /quiet ADDLOCAL=all

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

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

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

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

Installing the Luna HSM Client for the Luna Network HSM

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

To install the Luna HSM Client for the Luna Network HSM

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

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

LunaHSMClient.exe /install /quiet ADDLOCAL=NETWORK

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

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

LunaHSMClient.exe /install /quiet ADDLOCAL=NETWORK,CSP_KSP,JSP,SDK,JCProv

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

Installing the Luna HSM Client for the Luna PCIe HSM

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

To install the Luna HSM Client for the Luna PCIe HSM

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

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

LunaHSMClient.exe /install /quiet ADDLOCAL=PCI

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

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

LunaHSMClient.exe /install /quiet ADDLOCAL=PCI,CSP_KSP,JSP,SDK,JCProv,SNMP

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

Installing the Luna HSM Client for the Luna USB HSM

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

To install the Luna HSM Client for the Luna USB HSM

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

- > Install for Luna USB HSM

LunaHSMClient.exe /install /quiet ADDLOCAL=USB

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

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

LunaHSMClient.exe /install /quiet ADDLOCAL=USB,CSP_KSP,JSP,SDK,JCProv,SNMP

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

Installing the Luna HSM Client for the 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,snmp

Installing the Luna HSM Client for Remote PED

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

To install the Luna HSM Client for the Luna Backup HSM

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

LunaHSMClient.exe /install /quiet addlocal=ped

Installation Location

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

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

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

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

Logging

If problems are encountered during installation or uninstallation of the software and you wish to determine the reason, or if Thales 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
```

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](#)
- > ["Installing the Client Software" on the next page](#)
- > ["Installing the Minimal Client Software" on page 39](#)
- > ["Controlling User Access to Your Attached HSMs and Partitions" on page 39](#)
- > ["Uninstalling the Client Software or Removing Components" on page 40](#)
- > ["Java" on page 40](#)
- > ["Scripted or Unattended Installation" on page 41](#)
- > ["Interrupting the Installation" on page 42](#)
- > ["Modifying the Number of Luna Backup HSM Slots" on page 42](#)

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

Prerequisites

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

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

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

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

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

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

Debian Requires alien

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

SUSE Linux on IBM PPC

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

Where to install, and SELinux

The instructions on this page assume that much of the installation goes into /usr. If you retain that default location, installation "should just work" uneventfully.

You can change that install location (see "[Flexible Install paths](#)" on the next page). 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 CentOS8 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 make SELinux happy when it is in Enforcing mode.

Installing the Client Software

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

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

The installation script

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

- > interactive: **sh install.sh [-install_directory <prefix>]**
- > all: **sh install.sh all [-install_directory <prefix>]**
- > scriptable: **sh install.sh -p [network|pci|usb|backup|ped] [-c sdk|jsp|jcpov|snmp]|fmsdk|fm_tools [-install_directory </usr>]**

The options on the script are:

- > device(s)
 - "network" is the Luna Network HSM (software only, no drivers)
 - "pci" is the Luna PCIe HSM (software plus driver for the PCI HSM)
 - "usb" is the Luna USB and Backup HSMs (software plus driver for the G5-based and G7-based HSMs)
 - "backup" is software to enable Remote Backup
 - "ped" is software for the Luna Remote PED
- > components include the optional Software Development kit, Java providers, SNMP instance (not needed for Network HSM which has it built in), Functional Module tools, and the Functional Module SDK

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 We recommend verifying the integrity of the Universal 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.

To install the Luna HSM Client software on a Linux workstation

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

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

```
tar xvf <filename>.tar
```

3. Go to the untarred directory for your operating system (**32** or **64**-bit):

```
cd /<untarred_dir>/<32/64>
```

4. To install the software, run the **install.sh** installation script. You can run the script in interactive mode, or you can script the installation, as described in ["Scripted or Unattended Installation" on page 41](#).

- To display the help, or a list of available installer options, type:

```
sudo sh install.sh -? or sudo sh install.sh help
```

- To install all available products and optional components, type:

```
sudo sh install.sh all
```

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

```
sudo sh install.sh
```

NOTE Do not interrupt the installation script in progress. An uninterruptible power supply (UPS) is recommended. See ["Interrupting the Installation" on page 42](#) 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 JCProv (Java)

[4]: Luna SNMP subagent

[5]: Luna Functionality Module Tools

[6]: Luna Functionality Module Software Development Kit

[B|b]: Back to Products selection

[I|i]: Install

[Q|q]: Quit

Enter selection:
```

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

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

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

If the script detects an existing cryptoki library, it stops and suggests that you uninstall your previous 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
```

Installing the Minimal Client Software

The minimal client package contains the minimum run-time libraries required for a cryptography application to connect to Luna Network HSM using PKCS#11 or Java APIs, or Functionality Modules on an FM-enabled HSM. Minimal client install is intended for container instances to interact with Luna HSM partitions or services.

Installing is as simple as copying the tarball and untarring it where you want it. A copy of a configured `Chrystoki.conf` file, along with client and server certificate files (and optionally, STC configuration files) must be available to any instance of Luna Minimal Client at run time.

See "[Luna Minimal Client Install for Linux - Overview](#)" on page 43 for a general example using Docker.

Controlling User Access to Your Attached HSMs and Partitions

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

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

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 (say) `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 Client Software or Removing Components

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

To uninstall the client software

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

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

3. Run the uninstall script:

```
sudo sh uninstall.sh
```

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

To remove individual components

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

Java

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

Scripted or Unattended Installation

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

```
[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
fntools  - Luna Functionality Module Tools
fmsdk    - Luna Functionality Module Software Development Kit
```

```
[myhost]$
```

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.

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 70](#).

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 (G7):
LunaG7Slots = <value>;

Effects of Kernel Upgrades

If you upgrade the Linux kernel after successful installation of Luna 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

No slots visible for Luna Network HSM = user can't read certs directory.

No slots visible for Luna PCIe HSM or Luna USB HSM = user can't read device (/dev/k7pf0, /dev/viper0, or /dev/lunauhd0).

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

Luna Minimal Client Install for Linux - Overview

Minimal client install is intended for container instances to interact with Luna HSM partitions, and contains the minimum run-time libraries required for a cryptography application to connect to Luna Network HSM using PKCS#11 or Java APIs, in addition to some configuration tools. The Luna Minimal Install is provided as a tarball that you can unpack where desired, and choose the files that you need.

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

The minimal client does not have an installer, and **omits** drivers and other material, for backup HSMs, for Luna PED, or for the Luna PCIe HSM. For any of those, you would use the full Luna HSM Client Installer.

Mandatory files for configuration and secure communication, where to get them and where to keep them

The Luna Minimal Client, when installed on minimalist or micro-service containers, requires that you have the appropriate files and folders available

- > Chrystoki.conf configuration file (includes settings, and pointers to resources),
- > certificates folders (for secure communications protocols, NTLS or STC)
- > libraries and plugins required for secure communications protocols.

The Luna Minimal Client tarball includes a "template" version of the `Chrystoki.conf` file that you can edit for any non-default settings needed by your application, and to reflect the actual paths to resources.

Alternatively, you might already have a configured `Chrystoki.conf` file that you can copy into the Docker container with the minimal client, or that you can leave at an external location that is mountable from within the Docker container.

Similarly, the Docker container with the minimal client must have access to the certificates (local host certificate, and certificates from any registered application partitions or Thales Data Protection on Demand (DPoD) Luna Cloud HSM services) for secure communication. Those can reside inside the container, or can reside on an external mountable drive - either way, the paths in the `Chrystoki.conf` file must point to their location.

Configure and link, inside your Docker container

You will need to untar the Minimal Client tarball in your container, or open it elsewhere and copy the desired files to your container.

If you already have a `Chrystoki.conf` file with most, or all, of your desired settings, you can copy it into the container and edit it manually.

If you do not have suitable `Chrystoki.conf` file, the minimal client tarball contains a config template file that you can modify with the configurator utility.

At the same time, you can create and exchange certificates by means of the included `vtl` utility. Ensure that the resulting certificates are pointed-to in `Chrystoki.conf` file. For example instructions, see ["Installing Luna Minimal Client on Linux Using Docker" on page 48](#).

Configure and link, exterior to your Docker container

To configure `Chrystoki.conf` and to establish an NTLS or STC link outside your Docker container, for later use by one-or-more Docker containers, you can

- Untar the Luna Minimal Client tarball at the desired staging location, use configurator or manually edit the `Chrystoki.conf` file, and use `vtl` to establish the secure link to Luna Network HSM appliance.

OR

- Install the full Luna HSM Client, and follow the instructions to create/update the `Chrystoki.conf` file, and create and exchange certificates for a secure link to a Network HSM appliance.

The above could be done before the Docker container is created, or after one exists.

Whether you elect to pre-configure externally, with a full Luna HSM Client Installation or with a copy of the Luna Minimal Client, or from inside each Docker container after it is created (and populated and configured with the Luna Minimal Client), two general networking approaches are possible:

[Network OPTION] Dynamic *private* IP address per container

If each Docker container (default) has a *private* IP address dynamically assigned to the container at run time:

- A single set of configuration file and certificate folders is needed, that will apply to any container within that hidden/translated subnet.
- Each container can mount the needed configuration from the one location on the host.

- Because all containers have the same IP address and appear as the same client, you must *disable ntlis ipchecking* on the Luna Network HSM appliance.

[Network OPTION] Unique *public* IP address per container

If a unique *public* IP address is assigned to each Docker container, visible to the Luna Network HSM appliance:

- A separate NTLS configuration is performed, either externally on the host computer, for each proposed container IP, with the resulting configuration file and certificates folders saved to unique mountable locations on the host file system, OR configuration and certificate exchange is performed from the minimal client within each container after it is created.
- Each container gets its own configuration file and unique certificates whether mounted externally or residing inside the container.
- Because each container has its own unique public IP address, and is considered its own client, keep *ntlis ipcheck enabled* on the Luna Network HSM appliance.

DPoD

With the additional tools included in the minimal install archive, as of release 7.6, the expanded minimal client has the needed tools for local (in-container) configuration. If you intend to connect with DPoD Luna Cloud HSM services, see "[From Linux Minimal Client Create a Docker Container to Access a DPOD Luna Cloud HSM Service](#)" on page 52 for additional steps.

Included in the Minimal Client

The following components are included in the Luna Minimal Client tar ball:

Component	Used or needed for...
JCPROV	
LunaClient-Minimal-<release_version>.x86_64/jcprov/jcprov.jar	JCPROV jar file
LunaClient-Minimal-<release_version>.x86_64/jcprov/64/libjcprov.so	JCPROV library
JSP	
LunaClient-Minimal-<release_version>.x86_64/jsp/LunaProvider.jar	JSP jar file
LunaClient-Minimal-<release_version>.x86_64/jsp/64/libLunaAPI.so	JSP library
LIBRARIES	
LunaClient-Minimal-<release_version>.x86_64/libs/64/libCryptoki2.so	Library to address cryptographic functions of the HSM
LunaClient-Minimal-<release_version>.x86_64/libs/64/libCryptoki2_64.so	Symbolic link pointing to libCryptoki2.so, needed for FM hostapps compiled against libCryptoki2_64.so

Component	Used or needed for...
LunaClient-Minimal -<release_version>. x86_64/libs/64/libethsm.so	Library to interact with Functionality Modules
LunaClient-Minimal -<release_version>. x86_64/libs/64/libSoftToken.so	Library for STC connection (alternative to NTLS)
LunaClient-Minimal -<release_version>. x86_64/libs/64/libcklog2.so	Logging library - invoked by vtl cklog enable command to log commands before passing them to the cryptoki library and the HSM.
PLUG-INS	
LunaClient-Minimal -<release_version>. x86_64/plugins/libdpod.plugin	Enable connection protocol with Luna Cloud HSM services (See also the related XTC and REST sections of chrystoki.conf file)
CONFIGURATION FILES	
LunaClient-Minimal -<release_version>. x86_64/Chrystoki-template.conf	Chrystoki.conf template in case you don't already have a conf file.
LunaClient-Minimal -<release_version>. x86_64/openssl.cnf	Configuration file for OpenSSL.
BINARIES/TOOLS	
LunaClient-Minimal -<release_version>. x86_64/bin/64/mkfm	Allow client to connect to Functionality Modules (if you have installed any in the HSM)
LunaClient-Minimal -<release_version>. x86_64/bin/64/configurator	Configuration file management tool
LunaClient-Minimal -<release_version>. x86_64/bin/64/ckdemo	Demonstrates individual, atomic, PKCS#11 operations in the HSM
LunaClient-Minimal -<release_version>. x86_64/bin/64/lunacm	Partition administration tool
LunaClient-Minimal -<release_version>. x86_64/bin/64/cmu	Certificate Management Utility
LunaClient-Minimal -<release_version>. x86_64/bin/64/multitoken	Perform multiple crypto commands on multiple slots
LunaClient-Minimal -<release_version>. x86_64/bin/64/pscp LunaClient-Minimal -<release_version>. x86_64/bin/64/plink	Used for One Step NTLS
LunaClient-Minimal -<release_version>. x86_64/bin/64/salopin	Persistent application connection tool
LunaClient-Minimal -<release_version>. x86_64/bin/64/vtl	Configuration tool (certificate creation and exchange, registration of clients with partitions, logging, etc.)
LICENSE AGREEMENT	

Component	Used or needed for...
LunaClient-Minimal-<release_version>.x86_64/008-010068-001_EULA_HSM7_SW_revB.pdf	
LunaClient-Minimal-<release_version>.x86_64/008-010068-001_EULA_HSM7_SW_revB.txt	

The configuration template file is included, in case you wish to populate it via direct editing (perhaps by script). Otherwise, a configuration file is created and modified when you perform a full (non-minimal) installation and configuration elsewhere, and you can simply have your Docker containers mount the external location to make use of the resulting `chrystoki.conf` file and certificate folders.

Installation Prerequisites

Ensure that you have the following prerequisites before installing the Luna Minimal Client:

- > A Linux host system with Docker installed (see <https://www.docker.com/> for Docker download and install)
- > A copy of the Luna Minimal Client tarball package
- > A Luna Network HSM 7.x appliance, already initialized and ready to use (or an account for access to DPOD Luna Cloud HSM services) -- perform any of the actions not already done:
 - Configure the Luna Network HSM network settings.
 - Initialize the HSM.
 - Create an application partition on the Network HSM.
 - Exchange host certificates between Luna HSM Client and the Luna Network HSM and register each with the other (On the client side, add the Network HSM's certificate to the server certs folder and to the CAFile. On the Network HSM, register the client with `lunash:>client register`).
 - Start the NTLS service on the appliance with `lunash:>service restart ntl`, and assign the client to the application partition with `lunash:>client assign partition`.
 - On the client side, use LunaCM to configure the application partition (see "[Initializing an Application Partition](#)" on page 268), initializing the partition and creating roles as appropriate.
 - After configuring Luna HSM Client on a host system, edit the `Chrystoki.conf` file for use in containers, as described in "[Preparing the Configuration File for Use with Luna Minimal Client and Docker](#)" below.
- > A working knowledge of Docker.

Preparing the Configuration File for Use with Luna Minimal Client and Docker

Make the following edits to the `Chrystoki.conf` file before using it in the containers:

1. Change all the library paths (for example `LibUNIX64`) to `/usr/local/luna/libs/64`
2. Change the certificate and client token paths to the the directory you are making available to the containers at run-time (for example `/usr/local/luna/config/certs`)

Entry in Chrystoki.conf	Value in the host system	Value in the containers
ClientPrivKeyFile	/usr/safenet/lunaclient/cert/client	/usr/local/luna/config/certs
ClientCertFile	/usr/safenet/lunaclient/cert/client	/usr/local/luna/config/certs
ServerCAFile	/usr/safenet/lunaclient/cert/server	/usr/local/luna/config/certs/
PartitionPolicyTemplatePath	/usr/safenet/lunaclient/data/partition_policy_templates	/usr/local/luna/config/ppt/partition_policy_templates
LibUNIX64	/usr/safenet/lunaclient/lib/libCryptoki2_64.so	/usr/local/luna/libs/64/libCryptoki2.so
ClientTokenLib	/usr/safenet/lunaclient/lib/libSoftToken.so	/usr/local/luna/libs/64/libSoftToken.so
SoftTokenDir	/usr/safenet/lunaclient/configData/token	/usr/local/luna/config/stc/token
ClientIdentitiesDir	/usr/safenet/lunaclient/data/client_identities	/usr/local/luna/config/stc/client_identities
PartitionIdentitiesDir	/usr/safenet/lunaclient/data/partition_identities	/usr/local/luna/config/stc/partition_identities
ToolsDir	/usr/safenet/lunaclient/bin	/usr/local/luna/bin/64
SSLConfigFile	/usr/safenet/lunaclient/bin/openssl.cnf	/usr/local/luna/openssl.cnf

Ready to Install Minimal Client

For detailed instructions, see ["Installing Luna Minimal Client on Linux Using Docker"](#) below.

For additional instructions on using the minimal client with Functionality Modules, see ["Create a Luna HSM Client Docker image for use with Functionality Modules"](#) on page 53.

For additional instructions on using the minimal client with DPoD Luna Cloud HSM services, see ["From Linux Minimal Client Create a Docker Container to Access a DPoD Luna Cloud HSM Service"](#) on page 52.

Installing Luna Minimal Client on Linux Using Docker

The following procedure allows you to install the Luna Minimal Client in a Docker container on Linux, so that applications in that container can access Luna Network HSM partitions. For an overview description of Luna Minimal Client and its prerequisites, see ["Luna Minimal Client Install for Linux - Overview"](#) on page 43.

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

If SELinux is enabled in Enforcing mode, you must assign proper permissions to any container that needs to access the config directory.

To install the Luna Minimal Client software on a Linux 64-bit Docker instance:

This example uses NTLS. The use of STC is optional.

This example is based on CentOS 7; other operating systems might require adjustments to the commands and to the docker file.

1. Create a directory. In this example:


```
$HOME/luna-docker
```

The name is not important, only that you use it consistently.

2. Create the following subdirectories under that first directory:

```
$HOME/luna-docker/config
$HOME/luna-docker/config/certs
```

additionally, if you are configuring STC:

```
$HOME/luna-docker/config/stc
$HOME/luna-docker/config/stc/client_identities
$HOME/luna-docker/config/stc/partition_identities
$HOME/luna-docker/config/stc/token/001
```

and create an empty file

for pre-7.7.0

```
$HOME/luna-docker/config/stc/token/001/token.db
```

for 7.7.0 onward

```
$HOME/usr/safenet/lunaclient/configData/token/001/token_v2.db
```

The contents of the config directory are needed by the Docker containers.

3. Copy the Luna Minimal Client tarball to **\$HOME/luna-docker**.
4. Untar the Luna Minimal Client tarball.


```
>tar -xf $HOME/luna-docker/LunaClient-Minimal-<release_version>.x86_64.tar -C $HOME/luna-docker
```
5. Copy the Chrystoki.conf file from the Minimal Client directory to **\$HOME/luna-docker/config**.


```
>cp $HOME/luna-docker/LunaClient-Minimal-<release_version>.x86_64/Chrystoki-template.conf $HOME/luna-docker/config/Chrystoki.conf
```
6. Define the following environment variable:


```
>export ChrystokiConfigurationPath=$HOME/luna-docker/config
```
7. [Optional] If you choose to use STC, review the Luna Network HSM documentation and modify the following instructions. The goal is to have an HSM partition created and registered with the full Luna HSM Client before you create the Docker image and containers.
8. Update the Chrystoki.conf file paths so the tools work as expected


```
>MIN_CLIENT_DIR=$HOME/luna-docker/LunaClient-Minimal-<release_version>.x86_64
>$MIN_CLIENT_DIR/bin/64/configurator setValue -s Chrystoki2 -e LibUNIX -v $MIN_CLIENT_DIR/libs/64/libCryptoki2.so
>$MIN_CLIENT_DIR/bin/64/configurator setValue -s Chrystoki2 -e LibUNIX64 -v $MIN_CLIENT_DIR/libs/64/libCryptoki2_64.so
>$MIN_CLIENT_DIR/bin/64/configurator setValue -s Misc -e ToolsDir -v $MIN_CLIENT_DIR/bin/64
>$MIN_CLIENT_DIR/bin/64/configurator setValue -s "LunaSA Client" -e SSLConfigFile -v $MIN_CLIENT_DIR/openssl.cnf
```

```

>$MIN_CLIENT_DIR/bin/64/configurator setValue -s "LunaSA Client" -e ClientPrivKeyFile -v
$HOME/luna-docker/config/certs/dockerlunaclientKey.pem
>$MIN_CLIENT_DIR/bin/64/configurator setValue -s "LunaSA Client" -e ClientCertFile -v
$HOME/luna-docker/config/certs/dockerlunaclient.pem
>$MIN_CLIENT_DIR/bin/64/configurator setValue -s "LunaSA Client" -e ServerCAFile -v
$HOME/luna-docker/config/certs/CAFile.pem
>$MIN_CLIENT_DIR/bin/64/configurator setValue -s "Secure Trusted Channel" -e
ClientTokenLib -v $MIN_CLIENT_DIR/libs/64/libSoftToken.so
>$MIN_CLIENT_DIR/bin/64/configurator setValue -s "Secure Trusted Channel" -e SoftTokenDir
-v $HOME/luna-docker/config/stc/token
>$MIN_CLIENT_DIR/bin/64/configurator setValue -s "Secure Trusted Channel" -e
ClientIdentitiesDir -v $HOME/luna-docker/config/stc/client_identities
>$MIN_CLIENT_DIR/bin/64/configurator setValue -s "Secure Trusted Channel" -e
PartitionIdentitiesDir -v $HOME/luna-docker/config/stc/partition_identities

```

9. Create a Luna HSM Client certificate for the Docker containers.

```
>$MIN_CLIENT_DIR/bin/64/vtl createCert -n <cert_name>
```

10. Copy the client certificate to the Luna Network HSM appliance.

```
>scp $HOME/luna-docker/config/certs/<cert_name>.pem admin@<Network_HSM_IP>:
```

11. Copy the appliance server certificate (**server.pem**) to **\$HOME/luna-docker/config/certs**

```
>scp admin@<Network_HSM_IP>:server.pem $HOME/luna-docker/config/certs
```

12. Register the appliance server certificate with the Client.

```
>$MIN_CLIENT_DIR/bin/64/vtl addServer -c $HOME/luna-docker/config/certs/server.pem -n
<Network_HSM_IP>
```

13. Connect via SSH to the Luna Network HSM appliance and log in to LunaSH.

```
>ssh admin@<Network_HSM_IP>
```

14. Create a partition, if one does not already exist on the HSM.

```
lunash:>partition create -partition <partition_name>
```

15. Register the full Luna HSM Client with the appliance, and assign the partition to the client.

```
lunash:> client register -client <client_name> {-ip <client_IP> | -hostname <client_hostname>}
```

```
lunash:> client assignpartition -client <client_name> -partition <partition_name>
```

```
lunash:> ntlsl ipcheck disable
```

```
lunash:> exit
```

16. On the Client workstation, run LunaCM, set the active slot to the registered partition, and initialize it.

```
>$MIN_CLIENT_DIR/bin/64/lunacm
```

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

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

```
lunash:> exit
```

17. Update the paths of the libraries, certs and general fields to their future Docker image locations within the **\$ChrystokiConfigurationPath/Chrystoki.conf**.

```
>sed -i -e 's#"$HOME"/luna-docker/config#/usr/local/luna/config#g' -e 's#"$HOME"/luna-docker/LunaClient-Minimal-([0-9\.]+\.)x86_64#/usr/local/luna#g'
$ChrystokiConfigurationPath/Chrystoki.conf
```

Create a Luna HSM Client Docker image

The minimal client tarball includes files necessary for basic operation, and some tools; copy any additional files you want to include in the docker image to **\$HOME/luna-docker/**. This example includes the entire Luna Minimal Client.

18. Create a file named Dockerfile with the following contents:

```
FROM ubuntu:xenial
#FROM centos:centos7

ARG MIN_CLIENT
COPY $MIN_CLIENT.tar /tmp
RUN mkdir -p /usr/local/luna
RUN tar xvf /tmp/$MIN_CLIENT.tar --strip 1 -C /usr/local/luna
ENV ChrystokiConfigurationPath=/usr/local/luna/config
ENV PATH="/usr/local/luna/bin/64:${PATH}"

# The package below is necessary for One-Step NTLS if you want to setup NTLS within the Docker
# container.
# The only requirement beyond glibc.i686 (required by plink and pscp) would be a configured
# Chrystoki.conf
# The minimal client documentation section 8 has example commands, you should modify the value
# parameter ("-v")
# to point to desired files/directories.
# One-Step NTLS uses the section "Misc" entry "ToolsDir" to find the plink/pscp binaries,
# The Chrystoki.conf needs the following entries to be updated for One-Step NTLS to work:
# Section      | Entry
# -----
# Chrystoki2   | LibUNIX
# Chrystoki2   | LibUNIX64
# Misc         | ToolsDir
# "LunaSA Client" | SSLConfigFile
# "LunaSA Client" | ClientPrivKeyFile
# "LunaSA Client" | ClientCertFile
# "LunaSA Client" | ServerCAFile
# Syntax: configurator setValue -s <Section> -e <Entry> -v <value>
# Example: configurator setValue -s Misc -e ToolsDir -v /usr/local/luna/bin/64
# Ubuntu:
#RUN dpkg --add-architecture i386
#RUN apt-get update
#RUN apt-get -y install libc6:i386
# Centos:
#RUN yum install -y glibc.i686

ENTRYPOINT /bin/bash
#End of the Dockerfile
```

19. Build a Docker image.

```
>docker build . --build-arg MIN_CLIENT=LunaClient-Minimal-<release_version>.x86_64 -t
lunaclient-image
```

20. Use the following command to verify the Docker image has been created:

```
>docker images
```

Run the Docker container

21. Make the contents of the config directory available to the Containers when you create them, by mounting the config directory as a volume.

```
>docker run -it --name lunaclient -v $PWD/config:/usr/local/luna/config lunaclient-image
```

22. From the Docker container, verify that the container has a connection to the Luna Network HSM partition.

Functionality Modules (FMs) with Luna Minimal Client

To use FMs with the minimal client, see ["Create a Luna HSM Client Docker image for use with Functionality Modules" on the next page](#).

Thales Data Protection on Demand Luna Cloud HSM Service with Luna Minimal Client

To connect to Thales Data Protection on Demand (DPoD) Luna Cloud HSM services with the minimal client, see ["From Linux Minimal Client Create a Docker Container to Access a DPOD Luna Cloud HSM Service" below](#).

From Linux Minimal Client Create a Docker Container to Access a DPOD Luna Cloud HSM Service

This section describes steps to view Thales Data Protection on Demand (DPoD) Luna Cloud HSM services from a Luna Minimal Client. This example assumes that you have followed the steps in ["Installing Luna Minimal Client on Linux Using Docker" on page 48](#), or have otherwise created the appropriate directories and Dockerfile. This section assumes you have purchased a Luna Cloud HSM service.

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

1. Download the Luna Cloud HSM service client configuration zip file.
2. Unzip the Luna Cloud HSM service client configuration zip file.


```
>cd $HOME/luna-docker
>mkdir $HOME/luna-docker/dpod
>unzip </path/to/luna-cloud-hsm-client>.zip -d $HOME/luna-docker/dpod
```
3. Copy the Luna Cloud HSM service certificates into the certificate directory on the shared volume so that the Docker container can use them.


```
>cp $HOME/luna-docker/dpod/server-certificate.pem $HOME/luna-docker/config/certs/
>cp $HOME/luna-docker/dpod/partition-ca-certificate.pem $HOME/luna-docker/config/certs/
```

- ```
>cp $HOME/luna-docker/dpod/partition-certificate.pem $HOME/luna-docker/config/certs/
```
4. Copy over the entire REST and XTC sections from the unzipped Chrystoki.conf located at **\$HOME/luna-docker/dpod/Chrystoki.conf**:
 

```
>cat $HOME/luna-docker/dpod/Chrystoki.conf
```

```
>vi $HOME/luna-docker/config/Chrystoki.conf
```
  5. Update **\$HOME/luna-docker/config/Chrystoki.conf** with the expected paths that will be used by the Docker container.
 

```
>export ChrystokiConfigurationPath=$HOME/luna-docker/config
```

```
>MIN_CLIENT_DIR=$HOME/luna-docker/LunaClient-Minimal-<release_version>.x86_64
```

```
>$MIN_CLIENT_DIR/bin/64/configurator setValue -s XTC -e PartitionCAPath -v /usr/local/luna/config/certs/partition-ca-certificate.pem
```

```
>$MIN_CLIENT_DIR/bin/64/configurator setValue -s XTC -e PartitionCertPath00 -v /usr/local/luna/config/certs/partition-certificate.pem
```

```
>$MIN_CLIENT_DIR/bin/64/configurator setValue -s REST -e SSLClientSideVerifyFile -v /usr/local/luna/config/certs/server-certificate.pem
```
  6. The Luna Minimal Client now includes a Luna Cloud HSM service plugin which allows the LUNA client to be able to communicate with a Luna Cloud HSM service. That file can be located under **\$HOME/luna-docker/LunaClient-Minimal-<release\_version>.x86\_64/plugins/libdpod.plugin**. This example uses the Dockerfile mentioned above which extracts the Luna Minimal Client tarball into the Docker image.
 

```
>$MIN_CLIENT_DIR/bin/64/configurator setValue -s Misc -e PluginModuleDir -v /usr/local/luna/plugins
```
  7. Attach the Docker container. If it is stopped you must start the container first.
 

```
>docker ps -a
```

```
>docker start <container_id>
```

```
>docker attach <container_id>
```
  8. At this point you should be able to see the Luna Cloud HSM service
 

```
>lunacm
```

## Create a Luna HSM Client Docker image for use with Functionality Modules

The example "[Installing Luna Minimal Client on Linux Using Docker](#)" on page 48 uses the Luna Minimal Client to gain connection to a Luna Network HSM partition. This section explores some additional steps to sign a Functionality Module (FM) from a Docker container, and also execute a Host Application in order to communicate with the Functionality Module in the Luna Network HSM.

**NOTE** This feature requires minimum client version 7.4. See [Version Dependencies by Feature](#) for more information.

FMs consist of two components - the FM itself, that resides in the HSM, extending its functionality, and the Host Application component that resides with the clients that need to connect with that FM.

Due to the size of the FM SDK and ELDK, those have not been included in the Minimal Client as they would greatly expand the size of the minimal client. The assumption is that you installed the full Luna HSM Client with HSM Software Development Kit, FM Software Development Kit and other components, and then created and compiled your Functionality Modules elsewhere, and that you would be importing FM components and using FMs, but not developing and compiling them inside a Docker container.

But the above-mentioned use-cases should help in common tasks such as signing Functionality Modules or Communicating with them via Host Applications.

1. On a Linux client with the Functionality Module SDK Component installed (which also installs the Embedded Linux Development Kit (ELDK)), compile the sample FMs and Host application binaries.

```
>make -C /usr/safenet/lunafmsdk/samples/pinenc all
```

```
>make -C /usr/safenet/lunafmsdk/samples/skeleton all
```

```
>make -C /usr/safenet/lunafmsdk/samples/wrap-comp all
```

2. Create a directory on the shared volume to store the Host applications and unsigned FM binaries.

```
>mkdir $HOME/luna-docker/config/fm
```

3. Copy the generated files over.

```
>cp /usr/safenet/lunafmsdk/samples/pinenc/fm/bin-ppc/* $HOME/luna-docker/config/fm/
```

```
>cp /usr/safenet/lunafmsdk/samples/skeleton/fm/bin-ppc/* $HOME/luna-docker/config/fm/
```

```
>cp /usr/safenet/lunafmsdk/samples/wrap-comp/fm/bin-ppc/* $HOME/luna-docker/config/fm/
```

```
>cp /usr/safenet/lunafmsdk/samples/pinenc/host/output/bin/* $HOME/luna-docker/config/fm/
```

```
>cp /usr/safenet/lunafmsdk/samples/skeleton/host/output/bin/* $HOME/luna-docker/config/fm/
```

```
>cp /usr/safenet/lunafmsdk/samples/wrap-comp/host/output/bin/* $HOME/luna-docker/config/fm/
```

4. Go back to the Docker container. If it is stopped you must start the container first.

```
>docker ps -a
```

```
>docker start <container_id>
```

```
>docker attach <container_id>
```

5. If you have not already done so, enable **LoginAllowedOnFMEnabledHSMs=1** in the `Chrystoki.conf` file, else you will be prompted on your first **partition init** or **role login** attempt to do so in LunaCM.

```
>configurator setValue -s Misc -e LoginAllowedOnFMEnabledHSMs -v 1
```

6. Ensure that the "Partition SO" and "Crypto Officer" users are initialized via LunaCM (see ["Initializing an Application Partition" on page 268](#) and ["The following procedures will allow you to initialize the Crypto Officer \(CO\) and Crypto User \(CU\) roles and set an initial credential." on page 295](#)).

7. Generate a key pair and Self-Signed Certificate, then sign the FM binary using **mkfm** and export the Self-Signed Certificate.

```
>cmu generatekeypair -labelpublic=fmpub -labelprivate=fmpri -sign=1 -verify=1 -keytype=rsa -mech=pkcs -publicexponent=3 -modulusbits=2048 -slot <slotnum>
```

```
>cmu list -slot <slotnum>
```

```
>cmu selfsigncertificate -publichandle=<public_key_handle> -privatehandle=<private_key_handle>
-label=FmSign -serialnumber=1 -cn=FmSign -startdate=20180606 -enddate=20201231 -slot
<slotnum>
```

```
>mkfm -f /usr/local/luna/config/fm/pinenc.bin -o /usr/local/luna/config/fm/pinenc.fm -
kSLOTID=<slotnum>/fmpri
```

```
>mkfm -f /usr/local/luna/config/fm/skeleton.bin -o /usr/local/luna/config/fm/skeleton.fm -
kSLOTID=<slotnum>/fmpri
```

```
>mkfm -f /usr/local/luna/config/fm/wrap-comp.bin -o /usr/local/luna/config/fm/wrapcomp.fm -
kSLOTID=<slotnum>/fmpri
```

```
>cmu export -slot <slotnum> -label FmSign -outputfile=/usr/local/luna/config/fm/FmSign.cert
```

- Copy the signed FMs and Self-Signed Certificate to the Luna Network HSM appliance. If your Docker container supports scp, then use that. If you've uncommented the pre-requisites in the Dockerfile regarding **pscp** and **plink**, then you could use that as well. If the above two scenarios are not applicable, you can always copy the files from the shared fm directory volume:

```
>pscp $HOME/luna-docker/config/fm/pinenc.fm admin@<Network_HSM_IP>:
```

```
>pscp $HOME/luna-docker/config/fm/skeleton.fm admin@<Network_HSM_IP>:
```

```
>pscp $HOME/luna-docker/config/fm/wrapcomp.fm admin@<Network_HSM_IP>:
```

```
>pscp $HOME/luna-docker/config/fm/FmSign.cert admin@<Network_HSM_IP>:
```

- Connect via SSH to the Luna Network HSM appliance and log in to LunaSH.

```
>ssh admin@<Network_HSM_IP>
```

- Login as the HSM Admin (SO), then load the Functionality Modules.

```
lunash:> hsm login
```

```
lunash:> hsm fm load -fmFile pinenc.fm -certFile FmSign.cert
```

```
lunash:> hsm fm load -fmFile skeleton.fm -certFile FmSign.cert
```

```
lunash:> hsm fm load -fmFile wrapcomp.fm -certFile FmSign.cert
```

```
lunash:> hsm fm status
```

- If the **hsm fm status** command, in the previous step, mentioned “reboot HSM to activate” on any of the FMs, then you must reboot the HSM. Upon restarting the HSM, SO login status will be reset, thus you will have to login as SO later.

```
lunash:> hsm restart
```

```
lunash:> hsm login
```

- Activate Secure Memory File System (SMFS); you must be logged in as the HSM Admin. If you check the status of the FMs, they should all be “Enabled” status now.

```
lunash:> hsm fm smfs activate
```

```
lunash:> hsm fm status
```

- Verify that the Host Application can interact with the FM. If you have trouble loading the shared libraries, you can set the LD\_LIBRARY\_PATH environment variable.

```
>export LD_LIBRARY_PATH="/usr/local/luna/libs/64"
```

```
>/usr/local/luna/config/fm/pinenctest -s<slotnum> gen
>/usr/local/luna/config/fm/pinenctest -d<slotnum> test
>/usr/local/luna/config/fm/skeleton -s<slotnum> -t "Hello all"
>/usr/local/luna/config/fm/wrapcomptest -s<slotnum>
```



# Solaris Luna HSM Client Installation

**NOTE** Solaris Client was not included for Luna HSM 7.7.0 or 7.7.1 releases, or Universal Client 10.2 or 10.3.

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

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

- > ["Prerequisites" below](#)
- > ["Installing the Client Software" on the next page](#)
- > ["Solaris Luna HSM Client Installation" above](#)
- > ["Uninstalling the Luna HSM Client Software" on page 60](#)
- > ["Java" on page 60](#)
- > ["Scripted or Unattended Installation" on page 60](#)
- > ["Interrupting the installation - \[Ctrl\] \[C\]" on page 61](#)

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

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

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

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

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

## Prerequisites

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

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

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

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

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

## RNG/EGD

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

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

## Entropy Pool

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

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

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

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

## Installing the Client Software

**TIP** We recommend verifying the integrity of the Universal 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.

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

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

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

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

1. Log on to the client system, open a console or terminal window, and use **su** to gain administrative permissions for the installation.

2. Access the Luna HSM Client software:
  - a. Copy or move the **.tar** archive to a suitable directory where you can untar the archive and launch the installation script.
  - b. Extract the contents from the archive:

```
tar xvf <filename>.tar
```

3. Go to the install directory for your architecture:

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

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

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

```
sh install.sh -? or sh install.sh --help
```

To install all available products and optional components, type:

```
sh install.sh all
```

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

```
sh install.sh
```

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

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

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

**NOTE** The installer includes the 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 for use with your agent.

9. 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.
10. The system installs all packages related to the products and any optional components that you selected.
11. Although FMs are supported on Linux and Windows clients only in this release, the FM architecture requires a configuration file setting to allow partition login on an FM-enabled HSM. If the HSM you will be using with this client is FM-enabled (see "[Preparing the Luna Network HSM to Use FMs](#)" on page 1 for more information), you must add the following entry to the [Misc] section of the Chrystoki.conf file:

**[Misc]**

**LoginAllowedOnFMEnabledHSMs=1**

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

## Uninstalling the Luna HSM Client Software

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

## Java

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

## Scripted or Unattended Installation

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

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

At least one product should be specified.

usage:

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

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

-p <list of Luna products>
```

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

#### Luna products options

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

#### Luna components options

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

```
[myhost]$
```

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

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

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

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

```
If you select 'yes' or 'y' you agree to be bound by all the terms
and conditions 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 AND Luna Backup HSM.
```

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

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

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

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

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

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

### **What to do if installation is incomplete or damaged**

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

## AIX Luna HSM Client Installation

**NOTE** AIX Client was not included for Luna HSM 7.7.0 or 7.7.1 releases, or Universal Client 10.2 or 10.3.

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

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

- > ["Prerequisites" below](#)
- > ["Installing the Client Software" below](#)
- > ["AIX Luna HSM Client Installation" above](#)
- > ["Uninstalling the Luna HSM Client Software" on page 66](#)
- > ["Installing Java" on page 66](#)
- > ["Scripted or Unattended Installation" on page 66](#)
- > ["Interrupting the Installation" on page 67](#)

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

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

### Prerequisites

Each computer that connects to the Luna Network HSM appliance as a Client must have the cryptoki library, the vtl client shell and other utilities and supporting files installed. Each computer that is connected to a Luna Remote Backup HSM must have the cryptoki library and other utilities and supporting files installed - in this case, that would be a Windows or Linux computer with the "Luna Backup HSM" option chosen when Luna Client software is installed.

**TIP** We recommend verifying the integrity of the Universal 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.

### Installing the Client Software

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

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

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

```
tar xvf <filename>.tar
```

4. Change directory to the software version suitable for your system.
5. Install the client software as follows:

- To see the 'help', or a list of available installer options, type:

```
sh install.sh -? or ./sh install.sh --help
```

- To install all available products and optional components, type:

```
sh install.sh all
```

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

```
sh install.sh
```

**NOTE** Do not interrupt the installation script in progress. An uninterruptible power supply (UPS) is recommended. See ["Interrupting the Installation" on page 67](#) for more information.

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

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

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

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

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

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

```
(y/n)
```

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

```
Products
```

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

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

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



[Q|q]: Quit

Enter selection: 1

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

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

Products

Choose Luna Products to be installed

[1]: Luna Network HSM

[N|n]: Next

[Q|q]: Quit

Enter selection: 1

Advanced

Choose Luna Components to be installed

[1]: Luna SDK

\*[2]: Luna JSP (Java)

\*[3]: Luna JCProv (Java)

[B|b]: Back to Products selection

[I|i]: Install

[Q|q]: Quit

Enter selection:

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

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

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

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

11. Although FMs are supported on Linux and Windows clients only in this release, the FM architecture requires a configuration file setting to allow partition login on an FM-enabled HSM. If the HSM you will be

using with this client is FM-enabled (see ["Preparing the Luna Network HSM to Use FMs" on page 1](#) for more information), you must add the following entry to the [Misc] section of the Chrystoki.conf file:

**[Misc]**

**LoginAllowedOnFMEnabledHSMs=1**

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

## Uninstalling the Luna HSM Client Software

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

### To uninstall the Luna HSM Client software:

1. Log in as root. (use sudo instead)
2. Go to the client installation directory:  
**cd /usr/safenet/lunaclient/bin**
3. Run the uninstall script:  
**sudo sh uninstall.sh**

## Installing Java

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

## Scripted or Unattended Installation

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

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

At least one product should be specified.

usage:

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

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

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

Luna products options

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

Luna components options

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

```
[myhost]$
```

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

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

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

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

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

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

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

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

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

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

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

## Interrupting the Installation

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

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

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

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

## Adding a 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.

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

**NOTE** This feature requires minimum Luna HSM Client version 10.2. See [Version Dependencies by Feature](#) for more information.

### Prerequisites

- > You must be using Luna HSM Client software version 10.2 or higher (see ["Updating the Luna HSM Client Software" on page 85](#)).
- > 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 18](#)
  - ["Linux Luna HSM Client Installation" on page 34](#)
- > Luna Cloud HSM services are only compatible with password-authenticated Luna Network HSM partitions. For more information on Luna/Luna Cloud HSM service compatibility, refer to ["Cloning Keys Between Luna 6, Luna 7, and Luna Cloud HSM" on page 171](#). You can still use Luna Cloud HSM and PED-authenticated Luna partitions from the same client workstation, but they cannot clone cryptographic objects between them.
- > You must create a Luna Cloud HSM service using Thales DPoD:  
<https://cpl.thalesgroup.com/encryption/cloud-hsm-services-on-demand>

### 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 Luna HSM Client workstation using `pscp`, `scp`, or other secure means.
2. Extract the `.zip` file into a directory on your client workstation.
3. Extract or untar the appropriate client package for your operating system. Do not extract to a new subdirectory; place the files in the 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 script to create a new configuration file containing information required by the Luna Cloud HSM service.

- [Windows] Right-click **setenv.cmd** and select **Run as Administrator**.
- [Linux] Source the **setenv** script.

```
source ./setenv
```

- Open the configuration file in the Luna Cloud HSM service client directory.

- [Windows] **crystoki.ini**
- [Linux] **Chrystoki.conf**

- Copy the following sections from the Luna Cloud HSM service client configuration file to the existing version in the Luna HSM Client install directory.

```
[XTC]
Enabled=1
TimeoutSec=600

[REST]
AuthTokenClientId=<AuthTokenClientId>
AuthTokenClientSecret=<AuthTokenClientSecret>
AuthTokenConfigURI=<AuthTokenConfigURI>
ClientConnectIntervalMs=1000
ClientConnectRetryCount=900
ClientEofRetryCount=15
ClientPoolSize=32
ClientTimeoutSec=120
RestClient=1
ServerName=<ServerName>
ServerPort=443
```

Also, add the path to the plugins directory to the [Misc] section in your configuration file:

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

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

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

Save the configuration file. If you wish, you can now safely delete the extracted Luna Cloud HSM service client directory.

- Manually reset the **ChrystokiConfigurationPath** environment variable back to the location of the original configuration file.
  - [Windows] In the Control Panel, search for "environment" and select **Edit the system environment variables**. Click **Environment Variables**. In both the list boxes for the current user and system variables, edit **ChrystokiConfigurationPath** to point to the **crystoki.ini** file in the original client install directory.

- [Linux] Either open a new shell session, or reset the environment variable for the current session to the location of the original **Chrystoki.conf** file:  
**# export ChrystokiConfigurationPath=/etc/**

8. Launch or relaunch LunaCM to verify that both your Luna partitions and Luna Cloud HSM service are available.

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

- > ["Initializing an Application Partition" on page 268](#)
- > ["The following procedures will allow you to initialize the Crypto Officer \(CO\) and Crypto User \(CU\) roles and set an initial credential. " on page 295](#)

Refer to ["Cloning Keys Between Luna 6, Luna 7, and Luna Cloud HSM" on page 171](#) 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" on page 170](#)
- > ["Backup and Restore Using a Luna Backup HSM \(G5\) " on page 379](#)
- > ["Backup and Restore Using a Luna Backup HSM \(G7\)" on page 408](#)
- > ["Setting Up an HA Group" on page 350](#)

## Configuration File Summary

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

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

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

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

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

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

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

For Windows operations, the k7 driver cannot be signed when secure boot is enabled. The host machine will not allow functionality.

| Section/Setting                      | Description                                                                                                                                                                                                                                                                                                                                                                       |
|--------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Chrystoki2</b>                    |                                                                                                                                                                                                                                                                                                                                                                                   |
| LibNT                                | Path to the Chrystoki2 library on Windows operating systems.<br><b>Default: C:\Program Files\SafeNet\LunaClient\cryptoki.dll</b>                                                                                                                                                                                                                                                  |
| LibNT32                              | Path to the Chrystoki2 library on 32-bit Windows systems only.<br><b>Default: C:\Program Files\SafeNet\LunaClient\win32\libCryptoki2.dll</b><br><br><b>NOTE</b> Luna HSM Client 10.1 and newer includes libraries for 64-bit operating systems only.                                                                                                                              |
| LibUNIX64                            | Path to the Chrystoki2 library on 64-bit Linux/UNIX operating systems.<br><b>Default:</b><br>> <b>Linux/AIX: /usr/safenet/lunaclient/libs/64/libCryptoki2_64.so</b><br>> <b>Solaris: /opt/safenet/lunaclient/libs/64/libCryptoki2_64.so</b>                                                                                                                                       |
| <b>Luna (see * below this table)</b> |                                                                                                                                                                                                                                                                                                                                                                                   |
| CloningCommandTimeout                | The amount of time (in milliseconds) the library allows for the HSM to respond to a cloning command.<br><b>Default: 300000</b>                                                                                                                                                                                                                                                    |
| CommandTimeoutPedSet                 | This is an exception to DefaultTimeout (below). It defines the time (in milliseconds) allowed for all PED-related HSM commands. PED-related commands can take longer than ordinary commands governed by DefaultTimeOut.<br>Generally, the following formula applies:<br>CommandTimeOutPedSet = DefaultTimeOut + PEDTimeout1 + PEDTimeout2 + PEDTimeout3<br><b>Default: 720000</b> |

| Section/Setting    | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|--------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 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>                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| 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 <code>PEDTimeout2</code>, the HSM returns an appropriate result code (such as <code>PED_TIMEOUT</code>). 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 <code>PEDTimeout2 + PEDTimeout3</code>.</p> <p><b>Default: 20000</b></p>                                                                                                                                                                                                                                                                                          |
| <b>CardReader</b>  |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |



| Section/Setting                                                                                                                         | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|-----------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 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 (G5)s 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> |
| LunaG7Slots                                                                                                                             | <p>Number of Luna G7 Backup HSM slots reserved so that the library will check for connected devices.</p> <p><b>Valid Values:</b></p> <ul style="list-style-type: none"> <li>&gt; <b>0:</b> If you have no Luna G7 Backup HSMs and wish to eliminate the reserved spaces in your slot list, use this setting.</li> <li>&gt; <b>1-N:</b> Can be set to any number, but is effectively limited by the number of external USB devices supported by your client workstation.</li> </ul> <p><b>Default: 3</b></p>     |
| RemoteCommand                                                                                                                           | <p>This setting was used when debugging older 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" on page 1</a>. Config is done via vtl utility or by editing this config file directly.</p> |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| <b>RBS</b>                                                                                                                              | <b>NOTE</b> RBS is not supported with Luna Cloud HSM services.                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| CmdProcessor                                                                                                                            | <p>The location of the RBS library.</p> <p><b>Default:</b></p> <ul style="list-style-type: none"> <li>&gt; <b>Windows:</b> C:\Program Files\SafeNet\LunaClient\rbs_processor2.dll</li> <li>&gt; <b>Linux/AIX:</b> /usr/safenet/lunaclient/rbs/lib/librbs_processor2.dll</li> <li>&gt; <b>Solaris:</b> /opt/safenet/lunaclient/rbs/lib/librbs_processor2.dll</li> </ul>                                                                                                                                          |
| HostPort                                                                                                                                | <p>The port number used by the RBS server.</p> <p><b>Valid Values:</b> any unassigned port</p> <p><b>Default: 1792</b></p>                                                                                                                                                                                                                                                                                                                                                                                      |

| Section/Setting      | Description                                                                                                                                                                                                                                                                                                      |
|----------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ClientAuthFile       | The location of the RBS Client authentication file.<br><b>Default:</b><br>> <b>Windows:</b> C:\Program Files\SafeNet\LunaClient\config\clientauth.dat<br>> <b>Linux/AIX:</b> /usr/safenet/lunaclient/rbs/clientauth.dat<br>> <b>Solaris:</b> /opt/safenet/lunaclient/rbs/clientauth.dat                          |
| ServerSSLConfigFile  | The location of the OpenSSL configuration file used by RBS Server or Client.<br><b>Default:</b><br>> <b>Windows:</b> C:\Program Files\SafeNet\LunaClient\rbs\server.cnf<br>> <b>Linux/AIX:</b> /usr/safenet/lunaclient/rbs/server/server.cnf<br>> <b>Solaris:</b> /opt/safenet/lunaclient/rbs/server/server.cnf  |
| ServerPrivKeyFile    | The location of the RBS Server certificate private key file.<br><b>Default:</b><br>> <b>Windows:</b> C:\Program Files\SafeNet\LunaClient\cert\server\serverkey.pem<br>> <b>Linux/AIX:</b> /usr/safenet/lunaclient/rbs/server/serverkey.pem<br>> <b>Solaris:</b> /opt/safenet/lunaclient/rbs/server/serverkey.pem |
| ServerCertFile       | The location of the RBS Server certificate file.<br><b>Default:</b><br>> <b>Windows:</b> C:\Program Files\SafeNet\LunaClient\cert\server\server.pem<br>> <b>Linux/AIX:</b> /usr/safenet/lunaclient/rbs/server/server.pem<br>> <b>Solaris:</b> /opt/safenet/lunaclient/rbs/server/server.pem                      |
| NetServer            | Determines whether RBS acts as a server or client.<br><b>Valid Values:</b><br>> <b>0:</b> Client<br>> <b>1 (default):</b> Server                                                                                                                                                                                 |
| HostName             | The hostname or IP address that the RBS server will listen on.<br><b>Valid Value:</b> any hostname or IP address<br><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.<br><b>Default:</b> 20000                                                                                                                                                                                                                                          |

| Section/Setting   | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|-------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| SSLConfigFile     | <p>Location of the OpenSSL configuration file.</p> <p><b>Default:</b></p> <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 | <p>Location of the client private key. This value is set by <b>vti</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\client\<clientname&gt;key.pem< li=""> <li>&gt; <b>Linux/AIX:</b> /usr/safenet/lunaclient/cert/client/&lt;ClientName&gt;Key.pem</li> <li>&gt; <b>Solaris:</b> /opt/safenet/lunaclient/cert/client/&lt;ClientName&gt;Key.pem</li> </clientname&gt;key.pem<></li></ul>                                                   |
| ClientCertFile    | <p>Location of the client certificate that is uploaded to Luna Network HSM for NTLS. This value is set by <b>vti</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\client\<clientname&gt;cert.pem< li=""> <li>&gt; <b>Linux/AIX:</b> /usr/safenet/lunaclient/cert/client/&lt;ClientName&gt;Cert.pem</li> <li>&gt; <b>Solaris:</b> /opt/safenet/lunaclient/cert/client/&lt;ClientName&gt;Cert.pem</li> </clientname&gt;cert.pem<></li></ul> |
| ServerCAFile      | <p>Location of the server certificate file on the client workstation. This value is set by <b>vti</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>                                                                                                                                                                                                                                                                                 |

| Section/Setting     | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|---------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| TCPKeepAlive        | <p>TCPKeepAlive is a TCP stack option, available at the Luna HSM Client and the Luna Network HSM appliance. It is controlled via an entry in the Luna HSM Client configuration file, and an equivalent file on the Luna Network HSM.</p> <p>On the Luna Network HSM appliance, where you do not have direct access to the file system, the TCPKeepAlive= setting is controlled by lunash:&gt; <a href="#">ntls tcp_keeplive set</a>.</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</b> (default): true</li> </ul>                                                                                |
| ServerName##        | <p>These entries identify NTLS-linked Luna Network HSM servers/ports, and determines the order in which they are polled to create a slot list. These values are set by <a href="#">vtl</a> or lunacm:&gt; <a href="#">clientconfig deploy</a>.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| ServerPort##        |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| <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 HSMs 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 style="border: 1px solid black; padding: 5px; margin-top: 10px;"> <p><b>NOTE</b> This does not apply to Luna Network HSM 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 or HA virtual partitions. If you use this setting, you must specify a slot for all partitions on a specific HSM, or the partitions not listed here will not be visible to the client.</p> <p><b>Valid Values:</b> Comma-delimited list in the format &lt;slotnum&gt;(&lt;serialnum&gt;)</p> <p><b>Example:</b><br/> <b>ShowUserSlots=1(351970018022),2(351970018021),3(351970018020),...</b></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>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| 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: 5px; margin-top: 10px;"> <p><b>NOTE</b> This setting does not affect how slots are numbered in LunaCM; you can still configure individual member partitions with HAOnly mode enabled.</p> </div> |
| reconnAtt              | <p>Specifies the number of reconnection attempts the client makes to a missing HA member. Once this number is reached, you must manually reconnect the member when it becomes available (see <a href="#">"Manually Recovering a Failed HA Group Member"</a> on page 366).</p> <p>This value is set using lunacm:&gt; <a href="#">hagroup retry</a>.</p> <p><b>Valid Values:</b></p> <ul style="list-style-type: none"> <li>&gt; <b>-1:</b> Perform infinite reconnection attempts.</li> <li>&gt; <b>0:</b> Disable HA auto-recovery.</li> <li>&gt; <b>1-500:</b> Perform the specified number of reconnection attempts.</li> </ul>                                                                                                                                                                                                                                                                                                               |
| <b>Misc</b>            |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |

| Section/Setting                            | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|--------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Appld = <xxx>                              | <p>Application IDs are generated when the application starts, and are 16 bytes for Luna firmware 7.7.0 and compatible client software. Application IDs are not supported for Luna Cloud HSM services. For earlier HSM firmware or clients, see "<a href="#">Application IDs</a>" on page 1. You can override this functionality and specify an Appld if desired.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| CopyRSAPublicValues<br>FromPrivateTemplate | <p>Controls whether the public exponent of an RSA key can be copied from the private key template, if the public key template does not already have a public exponent attribute set.</p> <p><b>Valid Values:</b></p> <ul style="list-style-type: none"> <li>&gt; <b>0</b>: if no public exponent is provided in the public template, an error is returned (expected behavior).</li> <li>&gt; <b>1</b>(default): if no public exponent is provided in the public template, the private exponent is copied from the private template to populate the public template.</li> </ul> <p>For PKCS#11 compliance, this should be set to <b>0</b>.</p> <div style="border: 1px solid black; padding: 5px; margin-top: 10px;"> <p><b>NOTE</b> This functionality requires Luna HSM Client 7.1.0 or newer.</p> </div> |
| FunctionBindLevel                          | <p>Determines what action to take if a function binding fails during a CryptokiConnect() operation.</p> <p><b>Valid Values:</b></p> <ul style="list-style-type: none"> <li>&gt; <b>0</b> (default): fail if not all functions can be resolved</li> <li>&gt; <b>1</b>: do not fail but issue warning for each function not resolved</li> <li>&gt; <b>2</b>: do not fail and do not issue warning (silent mode)</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                   |
| LoginAllowedOn<br>FMEnabledHSMs            | <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>                                                                                                                |

| 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. This must be set to <b>0</b> to use Luna 6 partitions in a mixed-version HA group (see "<a href="#">Cloning Keys Between Luna 6, Luna 7, and Luna Cloud HSM</a>" on <a href="#">page 171</a>).</p> <p><b>Valid Values:</b></p> <ul style="list-style-type: none"> <li>&gt; <b>0</b>: SafeXcel co-processor is disabled on Luna 6 HSMs.</li> <li>&gt; <b>1</b> (default): SafeXcel co-processor is enabled on Luna 6 HSMs.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                            |
| 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</b> (default): no challenge request</li> <li>&gt; <b>1</b>: check for Crypto Officer challenge request</li> <li>&gt; <b>2</b>: check for Crypto User challenge request</li> </ul> <div style="border: 1px solid black; padding: 5px; margin-top: 10px;"> <p><b>NOTE</b> This functionality requires Luna HSM Client 7.1.0 or newer.</p> </div>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| RSAKeyGenMechRemap                    | <p>This entry remaps calls to certain older mechanisms, no longer supported on the latest firmware, to use newer, more secure mechanisms instead.</p> <ul style="list-style-type: none"> <li>&gt; <b>0</b>: No re-mapping is performed.</li> <li>&gt; <b>1</b>: The following re-mapping occurs: <ul style="list-style-type: none"> <li>• PKCS Key Gen -&gt; 186-3 Prime key gen</li> <li>• X9.31 Key Gen -&gt; 186-3 Aux Prime key gen (see <a href="#">Mechanism Remap for FIPS Compliance</a>)</li> </ul> </li> </ul> <div style="border: 1px solid black; padding: 5px; margin-top: 10px;"> <p><b>NOTE</b> Mechanism remapping is automatic, and ignores the configuration file entry:</p> <ul style="list-style-type: none"> <li>• if you are using Luna HSM Client 10.1 or newer, and</li> <li>• HSM firmware is earlier than version 7.7.1 (which introduced the ability for a partition to be FIPS-mode when the HSM is non-FIPS; clients up to, and including, 10.3.0 are unaware of the independent partition setting and do not remap mechanisms).</li> </ul> </div> |

| Section/Setting               | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|-------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| RSAPre1863KeyGen<br>MechRemap | <p>This entry remaps calls to newer mechanisms, when they are not available on older firmware, to use older mechanisms instead. Intended for evaluation purposes, such as with existing integrations that require newer mechanisms, before you update to firmware that actually supports the more secure mechanisms. Be careful with this setting, which makes it appear you are using a new, secure mechanism, when really you are using an outdated, insecure mechanism (see <a href="#">Mechanism Remap for FIPS Compliance</a>).</p> <ul style="list-style-type: none"> <li>&gt; <b>0:</b> No re-mapping is performed.</li> <li>&gt; <b>1:</b> The following re-mapping occurs if the HSM firmware permits: <ul style="list-style-type: none"> <li>• 186-3 Prime key gen -&gt; PKCS Key Gen</li> <li>• 186-3 Aux Prime key gen -&gt; X9.31 Key Gen</li> </ul> </li> </ul> <div style="border: 1px solid black; padding: 5px; margin-top: 10px;"> <p><b>NOTE</b> Mechanism remapping is automatic, and ignores the configuration file entry:</p> <ul style="list-style-type: none"> <li>• if you are using Luna HSM Client 10.1 or newer, and</li> <li>• HSM firmware is earlier than version 7.7.1 (which introduced the ability for a partition to be FIPS-mode when the HSM is non-FIPS; clients up to, and including, 10.3.0 are unaware of the independent partition setting and do not remap mechanisms).</li> </ul> </div> |
| ToolsDir                      | <p>The location of the Luna HSM Client tools.</p> <p><b>Default:</b></p> <ul style="list-style-type: none"> <li>&gt; <b>Windows:</b> C:\Program Files\SafeNet\LunaClient\</li> <li>&gt; <b>Linux/AIX:</b> /usr/safenet/lunaclient/bin/</li> <li>&gt; <b>Solaris:</b> /opt/safenet/lunaclient/bin/</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| 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>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| ClientIdentitiesDir           | <p>Specifies the directory used to store the STC client identity.</p> <p><b>Default:</b></p> <ul style="list-style-type: none"> <li>&gt; <b>Windows:</b> C:\Program Files\SafeNet\LunaClient\data\client_identities</li> <li>&gt; <b>Linux/AIX:</b> /usr/safenet/lunaclient/data/client_identities</li> <li>&gt; <b>Solaris:</b> /opt/safenet/lunaclient/data/client_identities</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |



| Section/Setting                                  | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|--------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ClientTokenLib<br>(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<br>(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: C:\Windows\SysWOW64\etoken.dll</b></p> <div style="border: 1px solid black; padding: 5px; margin-top: 10px;"> <p><b>NOTE</b> Luna HSM Client 10.1 and newer includes libraries for 64-bit operating systems only.</p> </div> |
| PartitionIdentitiesDir                           | <p>Specifies the directory used to store the STC partition identities exported using lunacm:&gt; <a href="#">stcconfig partitionidexport</a>.</p> <p><b>Default:</b></p> <ul style="list-style-type: none"> <li>&gt; <b>Windows: C:\Program Files\SafeNet\LunaClient\data\partition_identities</b></li> <li>&gt; <b>Linux/AIX: /usr/safenet/lunaclient/data/partition_identities</b></li> <li>&gt; <b>Solaris: /opt/safenet/lunaclient/data/partition_identities</b></li> </ul>                                                                                                                                                                                                                                                                                                     |
| SoftTokenDir                                     | <p>Specifies the location where the STC client soft token (<b>token.db</b>) is stored.</p> <p><b>Default:</b></p> <ul style="list-style-type: none"> <li>&gt; <b>Windows: C:\Program Files\SafeNet\LunaClient\softtoken\001\</b></li> <li>&gt; <b>Linux/AIX: /usr/safenet/lunaclient/softtoken/001/</b></li> <li>&gt; <b>Solaris: /opt/safenet/lunaclient/softtoken/001/</b></li> </ul>                                                                                                                                                                                                                                                                                                                                                                                             |
| <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>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |

| Section/Setting     | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|---------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 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 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 and your client application does proper housekeeping, or if your application is connecting via NTLS to a Luna Network HSM.</li> </ul>                                                                                                                                |
| <b>Toggles</b>      | <p><b>NOTE</b> This section is not created automatically. To change any of the following values, you must first create this section in the configuration file.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| legacy_memory_rep = | <p>Controls the manner in which the HSM reports the available RAM space.</p> <p><b>Valid Values:</b></p> <ul style="list-style-type: none"> <li>&gt; <b>0</b> (default): the public and private memory total/free values reported in the CK_TOKEN_INFO structure indicate the available flash memory for permanent (TOKEN) objects that are in either the public or private space respectively; this method is PKCS#11 compliant.</li> <li>&gt; <b>1</b>: the public memory values indicate the total/free RAM memory; this non-standard legacy method was used by some customers to determine space available for session based objects, and must be explicitly selected in order to continue using the legacy method.</li> </ul> <p><b>NOTE</b> This functionality requires minimum firmware version 7.1.0.</p> |
| lunacm_cv_ha_ui =   | <p>Controls whether Thales DPoD Luna Cloud HSM services can be active members of an HA group.</p> <p><b>Valid Values:</b></p> <ul style="list-style-type: none"> <li>&gt; <b>0</b>: 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> <p><b>NOTE</b> This functionality requires Luna HSM Client 10.1 or newer.</p>                                                                                                                                                                                                                                                            |
| <b>REST</b>         | <p><b>NOTE</b> This section is not created automatically for clients obtained from the Thales Support Portal. For such clients, this section must be copied from a Luna Cloud HSM service client configuration file (see <a href="#">"Adding a Luna Cloud HSM Service" on page 68</a>). This section governs Luna Cloud HSM service functionality only and is not related to the Luna REST API. This functionality requires Luna HSM Client 10.1 or newer.</p>                                                                                                                                                                                                                                                                                                                                                    |

| Section/Setting         | Description                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|-------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ClientConnectIntervalMs | Interval in milliseconds between client connection attempts.<br><b>Default: 1000</b>                                                                                                                                                                                                                                                                                                                                                                      |
| ClientConnectRetryCount | Maximum connection attempts between the client and a Luna Cloud HSM service.<br><b>Default: 900</b>                                                                                                                                                                                                                                                                                                                                                       |
| ClientEofRetryCount     | Maximum command retries.<br><b>Default: 15</b>                                                                                                                                                                                                                                                                                                                                                                                                            |
| ClientPoolSize          | Number of threads in the thread pool available for client operations. This entry does not apply to Luna HSM Client 10.2 and newer – the pool size for these clients is always <b>64</b> . If the number of parallel connections is more than 64, old connections are closed to make space in the cache.<br><b>Default: 32</b>                                                                                                                             |
| ClientTimeoutSec        | Time (in seconds) that the client waits for a response from a Luna Cloud HSM service. This timeout applies to each retry attempt individually.<br><b>Default: 120</b><br><br><div style="border: 1px solid #ccc; padding: 5px; margin-top: 10px;"> <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> |
| CurlLogsEnabled         | Enables libcurl logging. This variable applies to Luna HSM Client 10.3.0 and newer.<br><b>Valid Values:</b><br><ul style="list-style-type: none"> <li>&gt; <b>0</b>: Libcurl logging is disabled.</li> <li>&gt; <b>1</b> (default): Libcurl logging is enabled.</li> </ul>                                                                                                                                                                                |
| CVAppSpecificData       | String containing identifying information about your Luna Cloud HSM service.                                                                                                                                                                                                                                                                                                                                                                              |
| RestClient              | Indicates that Luna HSM Client and associated tools are acting as REST clients.                                                                                                                                                                                                                                                                                                                                                                           |
| ServerName              | The name of the Luna Cloud HSM service server providing Luna Cloud HSM services. For Luna HSM Client version 10.2 and newer.                                                                                                                                                                                                                                                                                                                              |
| ServerPort              | The port used for Luna Cloud HSM service server traffic. For Luna HSM Client version 10.2 and newer.                                                                                                                                                                                                                                                                                                                                                      |
| SSLClientSideVerifyFile | Location of the Luna Cloud HSM service server certificate chain file ( <b>server-certificate.pem</b> ). This parameter applies to Luna HSM Client versions 10.1 and older. .                                                                                                                                                                                                                                                                              |

| Section/Setting      | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|----------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>XTC</b>           | <b>NOTE</b> This section is not created automatically for clients obtained from the Thales Support Portal. For such clients, this section must be copied from a Luna Cloud HSM service client configuration file (see " <a href="#">Adding a Luna Cloud HSM Service</a> " on page 68). This functionality requires Luna HSM Client 10.1 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.<br><b>Valid Values:</b><br>> <b>0</b> : XTC is disabled.<br>> <b>1</b> (default): XTC is enabled.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| PartitionCAPath      | Location of the Luna Cloud HSM service partition origin certificate ( <b>partition-ca-certificate.pem</b> ) for clients version 10.1 and older.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| PartitionCertPath00  | Location of the Luna Cloud HSM service partition messaging certificate ( <b>partition-certificate.pem</b> ) for clients version 10.1 and older.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| TimeoutSec           | Time (in seconds) before a cryptographic request expires. Timestamps are included in XTC headers, and the HSM rejects messages which have expired.<br><b>Valid Values: 1-600</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| <b>GemEngine</b>     | <b>NOTE</b> This section is not created automatically.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| DisableCheckFinalize | 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.<br><b>Valid Values:</b><br>> <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.<br>> <b>1</b> : Perform post-fork checking – the engine initializes the cryptoki library and maintains the connection to the HSM until the application terminates.<br><br>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. [ LUNA-22762 waiting for review and approval to remove NOTE condition and publish to thalesdocs.com ]<br><br>Not used for Windows. |

\* 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.

## 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 17).

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** We recommend verifying the integrity of the Universal 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 2: Client-Partition Connections

To allow clients to perform cryptographic operations, you must first give them access to an application partition on the HSM. This section contains the following information about client-partition connections:

- > ["Comparing NTLS and STC" below](#)
- > ["Creating an NTLS Connection Using Self-Signed Certificates" on page 92](#)
- > ["Creating an NTLS Connection Using a Self-Signed Appliance Certificate and a Client Certificate Signed by a Trusted Certificate Authority" on page 96](#)
- > ["Creating an NTLS Connection Using Certificates Signed by a Trusted Certificate Authority" on page 99](#)
- > ["Assigning or Revoking NTLS Client Access to a Partition" on page 103](#)
- > ["Creating an STC Connection" on page 104](#)
- > ["Connecting an Initialized STC Partition to Multiple Clients" on page 109](#)
- > ["Converting Initialized NTLS Partitions to STC" on page 113](#)
- > ["Using the STC Admin Channel" on page 115](#)
- > ["Configuring STC Identities and Settings" on page 117](#)
- > ["Restoring Broken NTLS or STC Connections" on page 121](#)

### Comparing NTLS and STC

---

Client access to the Luna Network HSM is provided via two different types of channel:

- > ["Network Trust Link Service" on the next page](#)
- > ["Secure Trusted Channel" on page 89](#)

| NTLS                                                                                                                                                                                                                                                                                                                                                           | STC                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <ul style="list-style-type: none"> <li>&gt; Ideally suited for high-performance applications and environments, executing many cryptographic operations per second.</li> <li>&gt; Best used in traditional data center environments, where the client can be identified by its IP address or hostname; not recommended for use with public networks.</li> </ul> | <ul style="list-style-type: none"> <li>&gt; Suited for higher-assurance applications requiring session protection beyond TLS; STC's message integrity and optional additional layer of encryption offers additional protection of client-to-HSM communications</li> <li>&gt; Best for virtual and cloud environments where virtual machines are frequently cloned, launched, and stopped—such as when virtual machine auto-scaling is implemented to meet service-level agreements</li> <li>&gt; Preferred in "HSM as a Service" environments where multiple customers, departments, or groups access partitions on a common HSM and want communication to be terminated on the Luna HSM card within the appliance</li> <li>&gt; Suited for applications with moderate performance requirements</li> </ul> |

## Network Trust Link Service

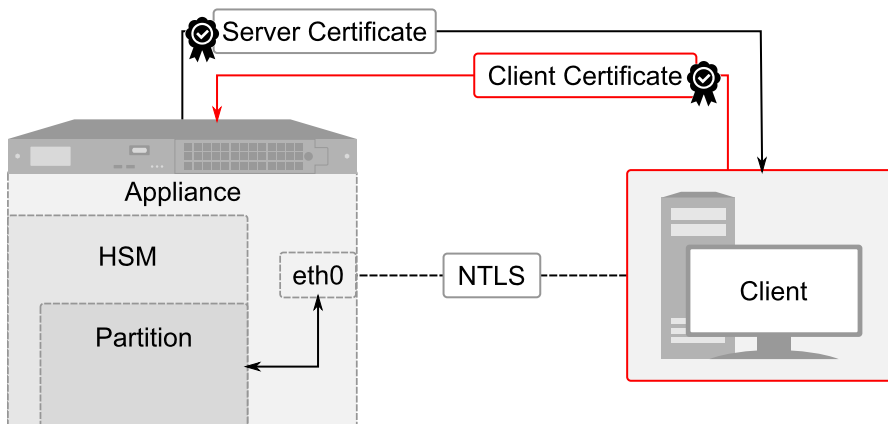
A Network Trust Link is a secure, authenticated network connection between the Luna Network HSM appliance and a client computer. NTLS uses two-way digital certificate authentication and TLS data encryption to protect your sensitive data during all communications between HSM partitions on the appliance and its clients.

The Luna Network HSM appliance can support up to 800 simultaneous NTLS connections.

The certificates that identify appliances and clients can be self-signed or signed by a trusted Certificate Authority (CA).

### NTLS Authenticated by Self-Signed Certificates

The figure below shows how a secure NTLS connection is created using self-signed certificates exchanged between the client and the appliance.



Self-signed certificates are created on both the appliance and the client. These certificates are exchanged to register the appliance and client with each other. Once registered, the client can access any partitions assigned to it in LunaSH. NTLS encrypts data between the network interfaces of the appliance (eth0 above) and client, but not between the network interface and the HSM within the appliance.

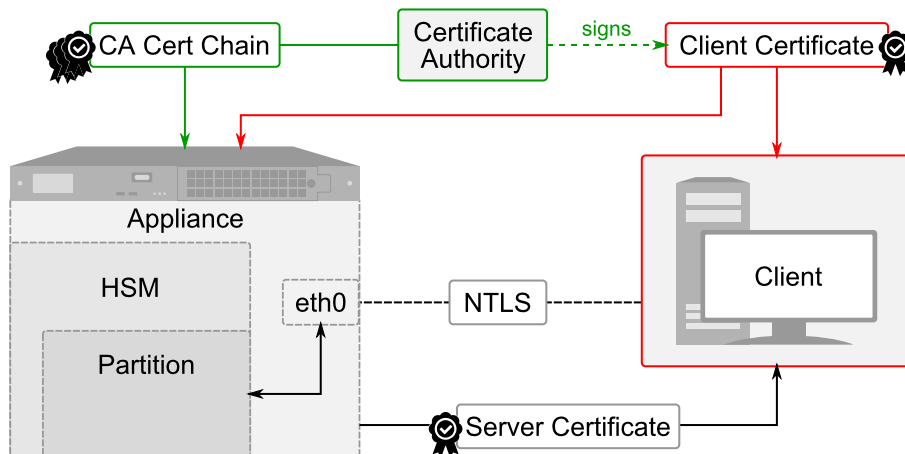
There are two methods of assigning partitions to a client via a self-signed NTLS connection:

- > A multi-step procedure, performed by the appliance administrator and a client administrator
- > A single-step procedure that automates the manual process. It can be used when the client administrator has **admin**-level access to the appliance, or through a custom registration account (see [Creating a One-Step NTLS Registration Role](#)).

See "[Creating an NTLS Connection Using Self-Signed Certificates](#)" on page 92.

### NTLS Authenticated by a Certificate Authority on the Client Side Only

The figure below shows how a secure NTLS connection is created using a self-signed appliance certificate and a client certificate signed by a trusted CA. This can be a commercial third-party CA or your organization's own signing station. This method requires Luna HSM Client 10.1.0 or newer.



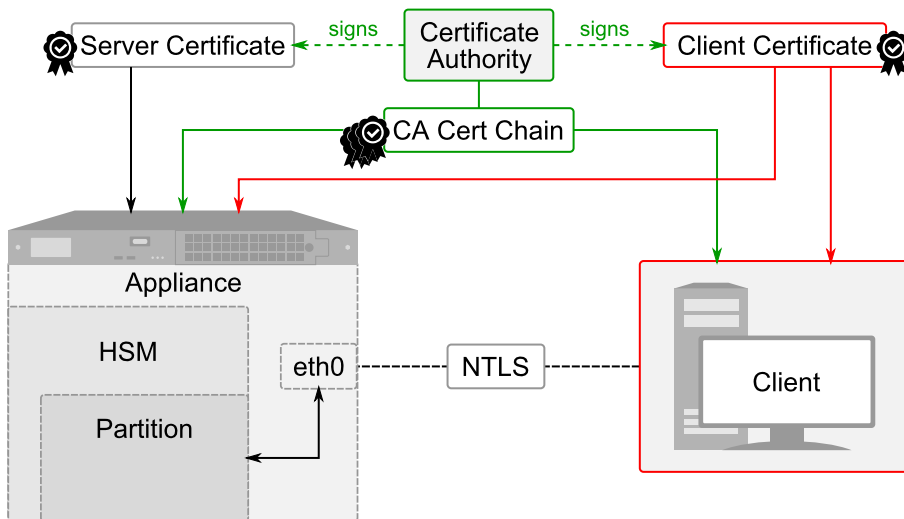
A Certificate Signing Request (CSR) is created on the client; this is an unsigned certificate that must be signed by your trusted Certificate Authority. The signed certificate is installed on the client, and the CA certificate chain is added to the trust store on the appliance. Finally, the client certificate is registered on the appliance and the client is then able to access any partitions that are assigned to it.

See "[Creating an NTLS Connection Using a Self-Signed Appliance Certificate and a Client Certificate Signed by a Trusted Certificate Authority](#)" on page 96.

### NTLS Authenticated by a Certificate Authority

The figure below shows how a secure NTLS connection is created using client and server certificates signed by a trusted Certificate Authority (CA). This can be a commercial third-party CA or your organization's own signing station. This method requires minimum Luna HSM Client 10.1.0 and Luna Network HSM appliance software 7.7.0.





A Certificate Signing Request (CSR) is created on the appliance, the client, or both—this is an unsigned certificate that must be signed by your trusted Certificate Authority. Each signed certificate is installed on its respective appliance/client, and the CA certificate chain is added to both trust stores. Finally, the client certificate is registered on the appliance and the client is then able to access any partitions that are assigned to it.

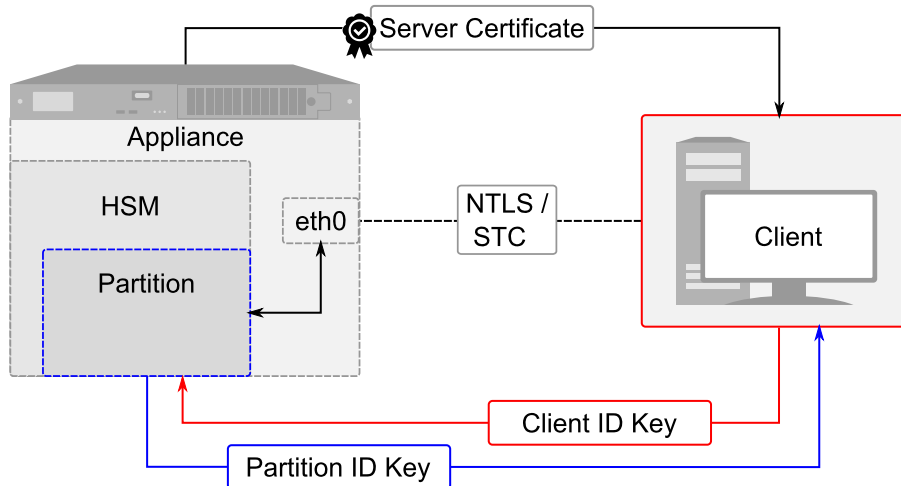
See ["Creating an NTLS Connection Using Certificates Signed by a Trusted Certificate Authority"](#) on page 99.

## Secure Trusted Channel

If you require a higher level of security for your network links than is offered by NTLS, such as in cloud environments, or in situations where message integrity is paramount, you can use Secure Trusted Channel (STC) to provide very secure client-partition links, even over unsecured networks. STC offers the following features to ensure the security and integrity of your client-partition communications:

- > All data is transmitted using symmetric encryption; only the end-points can decrypt messages
- > Message authentication codes prevent an attacker from intercepting and modifying any command or response
- > Mutual authentication of the HSM and the end-point ensure that only authorized entities can establish an STC connection

The figure below shows how an STC connection is made between the client and an application partition.



See the following procedures:

- > ["Creating an STC Connection" on page 104](#)
- > ["Connecting an Initialized STC Partition to Multiple Clients" on page 109](#)
- > ["Converting Initialized NTLS Partitions to STC" on page 113](#)

### Secure Tunnel Creation

Each STC connection is established between a client application and a specific partition on the HSM. As such, each application and partition pair goes through STC tunnel establishment individually. Before STC can create secure tunnels, trust must be established between the client and the partition through the manual exchange of public keys. Once trust has been established, unique session keys are created for each STC connection.

### Session Re-Negotiation

Session keys for the tunnel are periodically renegotiated, as specified by the STC rekey threshold set for a partition. The rekey threshold specifies the number of API calls, or messages, that can be transmitted over an STC link to the partition before the session keys are renegotiated. You can adjust this value based on your application use cases and security requirements. See ["Configuring STC Identities and Settings" on page 117](#) for more information.

### Abnormal Termination

When a client shuts down a connection under normal conditions, it sends a secured message informing the HSM that the connection can be terminated. If a client terminates abnormally, or the network link is lost, the STC Daemon (STCD) detects the abnormal termination, and sends a message to the HSM informing it that the connection has ended, and the connection is closed. If the STCD sends an incorrect connection termination message, the client transparently re-establishes a new STC tunnel.

### Secure Message Transport

Once a secure tunnel is established, any messages sent over the STC link are encrypted and authenticated using the unique session keys created when the tunnel is established. In addition, as with NTLS, all STC links use the TLS protocol to secure the link when it traverses a network.

Messages traversing an STC link are protected using Symmetric Encryption and Message Integrity Verification. These features are configurable for each partition and are used for each STC link to that partition. See ["Configuring STC Identities and Settings" on page 117](#) for more information.

### All messages protected outside the HSM

When STC is fully enabled on an HSM, all sensitive communications are protected all the way into the HSM. That is, any messages exchanged between a client application and the HSM use STC encryption, authentication, and verification from the client interface to the HSM interface, regardless of whether those links traverse a network, or are internal to the appliance (LunaSH to HSM) or Luna HSM Client workstation (client to HSM). All STC links that use a network connection also have the same network protection as NTLS links, that is, they are wrapped using SSL.

In addition to the STC connection between client and partition, you can also configure an STC connection between the HSM SO partition and the local services running on the appliance. This is referred to as the STC Admin channel.

See ["Using the STC Admin Channel" on page 115](#).

### Configurable options

The security features offered by STC are configurable, allowing you to specify the level of security you require, and achieve the correct balance between security and performance. Client/partition STC link parameters are configured using LunaCM. LunaSH/partition STC link parameters are configured using LunaSH.

### Client and Partition Identities

The identity of a client or partition at an STC endpoint is defined by a 2048-bit RSA asymmetric public/private key pair, unique to each endpoint. Before you can establish an STC link, you must exchange public keys between the client and partition to establish trust.

The partition's private key is always kept in the HSM and is strongly associated with its partition. Only the partition security officer can retrieve the partition's public key for delivery to a client. Upon receipt, the client administrator can use the public key hash to confirm its authenticity, before registering it. You can register multiple partition public keys to a client.

By default, the client's identity pair is stored in a software token on the client's file system, protected by the operating system's access control systems. When using a software token, the client's private key can be moved or copied to another host and used – so any client that possesses this identity pair is considered the authentic client. This enables an elastic client model for many applications.

### Performance Consideration

STC introduces additional overhead to the communication channel. Depending on the application use case and cryptographic algorithms employed, this could have an impact on application performance.

## Client to HSM Security Best Practices

While the Luna HSM is very secure, it is not the only component in the overall system. The HSM's application partitions become useful when client applications can communicate with those partitions, however this expands the potential attack surface. Good practices can go a long way toward minimizing that exposure.

This section suggests areas where practical choices and consistency can enhance security without sacrificing operational convenience.

## Security around Password-authenticated systems

Two things must be secured: NTLS private key and partition password

### Securing the partition password

The partition password is needed when logging in, so the primary means of protecting the partition password is to protect the connection to the HSM via NTLS or STC. NTLS and STC certificates reside in a subdirectory of the Luna HSM Client directory, on every system that connects to an application partition on a Luna Network HSM.

To secure an enterprise connection to the HSM the following means are available:

- > use operating system controls/permissions on the client to prevent unauthorized users from accessing the key material
- > use network segregation/software-defined networking or subnetting to prevent unauthorized machines from accessing the network HSM at all
- > implement a full firewall security flow policy, to assist in preventing unauthorized network access, allowing only certain IP addresses and ports to be open to the network HSM
- > practice proper password hygiene, in the form of a key and partition password-rotation policy, to prevent over-exposure should an NTLS key and/or partition password be compromised.

### Securing the NTLS private key

To secure a PaaS\*/container connection to the HSM the following means are available:

- > make use of whatever vault/secret-store approach a given PaaS implementation provides but ensure that it is truly secure and not merely a pretense of "security"-by-obfuscation
- > avoid bundling NTLS keys or partition passwords in VM/container images, but instead use the aforementioned PaaS vault/secret
- > if the PaaS implementation provides some form of service mesh, then take advantage of it to further mitigate client private-key/partition-password vulnerability, as the service mesh would prevent an attacker from being able to use the key/password outside of the service mesh; this forces the attacker to use the exposed material in a more secure and monitored environment, where the attack could be outright prevented or at least detected much sooner.

(\*PaaS = Platform as a Service)

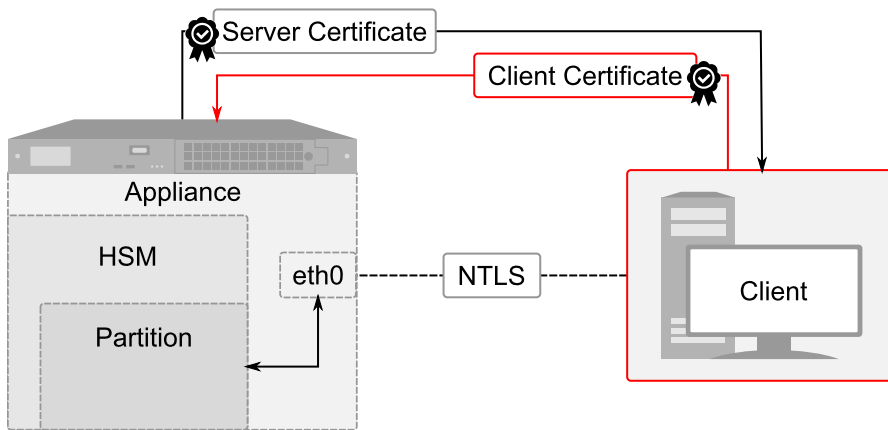
## Creating an NTLS Connection Using Self-Signed Certificates

To create an NTLS connection, the Luna Network HSM and the client must exchange certificates. Each registers the other's certificate in a trusted list. When both certificates are registered, the Network Trust Link is ready, and the appliance administrator can assign application partitions to the client for cryptographic operations. By default, this procedure uses self-signed certificates. To register your clients using certificates signed by a trusted Certificate Authority, see ["Creating an NTLS Connection Using a Self-Signed Appliance Certificate and a Client Certificate Signed by a Trusted Certificate Authority"](#) on page 96.

**NOTE** Secure Trusted Channel (STC) offers enhanced HSM-client message integrity, and an additional layer of protection for client-to-HSM communications, even over unsecured networks. To take advantage of this feature, see ["Creating an STC Connection" on page 104](#). For more on the differences between NTLS and STC connections, see ["Comparing NTLS and STC" on page 86](#).

There are two methods of assigning partitions to a client via a self-signed NTLS connection:

- > ["Multi-Step NTLS Connection Procedure" below](#): performed by the appliance administrator and a client administrator
- > ["One-Step NTLS Connection Procedure" on page 95](#): automates the multi-step process. It can be used when the client administrator has **admin**-level access to the appliance, or through a custom registration account.



## Multi-Step NTLS Connection Procedure

The multi-step procedure is performed by the appliance administrator and the client administrator.

### Prerequisites

- > You must have **admin**-level access to LunaSH on the appliance to register a client, or a custom account created to handle client registration (see [Creating a One-Step NTLS Registration Role](#)).
- > By default, you do not need to log in as HSM SO. You can force the appliance to require HSM SO login for this procedure with `lunash:> sysconf forcesologin enable`.
- > Luna HSM Client software must be installed on the client workstation (see ["Luna HSM Client Software Installation" on page 17](#) in the *Installation Guide*)
- > The client workstation must have an SSH client installed to provide secure shell access to the Luna Network HSM appliance. The PuTTY SSH client (**putty.exe**) is included in the Windows client installation.
- > Read/write access to the Luna HSM Client installation directory is required for the certificate exchange.
- > The client workstation must have network access to the Luna Network HSM appliance. The appliance auto-negotiates network bandwidth. See [Recommended Network Characteristics](#) for more information.

**NOTE** Administration commands can take a few seconds to be noted by NTLS. If you have added or deleted a client, wait a few seconds before connecting.

## To create a multi-step NTLS connection between the appliance and a client

1. On the client workstation, open a command prompt and navigate to the Luna HSM Client directory.

**NOTE** On Windows, ensure that you open a command prompt with Administrator privileges.

- Windows: **C:\Program Files\SafeNet\LunaClient**
  - Linux/AIX: **/usr/safenet/lunaclient/bin**
  - Solaris: **/opt/safenet/lunaclient/bin**
2. Use **pscp** or **scp** to import the HSM Appliance Server Certificate (**server.pem**) from the appliance to the client workstation. You require **admin**- or **operator**-level account access to complete this step. If you do not have SSL access to the appliance, or a firewall blocks file transfer over the network, the appliance **admin** must provide this certificate by other secure means.

**TIP** If you are importing certificates from multiple appliances to this client, rename each incoming certificate during the **pscp/scp** transfer. This will prevent you from accidentally overwriting one **server.pem** certificate with another.

```
pscp <user>@<host/IP>:server.pem <target_filename>
```

**NOTE** When using **pscp** or **scp** over an IPv6 network, enclose addresses in square brackets.

You must accept the SSH certificate the first time you open a **pscp/scp** or SSH link. You can check the SSH fingerprint in LunaSH to confirm the secure connection.

```
lunash:> sysconf fingerprint ssh
```

If the HSM appliance IP or hostname is changed, SSH detects a mismatch in the HSM appliance's server certification information and warns you of a potential security breach. To resolve this issue, delete the server's certificate information from the client's known host file at: `/<user home dir>/ssh/known_hosts2`, and re-import the server certificate.

3. Register the HSM Server Certificate with the client, using the **vtl** utility from the command line or shell prompt. If using a host name, ensure the name is reachable over the network (**ping <hostname>**). Thales recommends specifying an IP address to avoid network issues.

```
>vtl addServer -n <Network_HSM_hostname/IP> -c <server_certificate>
```

4. Create a certificate and private key for the client. If you specify a client hostname, it must match exactly the hostname reported by the **hostname** command.

**CAUTION!** If you are registering this client with multiple Luna Network HSM appliances, you only need to complete this step once. Use the same client certificate for all appliances. If you recreate the client certificate and key, any existing NTLS connections will be broken.

```
>vtl createCert -n <client_hostname/IP>
```

The certificate and private key are saved to the <client\_install\_dir>/cert/client directory and are named <client\_hostname/IP>.pem and <client\_hostname/IP>Key.pem, respectively. The command output displays the filepath.

5. Use **pscp** or **scp** to export the client certificate to the **admin** account (or an **admin**-level custom account) on the Network HSM appliance. The file arriving at the appliance is automatically placed in the appropriate directory. Do not specify a target directory.

```
pscp <cert_path/filename> admin@<host/IP>:[<target_filename>]
```

6. Connect to the appliance via SSH or a serial connection, and log in to LunaSH using an **admin**- or **operator**-level account (see [Logging In to LunaSH](#)).
7. Register the client certificate with the appliance, selecting a client name that can be used to easily identify the client. Specify either the **-hostname** or **-ip** option, according to which one you used to create the certificate.

```
lunash:> client register -client <client_name> {-hostname <client_hostname> | -ip <client_IP>}
```

8. [Optional] Verify the client registration.

```
lunash:> client list
```

Now that the NTLS connection is established, the Luna Network HSM appliance **admin** can assign partitions for the client to access (see ["Assigning or Revoking NTLS Client Access to a Partition" on page 103](#)).

## One-Step NTLS Connection Procedure

The Luna HSM Client provides a one-step NTLS setup option, which automates the multi-step procedure described above.

The One-Step NTLS procedure is performed by the client administrator, and requires SSL access to an **admin**-level account (or a specialized NTLS registration account) on the Luna Network HSM appliance. If you do not have SSL access to the appliance, an authorized user must provide the appliance certificate by other secure means, and you must use the multi-step procedure to manually register certificates.

This procedure uses **pscp/scp** to exchange certificates over the network. If a firewall prevents this file transfer, the procedure will fail. You must exchange the certificates by other secure means and perform the manual procedure.

One-Step NTLS can only be used to create a new NTLS connection, and not to assign additional partitions to the client. If an NTLS connection already exists between the client and the appliance, or if one has already registered the other's certificate, the operation fails.

### Luna Network HSM Prerequisites

- > The appliance certificate (**server.pem**) must be available on the appliance (see [Generating the HSM Server Certificate](#)).
- > An application partition must be available on the HSM (see [Creating or Deleting an Application Partition](#)).

- > The client must not have a certificate already registered on the appliance.

### Luna HSM Client Prerequisites

- > Client software must be installed (see ["Luna HSM Client Software Installation" on page 17](#)).
- > The client administrator must have access to an **admin**-level account, or a specialized NTLS registration account, on the appliance (see [Creating a One-Step NTLS Registration Role](#)).
- > The client administrator must know the name of an existing application partition that will be assigned to the client.
- > The appliance must not have a certificate already registered with the client.
- > For Linux 64-bit platforms only, ensure that **glibc.i686** is installed:

```
yum install glibc.i686
```

If you do not wish to install **glibc.i686**, use the ["Multi-Step NTLS Connection Procedure" on page 93](#) instead.

### To create a One-Step NTLS connection between the appliance and a client

1. Launch LunaCM on the client workstation.
2. Initiate the One-Step NTLS procedure by specifying the appliance and client hostnames/IPs, and the name of the application partition to assign to this client. By default, the request is sent to the **admin** account, but you can specify any other account.

```
lunacm:> clientconfig deploy -server <server_hostname/IP> -client <client hostname/IP> -partition <partition_name> [-user <appliance_username>][-password <password>][-verbose]
```

**NOTE** After you enter the account password, LunaCM appears to pause for 1-2 minutes while the registration procedure is completed. This is expected behavior.

The NTLS connection is now active, and the specified partition has been assigned to the client. If you want this client to have access to more partitions on this HSM, see ["Assigning or Revoking NTLS Client Access to a Partition" on page 103](#).

To initialize the application partition, see ["Initializing an Application Partition" on page 268](#).

To restore a broken NTLS client connection, see ["Restoring Broken NTLS or STC Connections" on page 121](#).

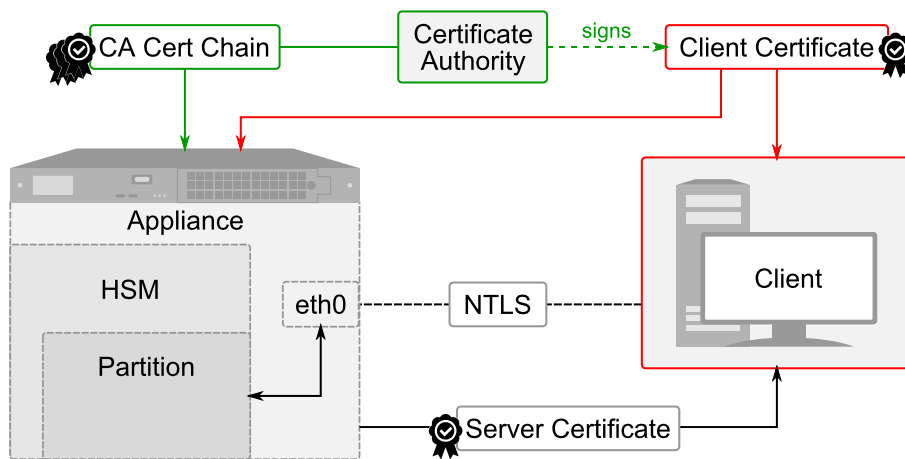
## Creating an NTLS Connection Using a Self-Signed Appliance Certificate and a Client Certificate Signed by a Trusted Certificate Authority

A trusted Certificate Authority (CA) can provide authentication for your NTLS connections. This can be a commercial third-party CA or your organization's own signing station. This type of connection is created in the following stages:

1. ["Registering the Appliance Certificate on the Client" on the next page](#)
2. ["Authenticating a Client Using a Trusted CA" on page 98](#)



### 3. "Registering the Client Certificate and CA Certificate Chain on the Appliance" on page 99



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

## Registering the Appliance Certificate on the Client

Use the following procedure to transfer the appliance's self-signed certificate to the client and register it.

### Prerequisites

- > You must have **admin**- or **operator**-level access to LunaSH on the appliance, or access to a custom LunaSH account.
- > You must have Administrator privileges on the client workstation.

### To register the appliance certificate to the client

1. Use **pscp** (Windows) or **scp** (Linux/UNIX) to import the HSM Appliance Server Certificate (**server.pem**) from the appliance to the client workstation. You require **admin**- or **operator**-level account access to complete this step. If you do not have SSL access to the appliance, or a firewall blocks file transfer over the network, the appliance **admin** must provide this certificate by other secure means.

**TIP** If you are importing certificates from multiple appliances to this client, rename each incoming certificate during the **pscp/scp** transfer. This will prevent you from accidentally overwriting one **server.pem** certificate with another.

```
pscp <user>@<host/IP>:server.pem <target_filename>
```

**NOTE** When using **pscp/scp** over an IPv6 network, enclose addresses in square brackets.

You must accept the SSH certificate the first time you open a **pscp/scp** or SSH link. You can check the SSH fingerprint in LunaSH to confirm the secure connection.

```
lunash:> sysconf fingerprint ssh
```

If the HSM appliance IP or hostname is changed, SSH detects a mismatch in the HSM appliance's server certification information and warns you of a potential security breach. To resolve this issue, delete the server's certificate information from the client's known host file at: `/<user home dir>/.ssh/known_hosts2`, and re-import the server certificate.

2. Register the HSM Server Certificate with the client, using the **vtl** utility from the command line or shell prompt. If using a host name, ensure the name is reachable over the network (**ping** <hostname>). Thales Group recommends specifying an IP address to avoid network issues.

```
>vtl addServer -n <Network_HSM_hostname/IP> -c <server_certificate>
```

## Authenticating a Client Using a Trusted CA

Use the following procedure to authenticate the client by having its certificate signed by your trusted CA.

### Prerequisites

- > You must have Administrator privileges on the client workstation.

### To authenticate a client using a certificate signed by a trusted CA

1. On the client workstation, open a command prompt and navigate to the Luna HSM Client directory.

**NOTE** On Windows, ensure that you open a command prompt with Administrator privileges.

- Windows: **C:\Program Files\SafeNet\LunaClient**
  - Linux/AIX: **/usr/safenet/lunaclient/bin**
  - Solaris: **/opt/safenet/lunaclient/bin**
2. Create a Certificate Signing Request (CSR) for the client—an unsigned certificate to be signed by a third-party Certificate Authority (CA). You must specify the client hostname or IP. You have the option to specify other information about the certificate.

**CAUTION!** Regenerating the client certificate will break any existing NTLS/STC connections.

```
> vtl createCSR -n <client_hostname/IP>
```

The certificate and private key are saved to the `<client_install_dir>/cert/client` directory and are named `<client_hostname/IP>CSR.pem` and `<client_hostname/IP>Key.pem`, respectively. The command output displays the filepath.

3. Submit the CSR file to be signed by your preferred or in-house Certificate Authority. You require the following artifacts from the CA:
  - Signed base64(PEM)-encoded client certificate in x509 format
  - The CA's base64(PEM)-encoded client certificate in x509 format, including the root certificate
4. Copy the signed client certificate to the following location in the Luna HSM Client directory:
  - Windows: **C:\Program Files\SafeNet\LunaClient\cert\client\**
  - Linux/AIX: **/usr/safenet/lunaclient/cert/client/**

- Solaris: `/opt/safenet/lunaclient/cert/client/`

## Registering the Client Certificate and CA Certificate Chain on the Appliance

Use the following procedure to register the client certificate on the appliance, and register the CA certificate chain so that the appliance can authenticate the client certificate.

### Prerequisites

- > You must have **admin**- or **operator**-level access to LunaSH on the Luna Network HSM appliance.
- > You require the signed base64(PEM)-encoded client certificate and the CA's base64-encoded certificate chain, including the root certificate, in x509 format.

**NOTE** All certificate chain files must be named for the certificate Common Name, with a **.pem** extension.

### To register the client certificate and CA certificate chain on the appliance

1. Transfer the client certificate and the CA certificate chain to the **admin** or **operator** user on the appliance (or the custom role that will perform the registration) using **pscp** or **scp**. The files arriving at the appliance are automatically placed in the appropriate directory. Do not specify a target directory.
2. Log in to LunaSH and register the client certificate with the appliance, selecting a client name that can be used to easily identify the client. Specify either the **-hostname** or **-ip** option, according to which one you used to create the certificate.

```
lunash:> client register -client <client_name> {-hostname <client_hostname> | -ip <client_IP>}
```

3. Register the CA certificate chain in the appliance trust store. Specify each certificate's filename, minus the **.pem** extension, using the **-hostname** option. Repeat this step until the entire certificate chain is registered.

```
lunash:> client register -client <cert_name> -hostname <cert_filename>
```

You can now assign partitions to the client (see "[Assigning or Revoking NTLS Client Access to a Partition](#)" on page 103).

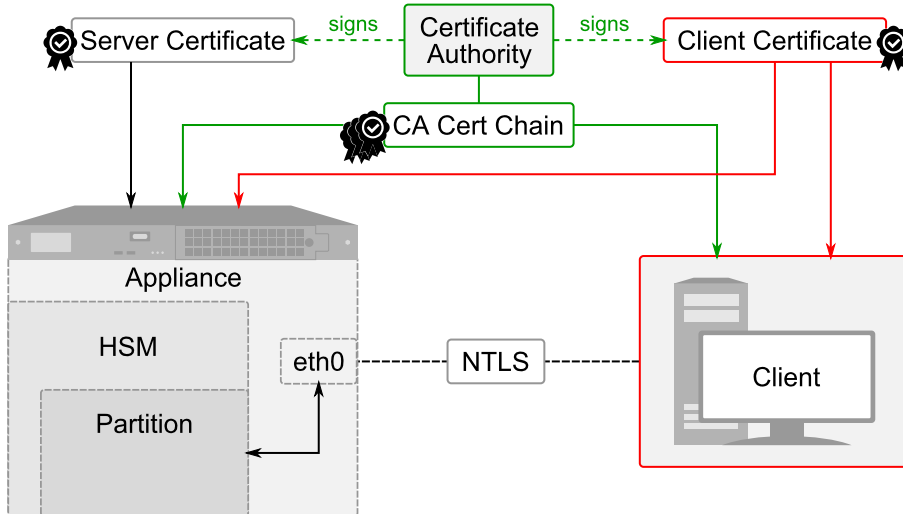
## Creating an NTLS Connection Using Certificates Signed by a Trusted Certificate Authority

A trusted Certificate Authority (CA) can provide authentication for your NTLS connections. This can be a commercial third-party CA or your organization's own signing station. This type of connection is created in the following stages:

1. "[Authenticating the Appliance Using a Trusted CA](#)" on the next page
2. "[Authenticating a Client Using a Trusted CA](#)" on page 101
3. "[Registering a Client to the Appliance](#)" on page 102

**NOTE** This feature requires minimum Luna HSM Client version 10.1.0 and appliance software version 7.7.0. See [Version Dependencies by Feature](#) for more information.

See also "[Using a Combination of Self-Signed and CA-Signed Certificates](#)" on page 103.



## Authenticating the Appliance Using a Trusted CA

Use the following procedure to authenticate the appliance by having its certificate signed by your trusted CA.

### Prerequisites

- > You must have **admin**-level access to LunaSH on the appliance.

### To authenticate the appliance using a certificate signed by a trusted CA

1. Log in to LunaSH as **admin** (see [Logging In to LunaSH](#)).
2. Regenerate the Luna Network HSM server certificate, specifying the **-csr** option to create a Certificate Signing Request (CSR)—an unsigned certificate to be signed by a Certificate Authority (CA). You have the option to specify other information about the certificate.

**CAUTION!** Regenerating the server certificate will break any existing NTLS/STC connections.

```
lunash:> sysconf regencert -csr
```

3. Transfer the CSR (**serverCSR.pem**) from the appliance to a workstation using **sftp** or **pscp**.

```
pscp <user>@<host/IP>:server.pem <target_filename>
```

**NOTE** When using **pscp** or **sftp** over an IPv6 network, enclose addresses in square brackets.

You must accept the SSH certificate the first time you open an SCP/PSCP or SSH link. You can check the SSH fingerprint in LunaSH to confirm the secure connection.

```
lunash:> sysconf fingerprint ssh
```

4. Submit the **serverCSR.pem** certificate file to be signed by the Certificate Authority, as directed by the documentation of the particular Certificate Authority. You require the following artifacts from the CA:
  - Signed base64(PEM)-encoded client certificate in x509 format
  - The CA's base64 certificate in x509 format, including the root certificate
5. Upon receiving the signed server certificate, transfer the signed server certificate and the CA certificate chain to the **admin** user on the appliance using **scp** or **pscp**. The files arriving at the appliance are automatically placed in the appropriate directory. Do not specify a target directory.
6. Log in to LunaSH as **admin** and register the CA certificate chain in the appliance trust store. Specify each certificate's filename, minus the **.pem** extension. Repeat this step until the entire certificate chain is registered.

```
lunash:> client addCA <filename>
```

```
lunash:>client addCA CAroot
```

```
Attempting to install CA cert CAroot:
```

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

7. [Optional] Display a list of CA certificates registered on the appliance.

```
lunash:> client listCAs
```

8. Install the signed appliance server certificate. This replaces the appliance's **server.pem** with the signed certificate.

```
lunash:> sysconf installcert <filename>
```

9. Restart the NTLS, STC and CBS services.

```
lunash:> service restart <service>
```

## Authenticating a Client Using a Trusted CA

Use the following procedure to authenticate the client by having its certificate signed by your trusted CA.

### Prerequisites

- > You must have Administrator privileges on the client workstation.

### To authenticate a client using a certificate signed by a trusted CA

1. On the client workstation, open a command prompt and navigate to the Luna HSM Client directory.

**NOTE** On Windows, ensure that you open a command prompt with Administrator privileges.

- Windows: **C:\Program Files\SafeNet\LunaClient**
- Linux/AIX: **/usr/safenet/lunaclient/bin**
- Solaris: **/opt/safenet/lunaclient/bin**

2. Create a Certificate Signing Request (CSR) for the client—an unsigned certificate to be signed by a third-party Certificate Authority (CA). You must specify the client hostname or IP. You have the option to specify other information about the certificate.

**CAUTION!** Regenerating the client certificate will break any existing NTLS/STC connections.

```
> vtl createCSR -n <client_hostname/IP>
```

The certificate and private key are saved to the <client\_install\_dir>/cert/client directory and are named <client\_hostname/IP>CSR.pem and <client\_hostname/IP>Key.pem, respectively. The command output displays the filepath.

3. Submit the CSR file to be signed by your preferred or in-house Certificate Authority. You require the following artifacts from the CA:

- Signed base64(PEM)-encoded client certificate in x509 format
- The CA's base64(PEM)-encoded certificate chain in x509 format, including the root certificate

4. Register the CA certificate chain in the client's trust store. Specify the full path and filename for each certificate. Repeat this step until the entire certificate chain is registered.

```
> vtl addCA -n <cert_name> -c <cert_filepath/name>
```

5. Copy the signed client certificate to the following location in the Luna HSM Client directory:

- Windows: **C:\Program Files\SafeNet\LunaClient\cert\client\**
- Linux/AIX: **/usr/safenet/lunaclient/cert/client/**
- Solaris: **/opt/safenet/lunaclient/cert/client/**

6. Add the IP/hostname of any Luna Network HSM appliance where the client will access application partitions. The CA chain used to sign the certificate must be added to the trust store of the appliance, as described in ["Authenticating the Appliance Using a Trusted CA" on page 100](#).

```
> vtl addServerNoCert -n <IP/hostname>
```

7. [Optional] Edit **crystoki.ini/Chrystoki.conf** to enable server IP/hostname validation on the client. Do this only if the appliance server certificate was created with Subject Alternate Names (SANs).

```
[Misc]
ValidateHost=1
```

## Registering a Client to the Appliance

Finally, you must transfer the signed client certificate to the appliance and register it.

### Prerequisites

- > The CA chain used to sign the certificate must be added to both the client's and the appliance's trust store.
- > You must have **admin**-level access to LunaSH on the appliance.

### To register a client to the appliance

1. Transfer the signed client certificate to the appliance using **pscp** or **scp**.

2. Log in to LunaSH as **admin** (see [Logging In to LunaSH](#)).
3. Register the client's certificate on the appliance. Specify the client's IP address or hostname, depending on which was used to create the certificate.

```
lunash:> client register -client <clientname> {-hostname <hostname> | -ip <IPaddress>}
```

You can now assign partitions to the client (see "[Assigning or Revoking NTLS Client Access to a Partition](#)" below).

## Using a Combination of Self-Signed and CA-Signed Certificates

It is possible to use a combination of self-signed and CA-signed certificates; meaning a CA-signed certificate on the Luna Network HSM appliance and a self-signed certificate on the client, or vice-versa. To use this configuration, modify the instructions above as follows:

### To use a self-signed client certificate and a CA-signed appliance certificate

- > The entire CA certificate chain must still be registered on both client and appliance.
- > Transfer the client's self-signed certificate (<IP/hostname>.pem) to the appliance and register it.

```
lunash:> client register -client <clientname> {-hostname <hostname> | -ip <IPaddress>}
```

### To use a self-signed appliance certificate and a CA-signed client certificate

- > The entire CA certificate chain must still be registered on both client and appliance.
- > Transfer the appliance's self-signed certificate (**server.pem**) to the client and register it.
  - > **vtl addServer -n** <IP/hostname> **-c** <cert\_filename>

## Assigning or Revoking NTLS Client Access to a Partition

Once an NTLS connection is established between the appliance and a client, the appliance **admin** must determine which application partitions the client can access. Usually this is done by the HSM Security Officer after they create the partition, but any **admin**-level appliance user can assign or revoke existing partitions to registered NTLS clients. You can assign a partition to more than one client at a time.

After you assign a partition to a client, the client can see the partition as a slot in LunaCM, initialize it, and use it for cryptographic applications.

### Prerequisites

- > An NTLS connection must be established between the appliance and the client (see "[Client-Partition Connections](#)" on page 86)
- > The HSM SO must create the application partition on the HSM (see [Creating or Deleting an Application Partition](#))

### To assign a partition to a client

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

2. [Optional] Display a list of available partitions.

```
lunash:> partition list
```

3. [Optional] Display a list of available registered clients.

```
lunash:> client list
```

4. Assign a partition to a registered client.

```
lunash:> client assignpartition -client <client_name> -partition <partition_name>
```

5. [Optional] Verify that the partition is assigned to the client.

```
lunash:> client show -client <client_name>
```

6. If you registered the client by hostname, the appliance uses a DNS server to look up the device IP address. To ensure that the client is reachable in the event of a DNS failure, map the client hostname to its IP address, and save the mapping locally on the appliance.

```
lunash:> client hostip map -client <client_name> -ip <client_IP>
```

7. Notify the client administrator that they can now access the partition and initialize it using LunaCM (see ["Initializing an Application Partition" on page 268](#)).

---

### To revoke partition access from a client

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

2. [Optional] Display a list of partitions currently assigned to the client.

```
lunash:> client show -client <client_name>
```

3. Revoke the client's access to the partition.

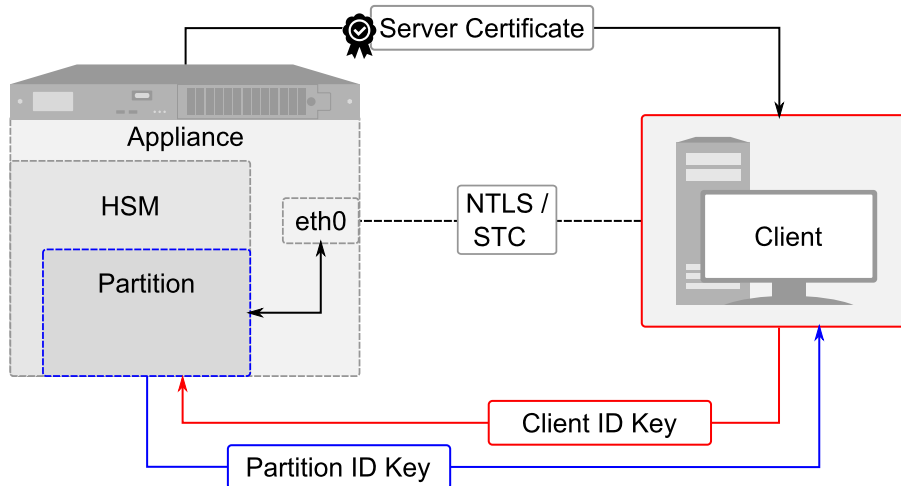
```
lunash:> client revokepartition -client <client_name> -partition <partition_name>
```

---

## Creating an STC Connection

To create a Secure Trusted Channel (STC) connection, a partition identity is created directly on the partition, and the client and partition exchange identities. This allows end-to-end encryption of all communications between partition and client. This section describes how to establish an STC connection between a client and a new partition. The procedure involves the HSM SO and the administrator of the client workstation.





**NOTE** The Luna Network HSM can create STC and NTLS channels to different clients as required. The client can also support both STC and NTLS links. However, all links from a specific client to a specific Luna Network HSM appliance must be either STC or NTLS. STC links are not supported over an IPv6 network. You must use NTLS to make partition-client connections via IPv6.

STC has been updated for the Luna 7.7.0 release. To use the updated STC connections, you require appliance software 7.7.0 or newer, Luna HSM firmware 7.7.0 or newer, and Luna HSM Client 10.3.0 or newer. See [Version Dependencies by Feature](#).

To use Functionality Modules (FMs) with STC client connections, you require Luna HSM firmware 7.7.0 or newer. To use FMs with earlier firmware versions, you must use NTLS connections.

1. ["Preparing the HSM/Partition to Use STC" below](#)
2. ["Preparing the Client to Use STC" on page 107](#)
3. ["Creating a Client-Partition STC Connection" on page 108](#)

## Preparing the HSM/Partition to Use STC

To establish an STC connection between partition and client, you must first enable STC on the HSM (depending on your HSM firmware version), create one or more partitions and export their partition identities. These operations are performed by the HSM SO.

**NOTE** When you enable HSM policy 39: Allow Secure Trusted Channel on Luna 7.4.x or earlier, the following LunaSH commands are blocked to protect the integrity of any STC links that are created:

- > **hsm stc identity create**
- > **hsm stc identity initialize**
- > **hsm stc identity delete**
- > **hsm stc identity partition deregister**

If you plan to use STC on the admin channel and want to recreate the HSM identity first, see "[Configuring STC Identities and Settings](#)" on page 117 before continuing.

### To prepare the HSM and partition(s) for STC connections

1. Connect to the appliance via SSH or a serial connection, and log in to LunaSH as **admin** (see [Logging In to LunaSH](#)).

2. Log in as HSM SO (see [Logging In as HSM Security Officer](#)).

```
lunash:> hsm login
```

3. Enable HSM Policy 39: Allow Secure Trusted Channel. If you are using Luna version 7.7.0 or newer, this policy has been removed; skip this step.

```
lunash:> hsm changepolicy -policy 39 -value 1
```

4. Create one or more new partitions for the client (see [Creating or Deleting an Application Partition](#)).

```
lunash:> partition create -partition <partition_name> [-size <bytes>]
```

**NOTE** Each client identity registered to a partition uses 2392 bytes of storage on the partition. Ensure that you create partitions large enough to store the identity of every client that will access the partition, in addition to cryptographic objects.

When you create a partition, a partition identity key pair is automatically created.

5. For each partition, export the partition identity public key to the Luna Network HSM file system. The file will be named with the partition's serial number. The command syntax is different depending on the Luna software/firmware version:

- **Luna 7.7.0 or newer:**

```
lunash:> partition stcidentity export -partition <partition_name>
```

```
lunash:>partition stcidentity export -partition app_par1
Successfully exported partition identity for partition app_par1 to file: 154438865304.pid
```

- **Luna 7.4.x or earlier:**

```
lunash:> stc partition export -partition <partition_name>
```

```
lunash:>stc partition export -partition app_par1
Successfully exported partition identity for partition app_par1 to file: 154438865304.pid
```

6. [Optional] View the partition identity public key hash. If you are not the client administrator, it is recommended that you provide it (via separate channel) so that the client administrator can verify the key's

integrity as described in ["Creating a Client-Partition STC Connection" on the next page](#). The command syntax is different depending on the Luna software/firmware version:

- **Luna 7.7.0 or newer:**

```
lunash:> partition stcidentity show -partition <partition_name>
```

- **Luna 7.4.x or earlier:**

```
lunash:> stc partition show -partition <partition_name>
```

7. If the client administrator does not have **admin** access to the appliance, or a firewall prevents you from using **pscp** or **scp**, you must transfer these files from the HSM and provide them to the client administrator by other secure means:
  - The HSM Server Certificate (**server.pem**) from the Luna Network HSM.
  - The partition identity public key for each partition the client will access (**154438865304.pid** in the example above).
  - [Optional] The partition identity public key hash for each partition the client will access. This is recommended so that the client can verify the key's integrity before using the partition. Do not send the hash by the same means as the certificates.

## Preparing the Client to Use STC

To access partitions on the HSM using STC, you must first create an STC token and identity on the client. These operations are performed by the client administrator.

**CAUTION!** If you already have STC connections to partitions on other HSMs, skip this procedure and use the existing client token/identity. If you re-initialize an existing client token/identity, active STC connections to this client will be broken.

### To prepare the client for STC connections

1. Open a command prompt or terminal and navigate to the Luna HSM Client directory.

**NOTE** On Windows, ensure that you open a command prompt with Administrator privileges.

- Windows: **C:\Program Files\SafeNet\LunaClient**
  - Linux/AIX: **/usr/safenet/lunaclient/bin**
  - Solaris: **/opt/safenet/lunaclient/bin**
2. [Optional] Launch LunaCM and verify that the STC client token is uninitialized.

```
lunacm:> stc tokenlist
```

3. Initialize the STC client token, specifying a token label.

```
lunacm:> stc tokeninit -label <token_label>
```

4. Create a client identity on the token.

```
lunacm:> stc identitycreate -label <client_identity>
```

The STC client identity public key is automatically exported to:

```
<client_install_directory>/data/client_identities/
```

## Creating a Client-Partition STC Connection

To access STC partitions on the Luna Network HSM appliance, you must first register the HSM Server Certificate. The STC connection is then created by registering one or more partition identity public keys to the client identity and enabling STC on the client. These operations are performed by the client administrator, with **admin** access to the Luna Network HSM appliance. If you do not have **admin** access, or a firewall blocks file transfer over the network, the appliance **admin** must provide these files by other secure means.

### To create a Client-Partition STC Connection

1. On the client workstation, use **pscp** or **scp** to import the HSM Appliance Server Certificate (**server.pem**) from the appliance. You require the appliance's **admin** password to complete this step.

**TIP** If you are importing certificates from multiple appliances to this client, rename each certificate during the **pscp/scp** transfer. This will prevent you from accidentally overwriting one **server.pem** certificate with another.

```
pscp admin@<host/IP>:server.pem <target_filename>
```

2. Register the HSM Server Certificate with the client, using the **vtl** utility from the command line or shell prompt. If using a host name, ensure the name is reachable over the network (**ping <hostname>**). Thales recommends specifying an IP address to avoid network issues.

```
> vtl addServer -n <Network_HSM_hostname/IP> -c <server_certificate>
```

3. [Optional] To check that you have successfully registered the appliance with the client, display the list of registered servers.

```
> vtl listServers
```

4. Use **pscp** or **scp** to import the partition identity public keys for all partitions you will access with STC. The files are named with the partition serial number (**<partitionSN>.pid**). You require the appliance's **admin** password to complete this step.
5. Register the partition identity public key to the client. Specify the path to the key file and, optionally, a label for the partition identity.

```
lunacm:> stc partitionregister -file <partition_identity> [-label <partition_label>]
```

```
lunacm:> stc partitionregister -file /usr/safenet/lunaclient/data/partition_
identities/154438865304.pid -label app_par1
```

```
Partition identity 154438865305 successfully registered.
```

Repeat this step for each partition identity public key you wish to register to this client.

6. [Optional] If the HSM SO provided the partition identity public key hash, verify that the hashes match.

```
lunacm:> stc identityshow
```

If the hashes do not match, deregister the partition and contact your HSM SO.

```
lunacm:> stc partitionderegister -serial <partitionSN>
```

7. Display the list of registered Luna Network HSM servers to find the server ID of the appliance that hosts the partition(s).

```
lunacm:> clientconfig listservers
```

8. Enable the STC connection.

**CAUTION!** This forces the client to use STC for all links to the specified Luna Network HSM appliance. If the server has partitions assigned to this client using NTLS, those connections will be terminated. Ensure you have registered the partition identity for all applicable partitions on this HSM before continuing.

```
lunacm:> stc enable -id <server_ID>
```

LunaCM restarts. If successful, the partition appears in the list of available slots.

9. [Optional] Set the active slot to the new partition and verify the STC link.

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

```
lunacm:> stc status
```

The Partition SO can now initialize the partition (see ["Initializing an Application Partition" on page 268](#)). When the partition is initialized, the following actions are performed automatically:

- > The client identity public key is registered to the partition.
- > Partition policy 37: Force Secure Trusted Channel is enabled on the partition.

Once the partition is initialized, you can allow additional clients to connect to it using STC (see ["Connecting an Initialized STC Partition to Multiple Clients" below](#)).

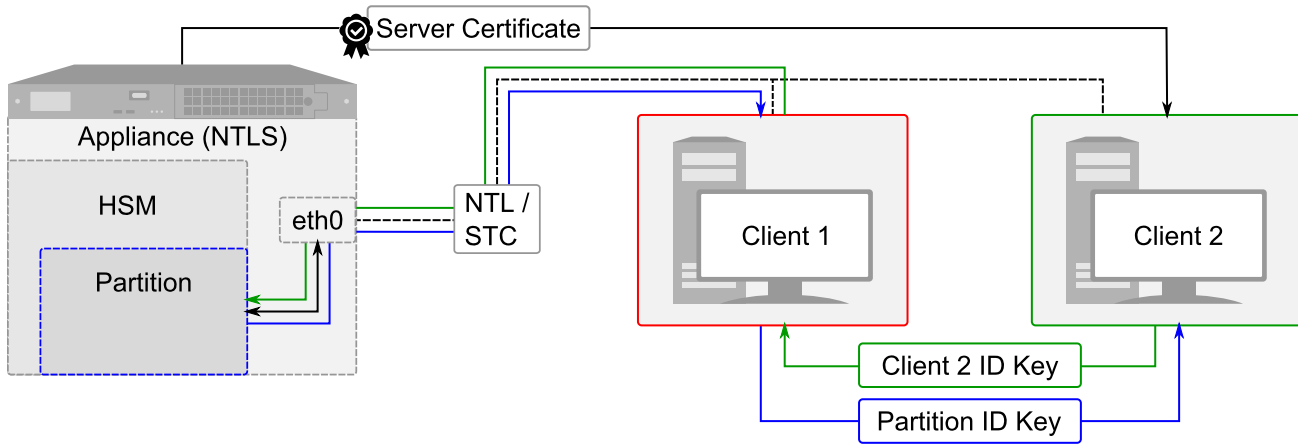
STC provides several configurable options that define the network settings for an STC link, and the security settings for the messages transmitted over the link. Although default values are provided that provide the optimal balance between security and performance, you can override the defaults, if desired. See ["Configuring STC Identities and Settings" on page 117](#) for more information.

## Connecting an Initialized STC Partition to Multiple Clients

Once an STC connection has been established between the partition and Client1, and the partition initialized, the Partition SO can allow other clients to access the partition. Since the Partition SO has control of the partition via Client1, they must provide the partition ID key to the Client2 administrator, and register Client2's ID key to the partition.

This procedure is completed by the Partition SO (using Client1) and the Client2 administrator in the following phases:

1. ["Preparing the Additional Client to Use STC" on the next page](#)
2. ["Connecting an Additional Client to the Initialized STC Partition" on page 111](#)



## Preparing the Additional Client to Use STC

To access partitions on the HSM using STC, you must first create an STC token and identity on the client. These operations are performed by the client administrator.

**CAUTION!** If you already have STC connections to partitions on other HSMs, skip this procedure and use the existing client token/identity. If you re-initialize an existing client token/identity, active STC connections to this client will be broken.

### To prepare the client for STC connections

1. Open a command prompt or terminal and navigate to the Luna HSM Client directory.

**NOTE** On Windows, ensure that you open a command prompt with Administrator privileges.

- Windows: **C:\Program Files\SafeNet\LunaClient**
  - Linux/AIX: **/usr/safenet/lunaclient/bin**
  - Solaris: **/opt/safenet/lunaclient/bin**
2. [Optional] Launch LunaCM and verify that the STC client token is uninitialized.  

```
lunacm:> stc tokenlist
```
  3. Initialize the STC client token, specifying a token label.  

```
lunacm:> stc tokeninit -label <token_label>
```
  4. Create a client identity on the token.  

```
lunacm:> stc identitycreate -label <client_identity>
```

The STC client identity public key is automatically exported to:  
<client\_install\_directory>/data/client\_identities/
  5. [Optional] Display the client ID key hash. You can provide this hash to the Partition SO to verify the key's integrity.  

```
lunacm:> stc identityshow
```

6. Provide the following certificate/information to the Partition SO (Client1) via **pscp**, **scp**, or other secure means:
  - Client2 identity public key
  - [Optional] Client2 identity public key hash (do not provide the hash by the same means as the key)

## Connecting an Additional Client to the Initialized STC Partition

This procedure will allow an additional client (Client2 in the examples below) to access an initialized STC partition. The Partition SO (using Client1) and the Client2 administrator must complete the procedure.

### Partition SO (Client1): To allow an additional client access to the STC partition

1. Ensure that you have received the following certificates/information from the Client2 administrator:
  - Client2 identity public key
  - [Optional] Client2 identity public key hash

2. On Client1, launch LunaCM and log in as Partition SO.

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

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

3. Register the Client2 ID key to the partition. Specify a label for Client2 and the path to the key file.

```
lunacm:> stcconfig clientregister -label <client_label> -file <path/client_ID>
```

4. [Optional] Display the hash for the Client2 identity.

```
lunacm:> stcconfig clientlist
```

If the displayed hash does not match the hash you received from the Client2 administrator, deregister the client identity and contact the Client2 administrator:

```
lunacm:>stcconfig clientderegister -label <client_label>
```

**NOTE** If the Client2 administrator has **admin** access to the Luna Network HSM appliance, and the partition identity public key is still available in the **admin** user's files on the appliance (lunash:> **my file list**), steps 5-7 are unnecessary.

5. Export a copy of the partition identity public key to the Client1 filesystem.

```
lunacm:> stcconfig partitionidexport
```

The partition ID key is named for the partition serial number (<serialnum>.**pid**) and automatically exported to:

```
<Lunaclient_install_directory>/data/partition_identities/
```

6. [Optional] Display the partition ID key hash. You can provide this hash to the Client2 administrator to verify the key's integrity. Do not send the hash by the same means as the key.

```
lunacm:> stc identityshow
```

7. Provide the following certificates/information to the Client2 administrator via **scp**, **pscp**, or other secure means (see **SCP and PSCP**):
  - Partition identity public key

- [Optional] Partition identity public key hash (do not provide the hash by the same means as the key)
- HSM Server Certificate, located in:  
`<Lunaclient_install_directory>/cert/server/<hostname/IP>Cert.pem`

### Client2 administrator: To create the client-partition STC connection

1. Ensure that you have received the following certificates/information from the Partition SO:

- HSM Server Certificate (\*.pem)
- Partition identity public key (\*.pid)
- [Optional] Partition identity public key hash

**NOTE** If the Client2 administrator has **admin** access to the Luna Network HSM appliance, and the partition identity public key is still available in the **admin** user's files on the appliance (lunash:> [my file list](#)), you can retrieve the HSM Server Certificate (**server.pem**) and the partition ID key (<partition\_serialnum>.pid) directly from the appliance using [pscp](#) or [scp](#).

2. Open a command prompt or terminal window and navigate to the Luna Network HSM client installation directory.

3. Register the HSM Server Certificate to the client.

```
> vtl addServer -n <HSM_hostname/IP> -c <server_certificate>
```

4. Launch LunaCM and register the partition ID key to the client. Specify the path to the key file and an optional label for the partition.

```
lunacm:> stc partitionregister -file <path/IDfile>.pid [-label <partition_label>]
```

5. [Optional] Display the hash for the partition ID key.

```
lunacm:> stc identityshow
```

If the displayed hash does not match the hash you received from the Partition SO, deregister the partition and contact the Partition SO:

```
lunacm:> stc partitionderegister -serial <partition_serialnum>
```

6. Display the list of registered Luna Network HSM servers to find the server ID of the appliance that hosts the partition(s).

```
lunacm:> clientconfig listservers
```

7. Enable the STC connection.

**CAUTION!** This forces the client to use STC for all links to the specified Luna Network HSM appliance. If the server has partitions assigned to this client using NTLS, those connections will be terminated. Ensure you have registered the partition identity for all applicable partitions on this HSM before continuing.

```
lunacm:> stc enable -id <server_ID>
```

LunaCM restarts. If successful, the partition appears in the list of available slots.

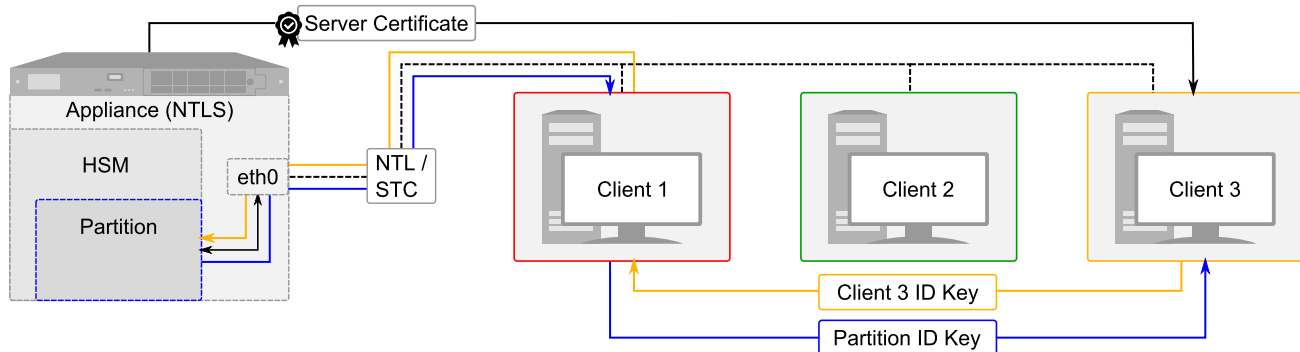
8. [Optional] Set the active slot to the new partition and verify the STC link.



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

```
lunacm:> stc status
```

Client2 can now access the partition via an STC connection. You can repeat the procedure to allow more clients to access the partition.



**NOTE** Each client identity registered to a partition uses 2392 bytes of storage on the partition. Ensure that the partition is large enough to store the identity of every client that will access the partition, in addition to cryptographic objects. If necessary, the HSM SO can re-size an existing partition (see [Customizing Partition Sizes](#)).

STC provides several configurable options that define the network settings for an STC link, and the security settings for the messages transmitted over the link. Although default values are provided that provide the optimal balance between security and performance, you can override the defaults, if desired. See "[Configuring STC Identities and Settings](#)" on page 117 for more information.

## Converting Initialized NTLS Partitions to STC

If you have initialized partitions already assigned to a client using NTLS, you can use the following procedure to switch to a more secure STC connection. All of the client's assigned partitions on the specified Luna Network HSM must be converted. It is not possible for a client to connect to multiple partitions on a single Luna Network HSM using a combination of NTLS and STC.

The Partition SO must complete this procedure on the client workstation.

### Prerequisites

- > If you are using Luna HSM firmware 7.4.x or earlier, the HSM SO must set HSM Policy 39: Allow Secure Trusted Channel to **1** (ON).

### To convert an NTLS partition-client connection to STC

1. Launch LunaCM and create the client token and identity.

**NOTE** This step is not required if you have already created a client token and identity. Verify using [stc identityshow](#). If you recreate the client identity, you will have to re-register any existing STC partitions.

```
lunacm:> stc tokeninit -label <token_label>
```

```
lunacm:> stc identitycreate -label <client_identity>
```

The STC client identity public key is automatically exported to:

```
<client_install_directory>/data/client_identities/
```

2. Log in as Partition SO and export the partition ID key.

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

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

```
lunacm:> stcconfig partitionidexport
```

The partition identity public key is named for the partition serial number (<partitionSN>.**pid**) and automatically exported to:

```
<client_install_directory>/data/partition_identities/
```

3. Register the partition's public key with the client identity. Specify the path to the key file.

```
lunacm:> stc partitionregister -file <path/filename>.pid [-label <partition_label>]
```

4. Register the client identity to the partition. Specify a label for the client and the path to the client identity file.

**NOTE** Each client identity registered to a partition uses 2392 bytes of storage on the partition. Ensure that there is enough free space before registering a client identity.

```
lunacm:> stcconfig clientregister -label <client_label> -file <path/client_identity>
```

5. Depending on your firmware version, enable partition policy 37: Force STC Connection.

- **Luna HSM firmware 7.4.x or earlier:** You must enable policy 37 to use STC. All clients accessing this partition must perform the STC registration procedure in steps 1-4.
- **Luna HSM firmware 7.7.0 or newer:** To enforce STC on all client connections to this partition, enable policy 37. If you want some clients to connect to this partition using NTLS, do not enable this policy.

**CAUTION!** Any existing NTLS client connections to this partition will be terminated when you enable policy 37. Ensure that all clients that access this partition have performed the STC registration procedure in steps 1-4 before you enable policy 37.

```
lunacm:> partition changepolicy -slot <slotnum> -policy 37 -value 1
```

**NOTE** When you enable partition policy 37, the client loses contact with the partition until you enable the STC connection in step 7. This is expected behavior.

6. Repeat steps 2-5 for each NTLS partition on the same Luna Network HSM you want to register to this client.
7. Find the server ID for the Luna Network HSM hosting the partition and enable its STC connection. You will be prompted to restart LunaCM and all current sessions will be closed.

**CAUTION!** This forces the client to use STC for all links to the specified appliance. Any remaining NTLS links from this client to the appliance will be terminated. Ensure that you have completed steps 2-5 for each of this client's partitions before continuing.

```
lunacm:> clientconfig listservers
```

```
lunacm:> stc enable -id <server_ID>
```

If a partition is not visible as a slot when LunaCM restarts, disable STC for the server using `lunacm:> stc disable -id <server_ID>`, and ensure that you have activated partition policy 37.

STC provides several configurable options that define the network settings for an STC link, and the security settings for the messages transmitted over the link. Although default values are provided that provide the optimal balance between security and performance, you can override the defaults, if desired. See "[Configuring STC Identities and Settings](#)" on page 117 for more information.

## Using the STC Admin Channel

Secure Trusted Channel (STC) can protect all communications to the HSM, including those originating on the Luna Network HSM appliance. The STC admin channel is local to the appliance, and is used to encrypt data transmitted between the HSM and the local services running on the appliance (such as LunaSH, NTLS, and the STC service). The STC admin channel link is configured separately from the client-partition links, and can be enabled or disabled as required by the HSM SO.

**NOTE** The STC admin channel is configurable using Luna Network HSM appliance software and Luna HSM firmware 7.4.x and earlier. This feature is not available in Luna Network HSM 7.7 and newer.

Unique STC identities, each defined by a 2048-bit RSA asymmetric public/private key pair, exist on the HSM and the Luna Network HSM appliance operating system. When you enable the STC admin channel, the HSM and the appliance create a trust link by exchanging public keys, and the private keys are used to encrypt all communications between them.

**NOTE** Enabling the STC admin channel forces all client-partition links (NTLS or STC) to use STC for communications between the appliance and the HSM. This may affect NTLS link performance.

## Enabling the STC Admin Channel

When enabled, all communications from the appliance operating system to the HSM are transmitted over the STC admin channel.

**NOTE** When you enable HSM policy 39: Allow Secure Trusted Channel on Luna 7.4.x or earlier, the following LunaSH commands are blocked to protect the integrity of any STC links that are created:

- > **hsm stc identity create**
- > **hsm stc identity initialize**
- > **hsm stc identity delete**
- > **hsm stc identity partition deregister**

If you plan to use STC on the admin channel and want to recreate the HSM identity first, see "[Configuring STC Identities and Settings](#)" on the next page before continuing.

### To enable the STC admin channel

1. Open a LunaSH session on the appliance and log in as the HSM SO.

```
lunash:> hsm login
```

2. If you have not already done so, enable HSM Policy 39: Allow Secure Trusted Channel.

```
lunash:> hsm changepolicy -policy 39 -value 1
```

3. Enable the STC admin channel.

**CAUTION!** Enabling the STC admin channel is service-affecting. It causes an STC service restart, which temporarily terminates all existing STC links to the appliance. It also terminates the existing HSM login session.

```
lunash:> hsm stc enable
```

### Disabling the STC Admin Channel

When disabled, all communications from the appliance operating system to the HSM are transmitted, unencrypted, over the local bus.

**NOTE** Disabling the STC admin channel is service affecting. It causes an STC service restart, which temporarily terminates all existing STC links to the appliance. It also terminates the existing HSM login session.

### To disable the STC admin channel

1. Open a LunaSH session on the appliance and log in as HSM SO.

```
lunash:> hsm login
```

2. Disable the STC admin channel.

```
lunash:> hsm stc disable
```

## Configuring the STC Admin Channel

STC provides several configurable options that define the network settings for an STC link, and the security settings for the messages transmitted over the link. Although default values are provided that provide the optimal balance between security and performance, you can override the defaults, if desired. See ["Configuring STC Identities and Settings"](#) below for more information.

## Configuring STC Identities and Settings

Depending on your organization's security needs, you may need to customize some aspects of your Secure Trusted Channel (STC) connections. This can include encryption levels for message verification, request timeouts, periodic replacement of client identities, and more. Luna Network HSM provides configurable options for customizing your STC connections.

- > ["Configuring STC Settings"](#) below
- > ["Configuring STC Tokens and Identities"](#) on page 119

## Configuring STC Settings

STC provides configurable options that define network settings for an STC link, and security settings for the messages transmitted over that link. Although default values are provided that provide the optimal balance between security and performance, you can override the defaults, if desired.

- > ["Link Activation Timeout"](#) below
- > ["Message Encryption"](#) on the next page
- > ["Message Integrity Verification"](#) on the next page
- > ["Rekey Threshold"](#) on page 119

For client-partition STC links, these options are set individually for each partition. Using Luna 7.4.x and earlier, they can be set by the HSM SO (using LunaSH) before the STC connection is established, or by the Partition SO (using LunaCM) after the STC partition is initialized. Using Luna 7.7.0 and newer, only the Partition SO can configure STC options, after the partition is initialized.

For the STC admin channel, the configuration applies to all communications between the HSM and local services on the appliance, such as LunaSH and NTLS. The STC admin channel options are set by the HSM SO.

**NOTE** The STC admin channel is configurable using Luna Network HSM appliance software and Luna HSM firmware 7.4.x and earlier. This feature is not available in Luna Network HSM 7.7 and newer.

### Link Activation Timeout

The activation timeout is the maximum time allowed to establish the STC link before the channel request is dropped. You can use the following commands to specify the activation timeout for STC links to this partition.

#### STC admin channel (HSM SO, Luna 7.4.x and earlier)

```
lunash:> hsm stc activationtimeout show
```

```
lunash:> hsm stc activationtimeout set -time <seconds>
```

---

### Uninitialized STC Partition (HSM SO, Luna 7.4.x and earlier)

```
lunash:> stc activationtimeout show
```

```
lunash:> stc activationtimeout set -partition <partition> -time <seconds>
```

---

### Initialized STC Partition (Partition SO)

```
lunacm:> stcconfig activationtimeoutshow
```

```
lunacm:> stcconfig activationtimeoutset -time <seconds>
```

## Message Encryption

By default, all messages traversing an STC link are encrypted. You can use the following commands to specify the level of encryption used (AES 128, AES 192, or AES 256) on all STC links to a partition, or to disable encryption on all STC links to a partition.

---

### STC admin channel (HSM SO, Luna 7.4.x and earlier)

```
lunash:> hsm stc cipher show
```

```
lunash:> hsm stc cipher enable {-all | -id <cipher_id>}
```

```
lunash:> hsm stc cipher disable {-all | -id <cipher_id>}
```

---

### Uninitialized STC Partition (HSM SO, Luna 7.4.x and earlier)

```
lunash:> stc cipher show
```

```
lunash:> stc cipher enable -partition <partition_name> {-all | -id <cipher_id>}
```

```
lunash:> stc cipher disable -partition <partition_name> {-all | -id <cipher_id>}
```

---

### Initialized STC Partition (Partition SO)

```
lunacm:> stcconfig ciphershow
```

```
lunacm:> stcconfig cipherenable {-id <cipher_ID> -all}
```

```
lunacm:> stcconfig cipherdisable {-id <cipher_ID> -all}
```

## Message Integrity Verification

By default, the integrity of all messages traversing an STC link is verified using an HMAC message digest algorithm. You can use the following commands to specify the algorithm used (HMAC with SHA 256, or HMAC with SHA 512).

---

### STC admin channel (HSM SO, Luna 7.4.x and earlier)

```
lunash:> hsm stc hmac show
```

```
lunash:> hsm stc hmac enable -id <hmac_ID>
```

```
lunash:> hsm stc hmac disable -id <hmac_ID>
```

**Uninitialized STC Partition (HSM SO, Luna 7.4.x and earlier)**

```

lunash:> stc hmac show
lunash:> stc hmac enable -partition <partition_name> -id <hmac_ID>
lunash:> stc hmac disable -partition <partition_name> -id <hmac_ID>

```

**Initialized STC Partition (Partition SO)**

```

lunacm:> stcconfig hmacshow
lunacm:> stcconfig hmacenable -id <hmac_ID>
lunacm:> stcconfig hmacdisable -id <hmac_ID>

```

**Rekey Threshold**

The session keys and encryption keys created when an STC tunnel is established are automatically regenerated after the number of messages specified by the rekey threshold have traversed the link. You can use the following commands to specify the key life for the session and encryption keys used on all STC links to a partition. Specify the <threshold> value in millions of messages.

**STC admin channel (HSM SO)**

```

lunash:> hsm stc rekeythreshold show
lunash:> hsm stc rekeythreshold set -value <threshold>

```

**Uninitialized STC Partition (HSM SO)**

```

lunash:> stc rekeythreshold show
lunash:> stc rekeythreshold set -partition <partition_name> -value <threshold>

```

**Initialized STC Partition (Partition SO)**

```

lunacm:> stcconfig rekeythresholdshow
lunacm:> stcconfig rekeythresholdset -value <threshold>

```

**Configuring STC Tokens and Identities**

Each Luna HSM Client and partition that serves as an STC endpoint (including the HSM SO partition and the appliance operating system) has a unique identity, defined by a 2048-bit RSA asymmetric public/private key pair. The STC identity key pair is stored in the STC token associated with the client or partition (or the appliance or HSM). Before STC can create secure tunnels, trust must be established through the exchange of public keys.

Partition and HSM tokens and identities are created automatically and cannot be recreated. Client tokens and identities are created manually using LunaCM. The appliance token and identity is created automatically but can be recreated if necessary using LunaSH.

Under normal operating conditions, you should not need to recreate the STC tokens or identities. If you have operational or security reasons to do so, use the following commands:

## Client Tokens and Identities

Use the following LunaCM commands:

| Command                              | Description                                                                                   |
|--------------------------------------|-----------------------------------------------------------------------------------------------|
| <code>stc identitycreate</code>      | Create a client identity on the STC client token.                                             |
| <code>stc identitydelete</code>      | Delete a client identity from the STC identity token.                                         |
| <code>stc identityexport</code>      | Export the STC client identify to a file.                                                     |
| <code>stc identityshow</code>        | Display the client name, public key hash, and registered partitions for the STC client token. |
| <code>stc partitionderegister</code> | Remove a partition identity from the STC client token.                                        |
| <code>stc partitionregister</code>   | Register a partition to the STC client token.                                                 |
| <code>stc tokeninit</code>           | Initialize a client token.                                                                    |
| <code>stc tokenlist</code>           | List the available STC client identity tokens.                                                |

## STC Admin Channel Appliance Identity

**NOTE** The STC admin channel is configurable using Luna Network HSM appliance software and Luna HSM firmware 7.4.x and earlier. This feature is not available in Luna Network HSM 7.7 and newer.

To ensure the integrity of existing STC connections, many of the following commands cannot be used when HSM policy 39: Allow Secure Trusted Channel is on. You must disable HSM policy 39 before recreating the admin channel identity.

Use the following LunaSH commands:

| Command                                            | Description                                                                                                           |
|----------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------|
| <code>hsm stc identity create</code>               | Create a STC client identity for the STC admin channel.                                                               |
| <code>hsm stc identity delete</code>               | Delete the STC admin channel client identity.                                                                         |
| <code>hsm stc identity initialize</code>           | Initialize the STC admin channel client token.                                                                        |
| <code>hsm stc identity partition deregister</code> | Remove the HSM SO partition identity public key that is currently registered with the STC admin channel client token. |
| <code>hsm stc identity partition register</code>   | Register the HSM SO partition identity public key with the STC admin channel client token.                            |



| Command                               | Description                                                                                          |
|---------------------------------------|------------------------------------------------------------------------------------------------------|
| <a href="#">hsm stc identity show</a> | Display the name, public key hash, and registered partitions for the STC admin channel client token. |

## Restoring Broken NTLS or STC Connections

If a certificate used to authenticate NTLS or STC connections is deleted, regenerated, or has expired, the TLS handshake fails, and connections must be re-established before cryptographic operations can resume. This can be the result of HSM or partition zeroization (STC), regeneration/expiry of the HSM server certificate (**server.pem**) on the Luna Network HSM appliance, or expiry of a client certificate. The procedures on this page will allow you to restore your broken connections, wherever possible.

- > ["Restoring NTLS/STC Connections after Regenerating the Server and/or Client Certificates" below](#)
- > ["Restoring Connections After HSM Zeroization" on the next page](#)
- > ["Restoring STC Connections After Partition Zeroization" on the next page](#)

### Restoring NTLS/STC Connections after Regenerating the Server and/or Client Certificates

If you regenerate the HSM server certificate (**server.pem**) and/or a client certificate, you must restore all NTLS and STC connections using the new certificate(s).

#### To restore NTLS connections using an HSM server certificate signed by a third-party CA

Restore NTLS connections using the procedure for ["Authenticating the Appliance Using a Trusted CA" on page 100](#). You do not need to re-install the CA certificate chain, only the new server certificate.

#### To restore NTLS connections using a client certificate signed by a third-party CA

Restore NTLS connections using the procedures for ["Authenticating a Client Using a Trusted CA" on page 101](#) and ["Registering a Client to the Appliance" on page 102](#). You do not need to re-install the CA certificate chain, only the new server certificate.

#### To restore NTLS or STC connections using a self-signed HSM server certificate

##### Appliance admin:

1. Using LunaSH, restart the NTLS and STC services.
 

```
lunash:> service restart ntls
lunash:> service restart stc
```
2. Provide the new HSM Server Certificate (**server.pem**) to each client by **pscp**, **scp**, or other secure means.

##### Client administrators:

1. If you have access to LunaSH on the Luna Network HSM appliance, you can retrieve the new HSM server certificate (**server.pem**) using **pscp** or **scp**. Otherwise, the appliance administrator must provide it.
2. Delete the original server identity from the client.

```
>vtl deleteServer -n <hostname/IP>
```

3. Register the new HSM server certificate with the client.

```
>vtl addServer -n <hostname/IP> -c <cert_filename>
```

4. If you are restoring STC connections, launch LunaCM, find the new Server ID, and enable STC for the server.

```
lunacm:> clientconfig listservers
```

```
lunacm:> stc enable -id <server_ID>
```

## Restoring Connections After HSM Zeroization

If the HSM is zeroized, all partitions and their contents are erased. New partitions must be created and assigned to their clients via the usual connection procedure.

### NTLS connections

The HSM SO must re-initialize the HSM, create new partitions, and assign them to their respective registered clients (see ["Assigning or Revoking NTLS Client Access to a Partition" on page 103](#)). You do not need to register new appliance/client certificates unless they are regenerated.

### STC connections

When the HSM is zeroized, the following occurs:

- > HSM policy 39: Allow Secure Trusted Channel is turned off.
- > The STC application partition identities are deleted along with the partitions.
- > If the STC admin channel is enabled, the STC admin partition identity is deleted, breaking the STC admin channel between LunaSH and the HSM.

Create new STC connections using the standard procedure found in ["Creating an STC Connection" on page 104](#). You can use the existing client tokens/identities. You do not need to register a new HSM server certificate unless it was regenerated using lunash:> [sysconf regencert](#).

## Restoring STC Connections After Partition Zeroization

The registered client identities used to validate STC clients are stored on each partition. Since they are not cryptographic objects, they are not backed up as part of a normal partition backup operation. If the partition is zeroized due to multiple login failures, the registered client identities are erased and regenerated. The HSM SO must provide the new partition identity to the client administrator, who must register the new identity.

### To restore an STC connection after partition zeroization

#### HSM SO:

1. Log in to LunaSH and log in as HSM SO.
 

```
lunash:> hsm login
```
2. Export the new partition identity key to the appliance filesystem.
 

```
lunash:> stc partition export -partition <label>
```

3. Provide the new partition identity key (<partitionSN>.pem) to the client by **pscp**, **scp**, or other secure means.

#### Client administrator:

1. If you have access to LunaSH on the Luna Network HSM appliance, you can retrieve the new partition identity key (<partitionSN>.pem) using **pscp** or **scp**. Otherwise, the HSM SO must provide it.

2. Launch LunaCM and de-register the original partition identity from the client.

```
lunacm:> stc partitionderegister -serial <partitionSN>
```

3. Register the new partition identity key (<partitionSN>.pem) to the client.

```
lunacm:> stc partitionregister -file <path/filename> [-label <label>]
```

4. Restart LunaCM.

```
lunacm:> clientconfig restart
```

You can now re-initialize the STC partition.

## Updating Luna Network HSM with STC Partitions to 7.7.0 or Newer

The Luna 7.7.0 release includes substantial improvements to Secure Trusted Channel. If you have been using STC with an older version of the Luna software/firmware, your STC identities are no longer compatible with the updated STC. Follow the procedure below to ensure that your cryptographic objects are preserved during the update process. This procedure must be performed in part by the HSM SO, and by the Partition SO and Crypto Officer for each STC partition on the HSM.

Previously,

**CAUTION!** Certain essential steps in this procedure are destructive; ensure that all STC partitions on the HSM are fully backed up to avoid losing your cryptographic objects.

### Cryptography is enhanced (requires firmware 7.7.0)

New FIPS and Common Criteria compliant cipher suites are added -- ECDH P-521 + AES-GCM and ECDH P-521 + AES-CTR + HMAC-SHA-512 -- for key derivation, encryption and authentication.

Key Derivation – Perfect forward secrecy

- > Each party provides an ephemeral key and a static key
- > Compromising the static key doesn't compromise all past and future communications

Bilateral Key Confirmation and Unidirectional AES keys [NIST requirement]

- > Both parties ensure that the other party has derived the same keys
- > 2 AES keys are derived: one for encryption and one for decryption
- > Prevents reverse replay attacks

## Prerequisites

- > [PED-authenticated] You require access to a Luna PED, updated to a supported firmware version:
  - Luna PED firmware 2.7.4 or newer for older PED
  - Luna PED firmware 2.9.0 or newer for refreshed PED
 See ["Updating Luna PED Firmware \(for older-version PED that requires a power-block\)" on page 218](#).
- > Update the Luna HSM Client software on all clients to 10.3.0 or newer (see ["Updating the Luna HSM Client Software" on page 85](#)).
- > You require a Luna Backup HSM (G5 or G7-based). Earlier firmware versions can be used for migration purposes, but after this procedure, the following minimum Backup HSM firmware versions are required to back up and restore the updated partitions:
  - Luna Backup HSM (G7) firmware 7.7.1 or newer (see ["Updating the Luna Backup HSM \(G7\) Firmware" on page 449](#))
  - Luna Backup HSM (G5) firmware 6.28.0 or newer (see ["Updating the Luna Backup HSM \(G5\) Firmware" on page 395](#))

## To update Luna Network HSM with STC Partitions to 7.7.0 or Newer

1. **Crypto Officer for each STC partition:** Back up all cryptographic objects. Parts of the update process are destructive; ensure that your partitions are fully backed up before proceeding.
  - ["Backup and Restore Using a Luna Backup HSM \(G7\)" on page 408](#)
  - ["Backup and Restore Using a Luna Backup HSM \(G5\)" on page 379](#)
2. **Partition SO for each STC partition:** Disable partition policy 37: Force Secure Trusted Channel. This is a destructive action; ensure that the partition is backed up before proceeding (see ["Setting Partition Policies Manually" on page 283](#)).
 

At this point in the procedure, all affected partitions have been zeroized and are available to the client using NTLS connections. Partition roles and credentials are preserved.
3. **HSM SO:** If you have STC enabled on the admin channel, disable it (see ["Disabling the STC Admin Channel" on page 116](#)).
4. **HSM SO:** Disable HSM policy 39: Allow Secure Trusted Channel (see [Setting HSM Policies Manually](#)).
5. **HSM SO:** Proceed with the appliance software update (see [Updating the Luna Network HSM Appliance Software](#)).
6. **HSM SO:** Install the HSM firmware update (see [Updating the Luna HSM Firmware](#)).
7. **Partition SO for each STC partition:** Re-establish the STC connection for each client and partition. Since the partitions are already initialized, use the following procedure. You must re-create the STC client identity on each affected client:
  - ["Converting Initialized NTLS Partitions to STC" on page 113](#)

If you have STC partitions that are being accessed by multiple clients, each client must re-create the STC client identity and re-establish connections using the following procedure:

  - ["Connecting an Initialized STC Partition to Multiple Clients" on page 109](#)
8. **Crypto Officer for each STC partition:** You may now restore your cryptographic objects from backup.

- ["Restoring From a Client-Connected Luna Backup HSM \(G7\) "](#) on page 426
- ["Backup/Restore Using a Client-Connected Luna Backup HSM \(G5\)"](#) on page 401

# What are "pre-firmware 7.7.0", and V0, and V1 partitions?

Luna HSM preserves traditional keys-in-hardware operation, and improves on it with fixes and security updates, while also adding the option to securely store more keys than will fit inside an HSM.

Traditional support of Luna features is retained in what we call version zero or V0 partitions, to distinguish from version one or V1 partitions, that:

- > implement "[Scalable Key Storage \(SKS\)](#)" on page 139 to securely externally store and manage keys in vastly greater quantities than can fit inside an HSM,
- > conform with FIPS SP 800-131A (revised),
- > comply with current and anticipated Common Criteria and eIDAS requirements (including "[Per-Key Authorization \(PKA\)](#)" on page 164 ),
- > support an improved version of Secure Trusted Channel ( see "[Creating an STC Connection](#)" on page 104 ).

You can create either kind of application partition (the default is V0) or you can update firmware from pre-7.7.0 and have your existing partitions automatically become version zero with no loss of functionality, and with a further option to convert to version one if there is ever a need.

This section is of interest

- > to customers who already have HSMs in operation and are looking to upgrade, where possible, or
- > to anyone wanting to know what differences in behavior to expect if you elect to change from the default V0 partition type to V1.

Version 7.x hardware can accept upgraded firmware, discussed in this section, and works best in conjunction with

- Luna Client software 10.3.0 or newer and
- Luna Network HSM appliance software 7.7.0 or newer.

You might be looking to migrate existing keys and objects from their application partitions to updated partitions, both for older HSM generations being supplanted, and for current hardware being updated.

The ability to migrate keys and objects from "pre-firmware 7.7.0" to new partitions is preserved. Some new administrative commands, and new options to pre-existing commands, have been added. Any API changes are as transparent as possible to maintain the function of existing customer and partner applications.

| Partition type ==><br>Firmware 7.7.0 and newer | V0                                                                                                                                                                                   | V1                                                                                                                                                                                                                                         |
|------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Description ==>                                | <ul style="list-style-type: none"> <li>&gt; Continues the Luna tradition of "keys always in hardware", for ongoing compatibility with existing applications and use-cases</li> </ul> | <ul style="list-style-type: none"> <li>&gt; Adds the ability to store large numbers of keys safely outside the HSM,</li> <li>&gt; Adds Per-Key Authorization capability,</li> <li>&gt; ... both for RSS and other applications.</li> </ul> |

The following sections go into greater, more explicit detail about how various aspects of HSM / application-Partition functionality are affected by upgrading and by creating new partitions with the relevant creation-time options.

## What is the origin of each partition type

### Pre-firmware 7.7.0 Partition

This is any partition on a Luna HSM from firmware version from 7.0 up to (but not including) version 7.7.0.

### V0 Partition (Firmware 7.7.0 or newer)

Any pre-existing partition, when HSM firmware is updated to version 7.7.0 or newer, becomes a V0 partition.

Any new partition, created using the default partition type ("-version" option) of the command ["partition create" on page 1](#) (in lunash).

Any partition created on a firmware-7.7.0 (or newer) HSM, by an older client that does not know about the V0 / V1 distinction, is always V0.

The V0 status is a partition policy (#41).

### V1 Partition (Firmware 7.7.0 or newer)

Any partition created with the [non-default] V1 option selected in the command ["partition create" on page 1](#) (in lunash).

A V0 partition (whether created as V0 or a pre-existing partition that got upgraded with 7.7.0 firmware) can be converted to a V1 partition, without losing any contained objects. Do this by changing Policy 41 to value 1.

## Partition Policy considerations

### Pre-firmware 7.7.0 Partition

There are no special considerations for pre-existing partitions, created with earlier firmware. Behavior with respect to Partition Policies is unchanged.

### V0 Partition (Firmware 7.7.0 or newer) and V1 Partition (Firmware 7.7.0 or newer)

#### *Partition policy 41 - Partition version*

- > Defaults to version zero (partition V0)
  - when a new partition is created on a firmware 7.7.0 (or newer) HSM
  - when a partition already exists on a pre-7.7.0 HSM that is then updated to firmware 7.7.0 (or newer)
- > Becomes version one (partition V1)
  - when **-version 1** is specified as a new partition is created on a firmware 7.7.0 (or newer) HSM
  - when lunacm command partition **changepolicy -policy 41 -value 1** is issued
- > V0 partition contents are preserved if/when policy 41 is set to version 1 (convert V0 partition to V1)
- > The V1 status persists for the life of the partition unless command partition **changepolicy -policy 41 -value 0** is issued
  - which reverts the partition to V0, and
  - all partition contents are erased, and
  - Scalable Key Storage and Per-Key Authorization are disabled.
- > Some other policies are also interdependent with the partition version status. See "[Partition Capabilities and Policies](#)" on page 272 3, 7, 31, 32, and 40.

## General HSM behavior

### Pre-firmware 7.7.0 Partition

There are no special considerations for pre-existing partitions, created with earlier firmware. Behavior with respect to cloning, backup, etc. is unchanged.

### V0 Partition (Firmware 7.7.0 or newer)

Behavior defaults to V0 behavior, where keys reside in hardware.

Keys can be archived to a Backup HSM or shared for purposes of redundancy and load-balancing in an HA environment, but only when securely cloned among HSMs within the same encryption domain.

Your historic applications and integrations are supported.

### V1 Partition (Firmware 7.7.0 or newer)

V1 option adds key export capability when you need to support larger numbers of keys than will fit inside an HSM, yet they must remain within the secure cryptographic boundary ("[Scalable Key Storage \(SKS\)](#)" on page 139)



The exported keys are always encrypted by a master key (SMK) that remains within an HSM and can be securely copied only to another HSM that shares the same cryptographic domain.

### **Admin Partition Behavior with Pre-7.7.0 HSM / Pre-10.3.0 Client**

Older client software (example 7.4 or 10.2.0) cannot create a V1 partition on an HSM with firmware 7.7.0 or newer.

Similarly, if a V1 partition is created on a 7.7.0 (or newer) Network HSM appliance and linked to an older Client, the client can see the remote partition, but cannot initialize or use the V1 partition. (Expect error CKR\_ACCESS\_ID\_INVALID)

Client must be version 10.3.0 or newer to create and work with V1 partitions (see \*\* at the bottom of this page).

## Cloning

### **Pre-firmware 7.7.0 Partition**

There are no special considerations for pre-existing partitions, created with earlier firmware. Behavior with respect to cloning, Key Export etc. is unchanged.

### **V0 Partition (Firmware 7.7.0 or newer)**

When an HSM's firmware is updated to version 7.7.0 or newer, any existing partitions become V0, and all contents are updated.

The cloning protocol becomes a newer, more secure version that can accept objects cloned from older versions, but that is not permitted to clone to an older version HSM.

### **V1 Partition (Firmware 7.7.0 or newer)**

When a new V1 partition is created, or when a V0 partition is converted to V1, cloning is restricted to only the SMK. Replication or archiving of objects is done via SKS only.

- > Objects cannot be cloned from a V0 partition or from a pre-7.7.0 partition into a V1 partition, and
- > objects cannot be cloned from a V1 partition to a non-V1 partition.

**NOTE** The library attempts to perform the individual actions of a cloning operation in sequence on the respective partitions. If the policies and partition types on the source and target partitions are incompatible, the **partition clone** command (or an attempted HA synchronization) can fail with a message like CKR\_DATA\_LEN\_RANGE while trying to clone. This can occur if a key object from the source partition is a different size than an equivalent object expected by the target.

## SMK (SKS Master Key)

### **Pre-firmware 7.7.0 Partition**

This is not applicable before firmware 7.7.0, because SKS and therefore the SMK do not exist in Luna HSM version 7 prior to firmware 7.7.0.

### **V0 Partition (Firmware 7.7.0 or newer)**

Each V0 partition has a unique Primary SMK generated when the Crypto Officer role logs in for the first time, but it cannot be seen or used while the partition is in V0 state. However, that SMK is in place, in case you ever change partition policy 41 to make the current partition a V1 partition.

### **V1 Partition (Firmware 7.7.0 or newer)**

Each V1 partition has a unique Primary SMK generated when the Crypto Officer role logs in for the first time, but it can also accept a replacement Primary SMK via cloning (such as when joining a partition to an existing HA group)

Each V1 partition also has additional SMK slots or holding areas for:

- > Rollover SMK,
- > SMKs from earlier-model HSMs,
- > FM SMK for partitions with Functionality Modules enabled.

The Primary SMK secret is used to extract and to insert keys/objects; all other SMK secrets can be used only to insert keys/objects.

## Behavior at partition level

### **Pre-firmware 7.7.0 Partition**

There are no special considerations for pre-existing partitions, created with earlier firmware. Behavior with respect to cloning, backup, HA, etc., is unchanged.

### **V0 Partition (Firmware 7.7.0 or newer)**

Whether pre-existing and updated, or newly created, V0 partitions should be generally indistinguishable from previous-firmware partitions -- continuing to work with your applications -- with provisos mentioned below. Cloning or Export/Import function as expected:

- > from older versions (pre-firmware 7.7),
- > to-or-from V0 partitions (firmware 7.7.0 or newer),
- > but not back to older-version partitions.

Client versions earlier than 10.3 do not support expression of V0/V1 partition types (policy 41) for Partition Policy Template (PPT)

- > **partition showPolicies -exportTemplate** does not report V0/V1 partition policy.
- > **partition init -label <somelabel> -applytemplate <template file>** supports management of V0/V1 partition template correctly.
- > Partition initialization without V0/V1 partition policy succeeds with correct default value (V0).

### **V1 Partition (Firmware 7.7.0 or newer)**

Only the SKS Master Key (the SMK) is cloned from partition to partition, or from HSM to HSM for HA or for Backup/Restore. All other objects are encrypted with the SMK and Extracted for external storage or retrieved from external storage and inserted for use within the HSM.

## Structure of partition

### Pre-firmware 7.7.0 Partition

There are no special considerations for pre-existing partitions, created with earlier firmware. Structure is unchanged until you update firmware to version 7.7.0 or newer.

### V0 Partition (Firmware 7.7.0 or newer)

Partition structure is generally as for pre-7.7.0 partition, but with some updated overhead taking up some space; a completely filled pre-7.7.0 partition would need more room for objects after migration/firmware-update, but this is taken care of by partition size increases, as needed, during firmware update. The increase is enabled by an increase in available memory that is also part of the update process (see below).

### V1 Partition (Firmware 7.7.0 or newer)

When a new partition is created at V1 or a V0 partition is converted to V1, the new structural overhead applies, including the space allotted for Primary and other SMKs.

Also, some keys can have new/additional attributes necessary to satisfy newer crypto and security standards.

## Objects in a partition

### Pre-firmware 7.7.0 Partition

Object characteristics and behavior are unchanged until you update firmware to version 7.7.0 or newer.

### V0 Partition (Firmware 7.7.0 or newer)

Memory allotment is increased (from pre-7.7) to allow increased partition size, all pre-existing keys and all new keys receive new attributes (if applicable to key type) but those attributes are not used for anything in V0 partitions (see \* at the bottom of this page).

### V1 Partition (Firmware 7.7.0 or newer)

Memory allotment is increased (from pre-7.7) to allow increased partition size. There are no pre-existing keys in new V1 partitions, and all new keys receive the new attributes.

## Memory

### Pre-firmware 7.7.0 Partition

Memory availability and usage are unchanged until you update firmware to version 7.7.0 or newer.

### V0 Partition (Firmware 7.7.0 or newer) and V1 Partition (Firmware 7.7.0 or newer)

| Size limit with FW version < 7.7.0 | New size limit after upgrading to FW version >= 7.7 |
|------------------------------------|-----------------------------------------------------|
| 2 MB                               | 4 MB                                                |
| 16 MB                              | 32 MB                                               |

| Size limit with FW version < 7.7.0 | New size limit after upgrading to FW version >= 7.7 |
|------------------------------------|-----------------------------------------------------|
| 32 MB                              | 64 MB                                               |

Example after mid-size update:

```
Partition Storage:
 Total Storage Space: 3306327
 Used Storage Space: 0
 Free Storage Space: 3306327
 Object Count: 0
 Overhead: 15560
```

In summary, if you could store X-number of a given size of keys on your partition or HSM, then you can still store them all after 7.7.0 f/w update. The increase, at each allotment level was chosen to accommodate increased partition overhead and object size changes, plus some extra just in case (see \* at the bottom of this page).

## Behavior at key level

### Pre-firmware 7.7.0 Partition

Key object characteristics and behavior are unchanged until you update firmware to version 7.7.0 or newer.

### V0 Partition (Firmware 7.7.0 or newer) and V1 Partition (Firmware 7.7.0 or newer)

Some key types and algorithms might have constraints on the allowed uses of some older key and algorithm types and sizes, due to changes in the security and threat environments over time.

Check the latest mechanism summary tables in the SDK.

## PPT (partition policy template)

### Pre-firmware 7.7.0 Partition

**partition showPolicies -exportTemplate** generates a template file containing current policy settings

**partition init -label <label> -applytemplate <template file>** applies an existing template with the contained policy settings

### V0 Partition (Firmware 7.7.0 or newer)

Both commands behave the same as in previous versions. V0 partitions have some policies that do not exist in pre-7.7.0 partitions. As long as none of the policies in your template conflict with the state of a new policy, your pre-existing templates should work correctly. Any policy that is not mentioned in a template is set to its default value when the template is applied.

If there is a mismatch between template policies and the default values of newer or dependent policies, then the attempt to apply the old policy would fail with `CKR_FAILED_DEPENDENCIES`.

You have the option to edit a policy file before applying it, to add newer policies.

### **V1 Partition (Firmware 7.7.0 or newer)**

The default for new partition creation with firmware 7.7.0 (or newer) is a V0 partition. You could apply your PPT to creating a V1 partition only by pre-editing the policy template file to include setting policy 41 to a value of 1.

See also the lists of dependencies below the table at ["Partition Capabilities and Policies" on page 272](#).

## Per-key Authorization

### **Pre-firmware 7.7.0 Partition**

This is a new feature with firmware 7.7.0 and has no bearing on partitions at earlier firmware versions.

### **V0 Partition (Firmware 7.7.0 or newer)**

Partition Policy 40 Enable Per-key Authorization Data defaults to 0 (zero, or off) for V0 partitions, and cannot be turned on.

### **V1 Partition (Firmware 7.7.0 or newer)**

Partition Policy 40 Enable Per-key Authorization Data defaults to 1 (one, or on) for V1 partitions, and can be turned off for performance.

Relevant keys have attributes that allow HSM owner to provide individual users access to specific keys for Sole Ownership and Control, such as in Remote Signing and Sealing applications.

## Multi-factor authentication (PED-auth)

### **Pre-firmware 7.7.0 Partition**

Behavior of partitions at earlier firmware versions continues as-is (except see exceptions in next paragraph, if PEDs are updated).

### **V0 Partition (Firmware 7.7.0 or newer) and V1 Partition (Firmware 7.7.0 or newer)**

- > Old-series PEDs (firmware 2.6.x through 2.7.2, PED powered by power block) have an upgrade path to PED version 2.7.4.
- > New-series PEDs (firmware 2.8.x, PED is USB-powered) have an upgrade path to PED version 2.9.0.
- > When an HSM is at firmware version 7.7.0 or newer, it verifies that any connecting PED is at PED firmware 2.7.4 or firmware 2.9.0, respectively, or the HSM refuses the connection and issues an error.
- > When updating pre-7.7.0 PED-auth HSMs, at least one PED must be updated first, so that it remains possible to authenticate to roles on the HSM before/during/after the HSM update.
- > An updated PED can function
  - with older HSMs (HSM f/w 5.x and 6.x) that will not be updated with the new PED communication protocols, or
  - with earlier f/w 7.x HSMs that have yet to be updated, or
  - with f/w 7.7.0 and newer HSMs that have been updated for compliance with eIDAS/Common Criteria and NIST 800-56A standards.
- > For Remote PED operation,

- any blank RPK must first be provisioned with new Critical Security Parameters (CSP) via a local PED connection;
  - the content of a previously provisioned orange Remote PED Key (RPK) with old CSP must be migrated to new CSP.
  - When the ped vector init' command raises the PED prompt about "reuse an existing keyset?" will lead to RPK migration (old to new).
- > For Local PED, the local-connection handshake is now similar to that being used for updated, improved-security connections with Remote PED.

## Client software interaction

### Pre-firmware 7.7.0 Partition

Newer client software can include commands and options that are not applicable to partitions older-firmware. HSMs.

### V0 Partition (Firmware 7.7.0 or newer)

Older client software (example 7.4) can create only a V0 partition on an HSM with firmware 7.7.0 or newer (see \*\* at the bottom of this page).

### V1 Partition (Firmware 7.7.0 or newer)

Older client software (example 7.4 or 10.2.0) cannot create a V1 partition on an HSM with firmware 7.7.0 or newer.

Similarly, if a V1 partition is created on a 7.7.0 (or newer) Network HSM appliance and linked to an older Client, the client can see the remote partition, but cannot initialize or use the V1 partition. (Expect error CKR\_ACCESS\_ID\_INVALID)

Client must be version 10.3.0 or newer to create and work with V1 partitions (see \*\* at the bottom of this page).

## HA (client mediated)

### Pre-firmware 7.7.0 Partition

HA behaves as it always has, for pre-7.7.0 HSMs.

### V0 Partition (Firmware 7.7.0 or newer)

Generally as-is (backward compatible) except for any provisos around permissibility of certain mechanisms and key sizes, such as in FIPS mode, and the usual considerations where an HA group should have all members at the same firmware .

Migration must be done via G5 or G7 Backup HSM while any application partitions on an HSM being updated to firmware 7.7.0 (or newer) must be removed from any HA group, at the time. The partitions can become members of HA groups after all are at the newer version.

Key/object replication among HA group members continues to use cloning.

### V1 Partition (Firmware 7.7.0 or newer)

With V1 partitions, HA must function with SKS as the method of object / key replication among members, rather than cloning. Because this type of HA is client-mediated, you need Luna Client 10.3.0 or newer.

### HA Indirect Login

This type of HA is set up and managed by means of the HA Indirect Login API (a.k.a. "roll your own HA"), and does not rely on the Client.

### Pre-firmware 7.7.0 Partition

HA behaves as it always has, for pre-7.7.0 HSMs (see ["High Availability Indirect Login Functions Prior to HSM Firmware 7.7" on page 1](#) ).

### V0 Partition (Firmware 7.7.0 or newer) and V1 Partition (Firmware 7.7.0 or newer)

For adjustments to API and behavior, see ["HA Indirect Login \(firmware 7.7.0 and newer\)" on page 1](#)

### Functionality Modules (FMs)

#### Pre-firmware 7.7.0 Partition

FM behavior is as previously, for pre-7.7.0 HSMs.

#### V0 Partition (Firmware 7.7.0 or newer) and V1 Partition (Firmware 7.7.0 or newer)

*Backup HSM (G5) at firmware 6.28 - FM-vs-non-FM support*

|                        | to HSM FW <= 7.4 FM | to HSM FW <= 7.4 non-FM | to HSM FW 7.7 V0 FM | to HSM FW 7.7 V0 non-FM | to HSM FW 7.7 V1 FM | to HSM FW 7.7 V1 non-FM |
|------------------------|---------------------|-------------------------|---------------------|-------------------------|---------------------|-------------------------|
| From HSM FW 7.4 FM     | yes                 | no                      | yes                 | yes                     | yes                 | yes                     |
| From HSM FW 7.4 non-FM | no                  | yes                     | no                  | yes                     | no                  | yes                     |

"yes" indicates a supported backup/restore path

### Partition Roles

#### Pre-firmware 7.7.0 Partition

Roles and their behavior remain as-is for pre-7.7.0 HSMs.

#### V0 Partition (Firmware 7.7.0 or newer)

As in pre-7.7.0

**V1 Partition (Firmware 7.7.0 or newer)**

V1 partitions add the Limited Crypto Officer role for Per-Key Authorization operations see saw

**Backup/Restore**

**Pre-firmware 7.7.0 Partition**

Backup and restore remain as-is for pre-7.7.0 HSMs.

**V0 Partition (Firmware 7.7.0 or newer) and V1 Partition (Firmware 7.7.0 or newer)**

Use of Luna Backup HSM (G5) with V0 or V1 partitions implies Backup HSM firmware 6.28 and Luna Client 10.3 (or newer). Both the Client and the RBS server version must be aligned -- that is, the RBS server must be installed from the 10.3 Client or newer, replacing any previous RBS server.

A Luna Backup HSM (G5) with firmware earlier than 6.28.0 can restore onto a partition in a firmware-7.7.0 (or newer) HSM, but the Luna Backup HSM (G5) must be at firmware 6.28.0 in order to properly backup from a version 7.7.0 (or newer) application partition. In other words, if your Luna Backup HSM (G5) is not updated, then its contents can be considered a backup for key-migration, but not a production backup for firmware 7.7.0 (and newer) HSM partitions.

If there is a need to maintain an older version of client library for your main application and to use Luna Backup HSM (G5) firmware 6.28.0 for backup/restore purposes, then you must have a separate workstation dedicated for running the RBS server from Luna Client 10.3.

Even if RBS service is not required, you would still need the separate workstation to run lunacm to take advantage of Luna Backup HSM (G5) firmware 6.28.0.

**Luna Backup HSM (G5) at firmware 6.28.0 used locally with Luna Network HSM appliance with software <=7.4**

|                       | to HSM FW<br><= 7.4 | to HSM FW<br>7.7 V0 | to HSM FW<br>7.7 V1 |
|-----------------------|---------------------|---------------------|---------------------|
| From HSM<br>FW <= 7.4 | not recommended     | supported           | supported           |

See also the Functionality Module-related G5 Backup concerns, above on this page.

**NOTE** To perform backup operations on HSM firmware 7.7.0 or newer (V0 or V1 partitions):

- > Luna Backup HSM (G7) requires minimum firmware version 7.7.1
- > Luna Backup HSM (G5) requires minimum firmware version 6.28.0

You can use a Luna Backup HSM with older firmware to restore objects to a V0 or V1 partition, but this is supported for purposes of getting your objects from the older partitions onto the newer V0 or V1 partitions only.

V0 and V1 partitions are considered more secure than partitions at earlier firmware versions - any attempt to restore from a higher-security status to lower-security status fails gracefully.

SMK backup for appliance is supported only with local connection.



The Limited Crypto Officer role does not do cloning, and therefore cannot transfer the current partition's SMK to a Backup HSM for SKS backup.

## STC (Secure Trusted Channel)

### Pre-firmware 7.7.0 Partition

STC remains as-is for pre-7.7.0 HSMs.

### V0 Partition (Firmware 7.7.0 or newer) and V1 Partition (Firmware 7.7.0 or newer)

- > 7.7.0 (and newer) version of STC is supported ["Creating an STC Connection" on page 104](#)
- > 7.7.0 appliance software and HSM firmware (or newer) and 10.3.0 Client software are required
- > previous version STC is not supported for 7.7.0-and-newer systems,
- > if STC was configured on your system, it must be shut down before update to HSM appliance software and firmware 7.7.0 or Client 10.3.0 (or newer) - disabling policy 37 is a destructive action, so keys must be backed up first
- > after the updates are completed, STC can be configured again.

-----

(\* If you had [say] thousands of very small keys, you would notice a definite increase in the partition space taken by those keys after update.

If you had [say] 100 big keys or fewer in the partition, you would barely notice a change in required space, as the overhead [new attributes] per key is proportionately much smaller against an individual large key. )

(\*\*Luna Client software has historically been named/numbered for the associated HSM version. The Client numbering has been restarted at 10.x to decouple from specific firmware and software versions. )

## Converting pre-7.7.0 partitions to V0, or V0 partitions to V1

---

**CAUTION!** Be sure to back up any important keys and objects.

### If your application partition is a member of an HA group...

... there are some additional considerations. See ["Updating Luna Network HSM HA Group Members to Luna 7.7.0 or Newer" on page 373](#).

### If your application partitions have been using STC...

...(secure trusted channel) to secure the client-to-network-HSM-partition connection, see ["Updating Luna Network HSM with STC Partitions to 7.7.0 or Newer" on page 123](#).

### Guidelines and Tips when partitions are part of an HA group

Refer to ["General guidelines for updating or converting of HA member partitions" on page 376](#)

## To convert from pre-7.7.0 to V0

If you have application partitions on your pre-firmware 7.7.0 HSM that you wish to convert to V0, do the following:

1. Update at least one client computer to Luna HSM Client version 10.3.0 or newer. The newer client can readily handle functioning with both current and older HSM firmware and Network HSM appliance software. To update an existing client installation, simply uninstall it, and then install the newer version -the configuration and certificate files are preserved.
2. In the case of a Luna Network HSM appliance, update the appliance software to version 7.7.0 or newer - follow the steps at "[Updating the Luna Network HSM Appliance Software](#)" on page 1.
3. Update the HSM firmware. Either update to the ready version that accompanied the HSM software, or acquire, from the Support Portal, and install the latest 7.7.0-or-newer firmware that has been FIPS-validated (whichever is desired) - [Updating the Luna HSM Firmware](#).
4. As part of the firmware update process from pre-7.7.0 firmware to 7.7.0 (or newer), any existing partitions are converted to V0, which adds key attributes where appropriate, and increases the HSM memory and the partition size to accommodate the new overhead requirements.

## To convert from V0 to V1

1. Have the chosen partition visible in lunacm.
2. Select that partition with the lunacm command **slot set -slot <slot number>**
3. [Optional] Show the current partition policy values and verify that policy 41 is set to version 0, **partition showpolicies**
4. Log into the partition as the Partition Security Officer with **role login -name po**
5. Change the value of policy 41 to version 1, with **partition changepolicy -policy 41 -value 1**

## To convert from V1 to V0

1. Backup any valuable keys or objects.

**CAUTION!** This operation, going from V1 back to V0, is destructive. All objects on the partition are destroyed, as well as the SMK(s). If any valuable objects were created and archived from a version one (V1) partition, then they must have been SKS-stored off the HSM, and the SMK that encrypted those objects must be preserved on a Backup HSM or in another partition (that remains at V1), if those objects might ever be needed in future.

If no valuable SKS blobs have been encrypted by the partition's current SMK, then there is no need for backup.

2. Have the chosen partition visible in lunacm.
3. Select that partition with the lunacm command **slot set -slot <slot number>**
4. [Optional] Show the current partition policy values and verify that policy 41 is set to version 1, **partition showpolicies**
5. Log into the partition as the Partition Security Officer with **role login -name po**
6. Change the value of policy 41 to version 0, with **partition changepolicy -policy 41 -value 0**

# Scalable Key Storage (SKS)

## What is Scalable Key Storage?

Scalable Key Storage (or SKS) is virtually unlimited secure storage and handling of your sensitive keys.

By default, keys have resided in HSM hardware for Luna HSMs. This remains true, by default, with the introduction of HSM firmware 7.7.0. However, firmware 7.7.0 (and newer) adds key export flexibility to expand the Luna HSM's assurance boundary, to encompass much greater numbers of keys than the internal capacity of an HSM.

### Keys secure anywhere, the SKS eIDAS model

Beginning with firmware 7.7.0, all partitions created with the Version 1 (V1) option use Scalable Key Storage (SKS). When a partition is created, it is given a unique SKS Master Key (SMK). SMKs can be cloned from partition to partition, within or across HSMs, or to-and-from Backup HSMs. Other keys and crypto objects are not cloned (for backup/restore, HA, etc.) and instead are encrypted by the SMK for extraction / insertion operations. Again, this applies to V1 partitions. ( See ["What are \"pre-firmware 7.7.0\", and V0, and V1 partitions?\" on page 126](#) )

SKS is based upon a model where keys generated on the HSM are securely extracted as encrypted SKS objects and inserted back into the HSM when cryptographic operations are to be performed with those keys. Similarly, when a unique key encrypts data, the data and the key can be stored as an encrypted **binary large object** (blob) up to 64KB in size, that can be decrypted only within the HSM. This means that any applications that interact with the HSM must be 'SKS aware' and use the SKS API functions to work with SKS objects.

If the HSM is upgraded from an earlier HSM firmware version to firmware 7.7.0 or newer, then any existing partitions become version zero (V0). Similarly, if you create a new partition on a firmware 7.7.0 (or newer) HSM, with the default "-version 0" option, it becomes a V0 partition. A V0 partition retains compatibility with older partitions and applications that rely on cloning (secure copying/moving of objects between HSMs or HSM partitions or Backup HSMs, also known as Keys Always in Hardware) while benefiting from fixes and security updates that come with the new firmware, but with no access to the newer eIDAS-mandated features.

If you create a new partition in an HSM with firmware 7.7.0 or newer, and select the V1 option ("-version 1"), then the new partition is version one (V1) and gets a unique SMK and uses SKS (rather than cloning) to replicate keys for HA or to Backup and Restore. The partition also engages Per Key Authorization and other eIDAS related features, but is incompatible with V0. You can also update a V0 partition to V1 while retaining existing objects, but not the direction.

**NOTE** If you have updated an HSM, with existing partitions, from pre-7.7.0 firmware to firmware 7.7.0 or newer, then

- > your existing partitions become version zero (V0),
- > your content is preserved,
- > your applications function with those partitions as they always did, and
- > HA replication and backup/restore operations are accomplished with cloning.

When creating *new* partitions on an upgraded HSM, the default is to invoke V0 as well, and such new partitions will work just like your old partitions with your applications and processes. These will enjoy the fixes and security updates that come with the newer firmware, but *will not have access* to the features that require V1.

You do not need anything on the pages in this SKS section *until* you

- convert an existing V0 partition to V1 or
- create new version one (V1) partitions

which will be using the new cloning protocol and Scalable Key Storage (SKS).

Here is what you will find in the pages of this section:

["What is Scalable Key Storage?" on the previous page](#)

["When to use SKS \(Use Cases\)" on the next page](#)

["The SKS model - how it works " on page 142](#)

- ["How does SKS work? " on page 143](#)
- ["Limitation and scalability " on page 144](#)

["Characteristics of the SKS Implementation " on page 144](#)

- ["Characteristics and Implementation Notes " on page 144](#)
- ["Functional Notes" on page 145](#)
- ["SMK Locations in a Partition " on page 145](#)

["High Availability and SKS" on page 146](#)

["Preparing and Administering SKS Partitions " on page 146](#)

- ["Provisioning SKS" on page 147](#)
- ["Replicating the SMK to another SKS Partition" on page 147](#)
- ["Backing up the SMK" on page 148](#)
- ["Restoring the SMK from Backup" on page 148](#)
- ["Preparing to use SKS" on page 148](#)

["Using SKS" on page 149](#)

- ["Using SKS - options" on page 149](#)
- ["API" on page 149](#)
- ["ckdemo example" on page 150](#)
- ["Java Sample" on page 151](#)

- "High Availability" on page 151
  - "Constraints on SKS HA" on page 151
  - "Replicating the SMK to all group members " on page 152
  - "When NOT to address the virtual slot" on page 153

"SKS Backup and Restore" on page 153

- "Constraints on SKS Backup and Restore" on page 154
- "Backup the SKS Master Key (SMK)" on page 154
- "Restore an SKS Master Key (SMK)" on page 155
- "Troubleshooting SKS Backup and Restore " on page 157

"SMK Rollover" on page 158

"Migrating Scalable Key Storage (SKS) " on page 159

- "Cloning the SKS Master Key (SMK)" on page 160
- "SKS Blob Migration" on page 162

## When to use SKS (Use Cases)

---

### When would it be appropriate to use SKS?

Use SKS when you need to handle greater numbers of keys and objects than can be stored within the HSM, and you want to employ methods more secure than wrap-off / wrap-on. You would also use it when needed to comply with a regulatory regime like eIDAS.

Any application where large numbers of very sensitive keys or records must be protected with the highest possible security, while remaining available and accessible to authorized users and applications, is a candidate for the Luna HSM with Scalable Key Storage. The SKS method - in contrast with merely wrapping-off/unwrapping-on - is needed when the HSM must be the assurance boundary for the keys. If it is permissible for the key material to originate outside the assurance boundary, or to reside outside the assurance boundary, then the extra security of SKS is not required.

A general use case for SKS is storing encrypted keys in external databases.

- > Generate keys inside the HSM.
- > Using the SIMExtract API, extract the encrypted keys and store them in external databases and delete the original keys inside the HSM.
- > Insert individual encrypted keys back into the HSM when you need to use them for cryptographic operations inside the HSM.

One example might be the creation and use of electronic signatures (for natural persons) or electronic seals (for organizations) for remote signing (RSS). The signatures or seal key materials are created within the HSM, extracted (not wrapped) in strongly encrypted form that preserves attributes, and stored in a repository. When they are needed, they are found in the repository by the managing system, inserted into the HSM for

decryption by a master key that never resides outside an HSM, then used for signing or sealing respectively, and discarded from the HSM (the encrypted versions remain stored in the repository for the next time they are needed).

Another example might be a database of customers, with their contact and shipping information, credit-card information, history of purchases, current/recent browse interests on your commerce site, etc. All of that is likely to be sensitive information protected by regulations and by your own published privacy policies. In this case, the primary concern is privacy of data.

A third example might be a government database of land ownership, including detailed and official property descriptions, current ownership with identifying details, history of title transfers, subdivisions, legal rulings and encumbrances (such as rights of way and covenants), liens, and so on. In this case, the data is meant to be publicly viewable, but its integrity against unauthorized change is paramount.

## Security consideration

Various models exist in the industry for handling of huge numbers of sensitive keys and objects. An important consideration is the manner in which the keys and objects are handled.

| Method             | Security                                                                                                                                                                                                                                                                                                                                             |
|--------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Wrap-off/wrap-on   | <p>Keys and objects can have unknown, uncontrolled origin, potentially outside the assurance boundary.</p> <p>Keys and objects can potentially be accessed outside the HSM, made available and used externally, in potentially unsafe environments. .</p> <p>Keys can have security attributes stripped.</p>                                         |
| SKS extract/insert | <p>The history of keys and objects is known, controlled, auditable.</p> <p>Keys and objects remain within the security and access envelope of the HSM. The master key never exists outside a Luna HSM, and all extracted keys and objects must be inserted back into the HSM at time of decryption and use.</p> <p>Keys retain their attributes.</p> |

## SKS model

On this page:

- ["The SKS model - how it works " below](#)
- ["How does SKS work? " on the next page](#)
- ["Limitation and scalability " on page 144](#)

### The SKS model - how it works

In an SKS model, in compliance with relevant standards, an application maintains thousands or millions of encrypted objects as records in a repository (such as a database, file system, cloud storage, etc.). The repository might have each record/object encrypted with a unique key. Examples of applications might include Remote Signing identities (Common Criteria PP 419221-5 use case). The salient points, for SKS, are that:

- > encryption and decryption of objects must take place in the HSM;
- > more individual object-encryption keys are needed by the application than can be accommodated by the internal capacity of any HSM;
- > records or objects, and the keys that encrypt them, do not exist in-the-clear - both the record (data object, ID, etc.) and its encrypting key are stored in encrypted form;
- > keys that encrypt objects or signatures must have originated within the assurance boundary and are only ever decrypted within the assurance boundary;
- > objects extracted from a current-version HSM cannot be inserted into older version HSMs with known vulnerabilities
- > objects extracted from an HSM with Functionality Modules disabled cannot be inserted into an HSM with FM's enabled (including via backup/restore operations) - security rules prevent moving keys from a more-secure to a less-secure environment.

### How does SKS work?

A key is created in an HSM partition at the direction of an application.

It might be intended as an ID for purposes of signing documents and verifying by private persons, or for sealing of documents and records by organizations.

It might be intended to encrypt records stored in an external database (perhaps customer-identifying records, perhaps medical records, perhaps supply-chain information, or other uses that require privacy and controlled access).

- > Each record-encrypting key, or ID key, when not in immediate use inside an HSM is itself encrypted for extraction by an extraction/insertion key derived (in compliance with NIST SP800-108) from a master encryption key that never leaves the HSM; this is the SKS Master Key, or SMK.
- > From the application's perspective, the data record, or the key/cert-as-ID, emerges from the HSM uniquely encrypted as a secure SKS blob (**binary large object** up to 64KB) that remains within the HSM's security and access envelope, so it can be safely stored anywhere.
- > The operations that an application might perform are:
  - creating an identity or a record or data object
  - acquiring a suitable key (SKS key) for encrypting that record or data object by either
    - requesting a new object-encryption key (new SKS key) to be generated by the HSM, or
    - providing an already existing object-encryption-key (SKS key) for the HSM to use
  - encrypting that ID or object with the new SKS key, (or with the pre-existing, supplied SKS key, which must first be inserted and decrypted for use by the HSM)
  - storing the encrypted record or key within the repository
  - retrieving the encrypted record or key at a later time (when called by the application)
  - inserting/decrypting the SKS blob into the HSM, using the SKS Master Key (SMK)
  - using the decrypted key
    - to sign or seal documents or transactions in the case of RSS, or

- to further decrypt a database record for reading or editing and then re-encrypting the record if it changed and sending the re-encrypted changed record back to storage
  - deleting / destroying the material from the HSM, once it is not needed (the encrypted SKS blob still exists in the external repository, for the next time it is required)
- > The application is responsible for the storage and availability of the SKS object in the repository of choice (database, file system, directory, NAS, cloud, etc.).

It is possible to create data objects to store any kind of data in an HSM partition, SKS blobs included (which is essentially what is done if you choose to archive SKS objects in a Backup HSM), but that is not the envisioned general workflow. Instead, a practical workflow is assumed to include backing up SMKs, but not SKS blobs, since the latter are already securely encrypted and can be stored anywhere that is reasonably secure, and in numbers far greater than the capacity of any HSM. However, we cannot anticipate all use-cases, so the onboard storage option exists.

Optionally, such as in the case of Trust Service Providers, during the SKS object creation process, authentication can be added such that a password must be provided before the keys in an SKS object can be used. SKS objects use 256-bit AES-GCM encryption for confidentiality and integrity protection. SHA-512 is also used for further integrity protection. See "[Per-Key Authorization \(PKA\)](#)" on page 164.

### Limitation and scalability

Because the SKS objects are stored external to the HSM (but must be individually inserted back into the HSM before use), there is *no capacity limitation* from an HSM perspective. The only scalability limitation would be based upon the number of SKS operations to be performed simultaneously (that is, SKS object creation/extract/insert, and resulting cryptographic operations).

## Characteristics and Implementation Notes

On this page:

- "[Characteristics and Implementation Notes](#)" above
- "[Functional Notes](#)" on the next page
- "[SMK Locations in a Partition](#)" on the next page

### Characteristics of the SKS Implementation

- > The SKS feature is implemented at the application partition level; this differs from the older SKS protocol that was applied HSM-wide.
- > The SKS mechanism complies with the per-key authorization requirements of Common Criteria PP 419221-5 ( "[Per-Key Authorization \(PKA\)](#)" on page 164 ).
- > The cryptographic mechanisms employed by SKS comply with the FIPS 140-2 and PP 419221-5 standards ( "[Secure External Scalable Key Storage \(SKS\) Extensions](#)" on page 1 ).
- > A migration path is available for customers using the Luna HSM firmware 6 SKS protocol, such that existing customer applications continue to work against the SKS implementation.
- > For certification requirements and/or security best practices, the following are not allowed:



- The SKS implementation prevents objects that are extracted from an HSM with firmware 7.x being inserted into an older version of the HSM that might have known vulnerabilities.
- The SKS implementation prevents objects that are extracted from an HSM that has Functionality Modules (FMs) *disabled*, from being inserted into an HSM that has FMs *enabled* (or ever had FMs *enabled*) - doing so via a backup HSM is also prevented.

## Functional Notes

SKS supports the following functionality:

- > You can extract all key objects within a given partition by specifying an empty list on the input. Otherwise, specify only individual objects that you wish to extract at one time.
- > You have the option to impose/require two possible authentication methods when extracting key objects:
  - None (no extra authentication data)
  - Password (MofN supported)
- > The AES-GCM algorithm is used for encryption of objects during the creation of SKS blobs (extraction from the partition) or decryption upon insertion of an external SKS blob into the partition.
- > You can see, and practice, examples of such usage in the `ckdemo` utility :
  - ["OFFBOARD KEY STORAGE Menu Functions" on page 1](#)

## SMK Locations in a Partition

Each SKS-capable partition supports several types of SMK, each with its own location and limitations within the partition.

The **Primary SMK**, generated at partition creation time, or replaced via **partition smkclone** command from another partition, resides in the Primary SMK location in the partition, and is used for extraction and insertion operations. Only the firmware 7.x primary SMK can be used for extraction. No path is allowed for extraction to older-version HSMs and partitions.

The **Rollover SMK** location holds the replaced primary, when **partition smkrollover start** command creates a new primary SMK. The rollover SMK is retained while SMK rollover is taking place, to allow all SKS blobs that were encrypted/extracted with the old SMK to be brought back into the HSM partition so that they can be re-extracted with the new primary SMK. When **partition smkrollover end** signals the completion of the rollover operation, the rollover SMK is deleted and the new Primary SMK remains.

The **FM SMK** location is specifically for transfer from an FM-enabled partition to an FM-never-enabled partition. That is, a **partition smkclone** command from an FM-enabled HSM partition places the source Primary SMK into the FM SMK location of the target partition. This ensures that key material can be transferred from FM-enabled partitions to FM-never-enabled partitions. It is not permitted to move key material from FM-never-enabled partition to FM-enabled partition, because a Functionality Module could extract in plain text. Similarly, there is no FM SMK rollover location.

The **Firmware 6 SMK** location can contain an SMK from a firmware 6.x HSM (if one has been cloned in) for the purpose of inserting SKS blobs that were extracted from a firmware 6.x partition. After insertion of such older blobs, the key material is extracted as a new firmware 7 SKS blob, encrypted via the partition's primary SMK. Whenever a partition is on the receiving end of a **partition smkclone** operation, any contents of the primary and non-primary locations from the source partition overwrite their equivalent locations in the target partition.

## High Availability and SKS

To address performance and availability requirements SKS supports high availability configurations similar to Luna HSM Cloning models, with some minor differences. High availability and load balancing is implemented in the Luna HSM Client software and is completely transparent to the application, in that the application is configured to use a virtual slot and not a physical slot on the HSM.

One difference, from cloning HSMs in HA configuration is that, for SKS HA, the **hagroup addmember** command clones the SMK from the initial SKS application partition to all other group member partitions as they are added. Thereafter, your application deals with the HA virtual slot, and HA operation is automatic.

**NOTE** Back up the SMK in any partition where that SMK is likely to be overwritten, if that SMK is ever likely to be needed to insert (decrypt) any SKS blobs.

If an SMK is cloned from one partition to another (such as must be done when adding members to an HA group), a pre-existing SMK already in the target partition is overwritten by the incoming SMK. Any blobs still encrypted with it are lost, unless a backup exists.

**NOTE** If a remote partition is involved (Network HSM) on either side of the SMK cloning operation, the HSM that contains the remote partition must have Network Replication enabled. See "[HSM Capabilities and Policies](#)" on page 1 "Policy 16 - Allow network replication".

When the application needs to perform a cryptographic operation, it employs the SKS API call, which imports an SKS object into the HSM. In an HA configuration, the Luna HSM Client also replicates the SKS blob to all HSMs that have been included in the defined HA group (by performing `sksextract` from the source partition and `skinsert` into the target partition as a single, combined operation, repeated for each), unless HA synchronization is turned off. When the application requests the "HSM" to perform a cryptographic operation (sign, encrypt, decrypt, etc.) the Luna HSM Client load balances the request to the application partition that is available, in essence making the SKS operation stateless. The SKS operation succeeds because all partitions in the HA group have a copy of the imported SKS object.

Replication of objects in HA is accomplished by SKS feature's `SIMextract` and `SIMinsert` in one call, transparently.

**TIP** If your primary use-case is to insert a key and use it for one signing operation, then consider using the multisign API for better performance with SKS under HA, since invoking multisign would use the key on just the one physical partition, and would avoid the overhead of having the inserted key replicated unnecessarily to other HA group members.

**NOTE** HA failover is not supported in the case of member failure during a `SIMinsert`, `SIMextract`, or `SIMMultisign` operation.

## Preparing and Administering SKS Partitions

On this page:

["Provisioning SKS" on the next page](#)

- ["Replicating the SMK to another SKS Partition" below](#)
- ["Backing up the SMK" on the next page](#)
- ["Restoring the SMK from Backup" on the next page](#)
- ["Preparing to use SKS" on the next page](#)

## Checklist

The following subsections describe briefly what you need

- > to set up one or more SKS partitions ready for use,
- > to backup and restore SKS Master Keys (SMK) from-and-to the SKS partition, and
- > to directly replicate the SMK from one SKS partition to another for High Availability operation.

Cross-reference links are provided to each topic or section, containing explicit instructions for each task.

## Provisioning SKS

- > You need at least one Luna Network HSM at appliance software version 7.7.0 or newer and HSM firmware version 7.7.0 or newer, or Luna PCIe HSM at firmware version 7.7.0 or newer.
- > If you already have an older 7.x HSM, download and install the updates from the [Support Portal](#).
- > Install a suitable Client software that includes a version of the lunacm tool that supports the "partition smkrollover" commands - this ensures that the associated library has the updated SKS capabilities and is also able to handle migration from legacy SKS instances
- > Follow the instructions at the beginning of ["Preparing to use SKS" on the next page](#) to get the appliance installed and network connected
- > If you plan to use an HA group, then repeat the above process with the second Network or PCIe HSM, and again with any additional active or standby members.

## Replicating the SMK to another SKS Partition

**Stand-alone** - If you are using a *single HSM* with your application, you should have at least one backup copy of the SMK (for each partition) so that any SKS blobs encrypted by that SMK are recoverable in case of loss or damage to the original HSM or partition.

- > proceed to ["Backup the SKS Master Key \(SMK\)" on page 154](#).

**HA group** - If you are using an *HA group* with your application, then initially, each member has a unique SMK created when its SKS partition is created. For HA operation, the **hagroup addmember** command replicates the desired SMK from the initial member to all additional members of the group. This means that, in order for a partition to take part in HA operation as the second or later member, its original SMK is overwritten by the SMK of the first member of the group.

- > Safeguard the desired SMK by backing it up to a Backup HSM before going further. See ["SKS Backup and Restore" on page 153](#).

**NOTE** If an SMK, already existing on a partition, has ever been used to encrypt an SKS key or objects, then you must backup the existing SMK before replacing/overwriting it, if you wish to ever retrieve the previously encrypted SKS key and objects.

- > Follow the instructions for using the **partition smkclone** command in ["High Availability and SKS" on page 146](#).

### Backing up the SMK

Always ensure that you have safeguarded any important SMK (one that has been used to encrypt key material for export from the HSM) by backing it up to a Backup HSM partition before you perform any action that might destroy that SMK (such as cloning a different SMK to the current HSM, or restoring a different SMK from a Backup HSM partition).

- > To backup, see ["Backup the SKS Master Key \(SMK\)" on page 154](#).

### Restoring the SMK from Backup

When you wish to use the SKS partition to encrypt objects or decrypt objects with an SMK other than the SMK that resides in the current partition, you must restore from a Backup of the desired SMK to overwrite the current SMK in the current partition. If the current SMK (before restoring from archive) is valuable, then back it up first before restoring a different SMK to overwrite the current one.

- > To restore, see ["Restore an SKS Master Key \(SMK\)" on page 155](#).

## Preparing to use SKS

Perform all the steps to install and configure a Luna HSM, as described at ["Installing and Configuring Your New Luna Network HSM" on page 1](#).

1. If your HSM is not already at firmware version 7.7.0, follow the instructions in the 7.7.0 Customer Release Notes, to securely copy the Release 7.7.0 Appliance Software Update package to the appliance, and perform the software and firmware update.

**NOTE** To update an HA group to firmware 7.7 or newer, all the *non-primary partitions* must be updated *first*, to ensure that the key objects from the firmware 7.7-or-newer primary can still move to the non-primaries through key cloning. *Then* the primary member can be updated.

2. When you reach the steps to create an application partition, ensure that it is created as the default version one (V1), which is necessary for SKS operation.

**NOTE** The SKS Master Key (or SMK) is created when the partition Crypto Officer logs in. For security reasons the SMK is not made visible in output of the usual commands that show objects on an HSM partition (lunacm:>**partition contents** and lunash:>**partition showcontents**).

3. Go to ["Using SKS" on the next page](#) to continue with SKS.

## Using SKS

On this page:

"Using SKS - options" below

- ["API" below](#)
- ["ckdemo example" on the next page](#)
- ["Java Sample" on page 151](#)
- ["High Availability" on page 151](#)
  - ["Constraints on SKS HA" on page 151](#)
  - ["Replicating the SMK to all group members " on page 152](#)
  - ["When NOT to address the virtual slot" on page 153](#)

Logistical considerations for SKS operation include:

- > you must create a V1 partition before you can use the SKS functionality;
- > creating and logging into an SKS partition (as CO) creates a unique SMK in that partition, at the same time;
- > you have the option to use the SMK that is created with the partition, or you can overwrite that SMK with
  - an SMK that is restored from an SKS partition on a Backup HSM (with **partition archive restore**), or
  - an SMK that is cloned (with **partition smkclone**) from another partition (usually for purposes of HA operation);

**NOTE** Back up the SMK in any partition where that SMK is likely to be overwritten, if that SMK is ever likely to be needed to insert (decrypt) any SKS blobs.

If an SMK is cloned from one partition to another (such as must be done when adding members to an HA group), a pre-existing SMK already in the target partition is overwritten by the incoming SMK. Any blobs still encrypted with it are lost, unless a backup exists.

## Using SKS - options

Two approaches are available, to use SKS :

- > Use the API, where you have the ability to write or modify your applications:
  - Directly access the PKCS#11 C-language extensions that interact with the HSM.
 or
  - Use the provided Java toolkit.
- > Use a commercial, off-the-shelf Windows CNG application, mediated by the provided SKS Client Extension for Luna HSM KSP.

## API

Authorization forms currently supported are none, and password.

Export a key from a partition as an SMK-encrypted blob, using SIMExtract function

```

SIM_AUTH_FORMS = (CKA_SIM_NO_AUTHORIZATION,
 CKA_SIM_PASSWORD)
CK_RV CA_SIMExtract(CK_ULONG handleCount, CK_ULONG *handleList,

 CK_ULONG authForm, CK_ULONG authDataCount, CK_ULONG subsetRequired,

 CK_BYTE **authDataList,

 CK_BOOL deleteAfterExtract,

 CK_ULONG *pBlobSize, CK_BYTE *pBlob);

```

Import a previously extracted blob, using the SIMInsert function

```

CK_RV SIMInsert(CK_ULONG blobSize, CK_BYTE *pBlob,

 CK_ULONG authForm, CK_ULONG authDataCount, CK_BYTE **authDataList,

 CK_ULONG *pHandleListSize, CK_ULONG *pHandleList);

```

For further information, refer to the SDK Guide ( "[Secure External Scalable Key Storage \(SKS\) Extract / Insert](#) " on page 1 ).

## ckdemo example

1. Start by running ckdemo and executing **Open Session (1)** to the slot and **Login (3)** as **Crypto Officer**, giving the partition password.
2. Generate an AES key using **Simple Generate Key (45)** and keep track of the object handle for the generated key.
3. Execute **SIMExtract (105)**.
  - Enter the object handle for **Enter handle of object to add to blob** and then
  - Enter **0** to **end the list**.
  - Enter **1** for **Enter authentication form**.
  - Enter **1** for **number of authorization secrets (N value)**.
  - Enter **1** for **Enter subset size required for key use (M value)**.
  - Enter a password.
  - Enter **1** for **Delete after extract**.
  - The masked key is saved to **blobfile.sim**.
4. List all of the objects in the partition by running **Find object (26)** with option **All Standard Objects (6)**.
5. Execute **SIMInsert (106)**.
  - Enter **blobfile.sim** for **Enter filename with object to insert**.
  - Enter **1** for **Enter authentication form**.
  - Enter **1** for **Enter number of authorization secrets to be provided**.
  - Enter the password that was entered in the previous step.

6. List all of the objects in the partition by running **Find object (26)** with option **All Standard Objects (6)**. The key that was extracted should now be present in the partition.

**NOTE** The example above uses the password authentication form. Other authentication forms can be used.

## Java Sample

As a prerequisite, ensure that the **LunaProvider.jar** and **libLunaAPI.so** has been installed to your JDK.

1. Navigate to the directory that contains the java sample:

```
cd JavaSample
```

2. In the **SIMExtractInsert.java**, modify the **slot** and **hsmPass** variables appropriately.
3. Compile the sample using **javac**:
 

```
javac SIMExtractInsert.java
```
4. Run the sample using java.

## High Availability

Replication of objects in HA is accomplished by SIMExtract and SIMInsert in one call, transparently.

**TIP** Turn off HA synchronization for better performance if the inserted keys are to be used for single operations. An inserted key would be replicated to all HA group members even if it were to be used only by one member for (say) one signing operation.

If inserted keys are likely to be used for multiple load-balanced operations, then the overhead of replicating to all members is unavoidable and would be minimal in that context.

OPTIONS for HA Operation are:

- > Use with V0 partitions. The assumption is that you have existing partitions and application(s) that use those partitions in HA. Continue as you already do. Your pre-existing upgraded partitions, as well as any new partitions that you create with the V0 option will work as before.
- > Use with V1 partitions - all HA group members must be at V1, and your application must be SKS-aware, because only SMKs are cloned between V1 partitions; all other objects are extracted/inserted as SKS blobs.

## Constraints on SKS HA

HA for SKS requires that each member of the HA group must have the same SMK.

**NOTE** For HA environments, if you perform SMK rollover on a member, then the new SMK must be cloned to all members. However, database / repository update for rollover should be done by directly addressing the primary physical member, and *not* using the virtual slot (to avoid the performance penalty when keys inserted to the virtual slot during rollover would be propagated to all members before the re-extraction).

## Replicating the SMK to all group members

**CAUTION!** Each SKS partition contains a single SMK, and this operation overwrites the SMK in the target partition. Therefore, always ensure that the SMK in the target partition is **not** of any use, or that it has been backed up, before you perform **partition smkclone**.

These steps are performed from the lunacm utility in the client computer.

1. Use **slot set** to select one of the HSM partitions, with the desired SMK, as the current slot.

```
lunacm:> slot set -slot 0
```

```
Command Result : No Error
```

2. Log into the current slot as Crypto Officer.

```
lunacm:> role login -name Crypto Officer
```

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

```
Command Result : No Error
```

3. Use the **partition smkclone** operation to clone the desired SMK from the current slot SKS partition to another SKS partition in a named slot. The SMK from the source slot overwrites the SMK in the target slot. You are logged into the source partition, where you are launching this command, but not to the target partition; specify the password for the target partition.

```
partition smkclone -slot 1 -password userpin
```

```
Logging in to target slot 1
```

```
Cloning the SMK.
```

```
The SMK was cloned successfully.
```

```
Command Result : No Error
```

To verify that the SMKclone operation was successful, see below.

4. Repeat the previous step for any other HA group members, to ensure that all members share the same SMK.
5. Set HA-only mode for the group, so that your application sees only the HA virtual slot, and not any of the physical slots.

```
lunacm:> haGroup HAOnly -enable
```

```
Command Result : No Error
```

6. Note the number of the HA virtual slot. Your application will direct all operations to that slot.



## Verify SMKclone

If necessary, verify the success of the SMKclone operation as follows.

1. Create an object on the original HSM partition (for example, a keypair).
2. SIMExport the object from that original HSM and SIMInsert it into the second (target) HSM, using any of the methods (API, CKDemo, or Java, earlier on this page). If the importation is successful, then the SMK on the second HSM is the same as the SMK on the first, or source HSM.

### When NOT to address the virtual slot

As indicated above, blob insertion results in the inserted key being propagated to the other HA members.

However, key external storage database rollover *should not* be done over the virtual slot as this would cause the inserted keys to be propagated *before* the re-extraction, affecting performance. Ideally, the database update should be done by direct communication with the primary HA member.

## SKS Backup and Restore

On this page:

- ["Constraints on SKS Backup and Restore" on the next page](#)
- ["Backup the SKS Master Key \(SMK\)" on the next page](#)
- ["Restore an SKS Master Key \(SMK\)" on page 155](#)
- ["Troubleshooting SKS Backup and Restore " on page 157](#)

As described, the partition permanently stores the SKS Master Key (SMK) from the time of its creation when the partition is created. The application partition is intended :

- > to create encryption keys as session objects
- > to encrypt those keys with the SMK, for SKS extraction from the HSM
- > to extract those encrypted keys, as encrypted SKS blobs, for storage by your application, external to the HSM
- > to temporarily SKS insert (decrypt) blobs to make individual keys available for crypto operations within the partition
- > to use the decrypted key
  - to sign or seal documents and other digital objects, using the inserted key as a personal or organization identity, or
  - to encrypt data (records) for your external database, archive, cloud, or other repository, or
  - decrypt and modify such records before re-encrypting them to go back into your repository.

Therefore, it is not intended that objects other than the SMK be stored in the SKS partitions; however, you can do so if you wish, up to the limits of the partition capacity.

From HSM firmware 7.7.0 onward, SMKs are replicated (for HA) or are backed up and restored using cloning. All other objects are treated as SKS objects and are encrypted/decrypted by the SMK for extraction and [re-]insertion as needed.

## Constraints on SKS Backup and Restore

SKS Backup and Restore are intended to redundantly safeguard the SMK, only. The following conditions and constraints apply :

- > The SMK is not visible as a partition object, and does not appear in list output.
- > Backing up and restoring the SMK uses the same commands as backing up and restoring ordinary cryptographic objects.
- > SKS Backup and Restore require a Backup HSM with firmware 6.28.0 or firmware 7.7.0 (or newer).
- > SKS Backup and Restore is supported only when the currently selected slot is an SKS partition (V1).
- > Individual SKS blobs are limited to 64KB in size. Large groups of keys, or larger data objects might need to be split across multiple blobs for extraction or insertion.
- > The **partition archive backup** and **partition archive restore** commands test the currently selected slot to ensure it is an SKS-capable (V1) partition.
- > If the current slot is an SKS partition, then the **partition archive** commands perform backup or restore of the SMK, and ignore any other objects.

**TIP** The assumption is that since any extracted SKS blobs are solidly encrypted and remain within the assurance boundary, they can be safely stored in any repository. There is no need to store such blobs in another crypto-capable HSM partition, nor in a Backup HSM partition (though you could do the latter by storing as data objects, if desired) - they can be decrypted and used only by SKS insertion into an HSM partition that contains the relevant SMK.

## Backup the SKS Master Key (SMK)

The SMK backup operation creates a new partition on the backup HSM, using a partition name that is automatically created at the time of the backup operation. The system ensures that the archive partition name does not already exist on the Backup HSM by creating the target partition with a unique name that combines

- the serial number of the source partition (from your Network HSM) with
- a time stamp.

### To back up the SMK, do the following:

1. Have a Backup HSM connected to the client workstation from which you are running the command, or have a Backup HSM connected through a Remote Backup Server (see ["Backup and Restore to a Remote Backup Service \(RBS\)-Connected Luna Backup HSM \(G7\)"](#) on page 447 or ["Configuring a Remote Luna Backup HSM \(G5\) Server"](#) on page 406). The Backup HSM must be visible as a slot.
2. Launch the lunacm utility.
3. Use **slot list** to determine the slot numbers of the SKS partition and of the Backup HSM.
4. Set the SKS partition as the current slot.

```
lunacm:> slot set -slot 4
```

```
Command Result : No Error
```

5. Log into the current slot as Crypto Officer.

```
lunacm:> role login -name Crypto Officer
```

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

```
Command Result : No Error
```

## 6. Use **partition archive backup** to backup the SMK from the current slot to the indicated Backup HSM.

**NOTE** Do not name the target partition to be created on the Backup HSM, because SKS backup creates the name from the serial number of the source partition, combined with a time-stamp.

```
lunacm:>partition archive backup -slot 5
```

```
You are backing up a SKS partition.
```

```
Only the SKS master key (SMK) will be backed up.
```

```
No other objects will be cloned.
```

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

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

```
Logging in as the SO on slot 5.
```

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

```
Creating partition 358628973182_2017:03:09-16:52:47 on slot 5.
```

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

```
Logging into the container 358628973182_2017:03:09-16:52:47 on slot 5 as the user.
```

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

```
Creating Domain for the partition 358628973182_2017:03:09-16:52:47 on slot 5.
```

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

```
The SMK was cloned successfully.
```

```
Command Result : No Error
```

## 7. You can test the success by

- a. creating and initializing a V1 test partition on any HSM with firmware 7.7.0 or newer,
- b. restoring the backed-up SMK onto that test partition, and
- c. successfully importing an SKS blob (that was previously extracted using the specific SMK) into that partition.

## Restore an SKS Master Key (SMK)

To restore the SMK from backup, follow these steps.

**CAUTION!** When you restore an SMK from a Backup HSM, that restored SMK overwrites (destroys) any SMK that was already present on the partition. If the current SMK has been used to encrypt any important keys, ensure that you have backed it up safely before restoring a different SMK over it.

Also be sure to record the particulars of that backup, including the backup partition name and some notes to identify which keys have been encrypted by the SMK archived in that partition, for future reference.

1. Have a Backup HSM connected to the client workstation from which you are running the command, or have a Backup HSM connected through a Remote Backup Server (see "[Backup and Restore to a Remote Backup Service \(RBS\)-Connected Luna Backup HSM \(G7\)](#)" on page 447 or "[Configuring a Remote Luna Backup HSM \(G5\) Server](#)" on page 406). The Backup HSM must be visible as a slot.

2. Launch the lunacm utility.

3. Use **slot list** to determine the slot numbers of the SKS partition and of the Backup HSM.

4. Set the SKS partition as the current slot.

```
lunacm:> slot set -slot 4
```

```
Command Result : No Error
```

5. Log into the current slot as Crypto Officer.

```
lunacm:> role login -name Crypto Officer
```

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

```
Command Result : No Error
```

6. Use **partition archive restore** to restore the SMK from the current slot to the indicated Backup HSM, naming the partition with the desired SMK, on the Backup HSM.

```
lunacm:>partition archive restore -slot 5 -partition 358628973182_2017:03:09-16:52:47
```

```
You are restoring a SKS partition.
```

```
Only the SKS master key (SMK) will be restored.
```

```
No other objects will be cloned.
```

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

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

```
Logging in to partition 358628973182_2017:03:09-16:52:47 on slot 5 as the user.
```

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

```
The SMK was cloned successfully.
```

```
Command Result : No Error
```

7. You could test the success by restoring the SMK to a test partition, and successfully importing an SKS object that was previously exported, encrypted with that SMK.

## Backup objects

In most cases, only the SMK needs preserving, and any crypto objects on the SKS partition are just passing through (as temporary session objects), so there is no provision to backup crypto objects from an SKS partition. It is possible to store SKS blobs, but only as data objects, not as crypto objects. Therefore, to use them in any way, they must be inserted back into a V1 partition that has the correct SMK in either the Primary SMK location or the Rollover SMK location.

The Backup HSM can support a mix of

- > SKS-only archive partitions that each can contain a single SMK, and
- > ordinary cloning-backup partitions that each can contain multiple cryptographic objects for traditional cloning-based (non-SKS) HSM backup and restore operations.

In other words,

- > you can use an SKS client to backup crypto objects
  - from a non-SKS partition
  - into a non-SKS archive partition on the Backup HSM)
- > you can restore crypto objects
  - from a non-SKS archive partition on the Backup HSM
  - to a regular cloning-based (non-SKS) HSM partition.
- > you cannot restore ordinary objects onto an SKS partition; they must be SKS inserted (siminsert API call.)

## Troubleshooting SKS Backup and Restore

The following are some examples that highlight incorrect usage, along with the communication from the system.

### Not logged into partition at current slot

Here is an example of the output if you attempt to use the partition archive command without logging in as "Crypto Officer" on the SKS partition slot, which must be the current slot.

**NOTE** "-slot 5" in the example points to the Backup HSM slot, not the current SKS partition slot.

```
lunacm:>partition archive backup -slot 5
```

```
You are backing up a SKS partition.
Only the SKS master key (SMK) will be backed up.
No other objects will be cloned.
```

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

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

```
Error: Failed to open session.
```

```
Command Result : 0xb0 (CKR_SESSION_CLOSED)
```

### An incorrect option is specified for backup

In this example, the command fails because the "-partition" option is not applicable for SKS backup:

```
lunacm:>partition archive backup -slot 5 -partition test
```

You are backing up a SKS partition.  
Only the SKS master key (SMK) will be backed up.  
No other objects will be cloned.

Are you sure you wish to continue?  
Type 'proceed' to continue, or 'quit' to quit now ->proceed

Syntax Error: Option -partition cannot be used for SKS operation.

Command Result : No Error

### Archive contains crypto objects

If the backup partition to be restored contains crypto objects and SKS backup is being performed, restore of the SMK proceeds with a warning.

```
lunacm:> par ar r -s 5 -par pre-7-7
```

You are restoring an SKS partition.  
Only the SKS master key (SMK) will be restored.  
CAUTION: The existing SMK will be overwritten.

Are you sure you wish to continue?  
Type 'proceed' to continue, or 'quit' to quit now -> proceed  
Logging in to partition mypar on slot 5 as the user.

Please attend to the PED.

WARNING: Crypto object(s) detected in the backup device container.  
Dedicated backup container for SKS Master key is recommended.

The SMK was cloned successfully.

Command Result : No Error

## SMK Rollover

Mandated rollover schedules might place limits on the allowable lifetimes of important keys, like the SMK. Toward this end, the **partition smkrollover** command generates a new SMK and allows you to re-encrypt your SKS blobs with a new SMK.

However, if a new SMK is created - such as in the SMK rollover operation - then every blob that has been encrypted with the old SMK must be inserted, its contained keys/objects re-encrypted with the new SMK and extracted as a new blob, and this must be accomplished for all such externally stored blobs, *during* the **smkrollover -start** to **smkrollover -end** interval. Any blobs for which the encrypting SMK no longer exists can no longer be decrypted.

## To rollover the current SMK

If you wish to perform SMK rollover, please realize that it is a disruptive process and a major one. Hence, plan it appropriately by scheduling a down-time and then follow this three-step procedure:

1. Dismantle the HA group.
2. Perform SMK Rollover.
  - a. Begin with **partition smkrollover -start**
    - the original SMK is moved to the Rollover area, and
    - a new SMK is created and placed in the Primary SMK area of the current HSM.
  - b. Retrieve every blob from your repository, one at a time, insert it into the HSM partition - the insert action is performed with *SIMInsert API* using the former-primary-now-rollover SMK.
  - c. After each key or object is inserted, extract it again to external storage - the extract action is performed with *SIMExtract* using the new Primary SMK.
  - d. When *all* blobs have been retrieved (from repository, database, backup HSM, etc), inserted and re-extracted, then perform **partition smkrollover -end** one time, to delete the previous SMK from the rollover slot, to conclude the rollover operation.
3. Re-create the HA group, cloning the *new* SMK to each HSM that will become a member of the recreated HA group, and resume operations.

You can generate a new SMK and immediately discard the old one with **partition smkrollover -start -end** command. Do this *only* if you know that no blobs exist that are encrypted with the old SMK, otherwise they will be orphaned.

**NOTE** For HA environments, if you perform SMK rollover on a member, then the new SMK must be cloned to all members. However, database / repository update for rollover should be done by directly addressing the primary physical member, and *not* using the virtual slot (to avoid the performance penalty when keys inserted to the virtual slot during rollover would be propagated to all members before the re-extraction).

## Migrating Scalable Key Storage (SKS)

On this page:

- ["Cloning the SKS Master Key \(SMK\)" on the next page](#)
- ["SKS Blob Migration" on page 162](#)

The SKS feature beginning with HSM firmware version 7.7.0 (and newer) uses the same API as previous SKS versions, to retain backward compatibility; your applications that used older SKS should still work. However, the new structure for SKS was developed in conjunction with an updated cloning protocol and other features of firmware 7.7.0 associated with V1 partitions, and you (or a regulatory regime under which your organization operates) might see benefit in migrating existing SKS secrets to the newer form.

For purposes of migration, the SKS Master Key (SMK) is cloned to a target partition - this is the only use for the cloning protocol in V1 partitions. Objects encrypted by the SMK (SKS blobs) are generally expected to be stored externally in a repository via SKS extract operation (SIMextract API call) from the partition and later SKS insert operation (SIMinsert API call) when needed. If blobs are small enough or few enough in number, such objects could be replicated to other members in an HA group, or stored on a Backup HSM if desired, but as data objects only.

Off-board storage is assumed to be the primary method of storing such blobs (and *not* storage inside a general purpose crypto HSM or a backup HSM).

### Cloning the SKS Master Key (SMK)

No changes to the existing older SKS host API are necessary for the cloning of the earlier and the newer SMKs. The choice is based on the formatting of the incoming SMK Secret.

**NOTE** If a remote partition is involved (Network HSM) on either side of the SMK cloning operation, the HSM that contains the remote partition must have Network Replication enabled. See "[HSM Capabilities and Policies](#)" on page 1 "Policy 16 - Allow network replication".

The following table shows possible migration paths for existing SMKs -- the leftmost column is possible sources, while the heading row across the top lists possible destinations, and the intersecting table cells are the possible result for each source-to-destination scenario.

|                                     | <b>FM6 SKS appliance</b> | <b>FW6 SKS G5 Backup (6.25)</b> | <b>FW7.7 eIDAS G5 Backup (6.28)</b>               | <b>FW&lt;7.7 HSM</b>            | <b>FW&gt;=7.7 FM HSM</b>                          | <b>FW&gt;=7.7 Non-FM HSM</b>                      |
|-------------------------------------|--------------------------|---------------------------------|---------------------------------------------------|---------------------------------|---------------------------------------------------|---------------------------------------------------|
| <b>FW6 SKS appliance</b>            | FW6 SMKs                 | FW6 SMKs                        | FW6 SMKs                                          | No SMK support on target        | Target has FM cert only                           | FW6 SMKs                                          |
| <b>FW6 SKS G5 Backup (6.25)</b>     | FW6 SMKs                 | FW6 SMKs                        | FW6 SMKs                                          | No SMK support on target        | Target has FM cert only                           | FW6 SMKs                                          |
| <b>FW7.7 eIDAS G5 Backup (6.28)</b> | FW6 SMKs                 | FW6 SMKs                        | All SMKs (cloning protocol used by V1 partitions) | No SMK support on source/target | All SMKs (cloning protocol used by V1 partitions) | All SMKs (cloning protocol used by V1 partitions) |
| <b>FW&lt;7.7 HSM</b>                | No SMK support on source | No SMK support on source        | No SMK support on source                          | No SMK support on target        | No SMK support on source                          | No SMK support on source                          |



|                             | FM6 SKS appliance                       | FW6 SKS G5 Backup (6.25)                | FW7.7 eIDAS G5 Backup (6.28)                      | FW<7.7 HSM               | FW>=7.7 FM HSM                                    | FW>=7.7 Non-FM HSM                                                          |
|-----------------------------|-----------------------------------------|-----------------------------------------|---------------------------------------------------|--------------------------|---------------------------------------------------|-----------------------------------------------------------------------------|
| <b>FW7.7 FM HSM</b>         | Source has FM cert only                 | Source has FM cert only                 | All SMKs (cloning protocol used by V1 partitions) | No SMK support on target | All SMKs (cloning protocol used by V1 partitions) | All SMKs (FW7.7-Primary -> FW7.7-FM, FW7.7-Rollover dropped) (V1 partition) |
| <b>FW7.7 Non-FM SKS HSM</b> | Required cloning protocol not on target | Required cloning protocol not on target | All SMKs (cloning protocol used by V1 partitions) | No SMK support on target | Blocked by V1 cloning protocol                    | All SMKs (cloning protocol used by V1 partitions)                           |

( **FW>=7.7** means HSM firmware version 7.7 or newer)

### To migrate an older SMK

To move/copy an SMK from one of the supported source configurations to one of the supported targets

1. If the source and target are crypto partitions, clone the SMK secrets between partitions with the **partition smkclone** lunacm command.
2. If the target is a Luna Backup HSM clone to the Backup HSM with the **partition archive backup** lunacm command.
3. If the source is a Luna Backup HSM, clone from the Backup HSM with the **partition archive restore** lunacm command.

Only some combinations of source and target are supported. Reasons for a path to not be supported are summarized in the table.

#### SCENARIO 1:

0. You have a pre-existing 7.7.0 SMK, and a bunch of extracted blobs (encrypted with that SMK) in a repository, all of which you want to preserve, and to which you want to add 6.x SMK and SKS blobs after migrating them.

1. Backup the modern 7.7.0 SMK to a partition on a firmware 6.28.0 or 7.7.0 Backup HSM (**partition archive backup**).
2. Backup the 6.x or 4.x SMK (**partition archive backup**).
3. Restore the 6.x SMK onto a V1 partition (**partition archive restore**). This puts it in the Primary SMK slot of that partition, overwriting any SMK that was there.
4. Perform **partition smkrollover -start** on the V1 partition. This moves the 6.x SMK into the Rollover slot of the partition and generates a new Primary SMK.

5. Restore the production 7.7.0 SMK that you backed-up earlier (**partition archive restore**). This overwrites the newly-generated Primary, but the Rollover partition still has the 6.x SMK.
6. Insert one of your 6.x SKS blobs. The HSM tests it and knows to use the Rollover SMK to perform the SKS insert operation.
7. Extract the key/crypto-object as a new blob - the HSM allows only the Primary (the one you just got back from archive) to perform the extraction.
8. Repeat for all your old-style blobs to get them all encrypted with the new SMK for storage in your repository.
9. Perform **partition smkrollover -start** which deletes the old SMK from the Rollover slot of the V1 partition.

#### SCENARIO 2:

You have 6.x SMK and SKS blobs. You want to migrate the older blobs to use in a new V1 partition (7.7). So, no 7.7.0 SMK and blobs currently exist that need conserving.

1. Backup the 6.x (to partition on 6.28.0 or 7.7.0 Backup HSM) with **partition archive backup** command.
2. Create a new V1 partition (**partition create**), initialize it (**partition initialize**), log in as CO (**role login - name co**) etc., but you don't care about the generated 7.7.0 SMK.
3. Restore the 6.x SMK onto the V1 partition (**partition archive restore**). This puts it in the Primary SMK slot of that partition, overwriting any SMK that was there.
4. Perform **partition smkrollover -start** on the V1 partition. This moves the 6.x SMK into the Rollover slot of the partition and generates a new Primary SMK.
5. Insert one of your 6.x SKS blobs. The HSM tests it and knows to use the Rollover SMK to perform the SIMinsert operation.
6. Extract the blob - the HSM allows only the Primary (recently generated) to do the extraction.
7. Repeat for all your old-style blobs to get them all encrypted with the new SMK for storage in your repository.
8. Perform **partition smkrollover -start** which deletes the old SMK from the Rollover slot of the V1 partition.

#### SKS Blob Migration

With no modifications to the pre-existing host API for offboard key storage (SKS), the version number for the mechanism used is prepended to the SKS blobs and employed to select the correct mechanism to insert the blob back into the HSM.

HSMs are allowed to extract key blobs using only the latest and greatest SMK secret and mechanism available to them. Incoming older blobs with older SMK secrets and mechanisms are accepted, provided that the HSM f/w supports them.

**NOTE** Migration from older HSMs, that used possibly outdated encrypting keys/mechanisms should not present a problem, since older blobs would be inserted only. The same material would then be extracted using newer or unrestricted key types or sizes.

The following table shows options for SKS blob insertion into a partition, Protocol and Key Import/Export vs External Storage.

The leftmost column is possible sources, while the heading row across the top lists possible destinations, and the intersecting table cells are the possible result for each source-to-destination scenario.

|                                          | <b>FW6 SKS appliance</b>                                    | <b>FW7.7.0 Non-FM HSM (V0 Partition)</b> | <b>FW7.7.0 FM HSM (V0 Partition)</b> | <b>FW7.7.0 Non-FM HSM (V1 Partition)</b>                                          | <b>FW7.7.0 FM HSM (V1 Partition)</b>                                              |
|------------------------------------------|-------------------------------------------------------------|------------------------------------------|--------------------------------------|-----------------------------------------------------------------------------------|-----------------------------------------------------------------------------------|
| <b>FW6 SKS appliance</b>                 | Using FW6 SMK (V1 partition cloning protocol) Import/Export | No SKS Support on source/target          | No SKS Support on source/target      | Using FW6 SMK (V0 partition cloning protocol) Import/Export                       | No FW6 SMKs on Target                                                             |
| <b>FW7.7.0 Non-FM HSM (V0 Partition)</b> | No FW7.7.0-Primary SMK on Target                            | No SKS Support on source/target          | No SKS Support on source/target      | No SKS Support on source                                                          | No identical FW7.7.0-Primary SMK on Target                                        |
| <b>FW7.7.0 FM HSM (V0 Partition)</b>     | No FW7.7.0-FM SMK on Target                                 | No SKS Support on source/target          | No SKS Support on source/target      | No SKS Support on source                                                          | No SKS Support on source                                                          |
| <b>FW7.7.0 Non-FM HSM (V1 Partition)</b> | No FW7.7.0-Primary SMK on Target                            | No SKS Support on source/target          | No SKS Support on source/target      | Using FW7.7.0-Primary SMK (V1 partition cloning protocol) <b>External Storage</b> | No identical FW7.7.0-Primary SMK on Target                                        |
| <b>FW7.7.0 FM HSM (V1 Partition)</b>     | No FW7.7.0-FM SMK on Target                                 | No SKS Support on source/target          | No SKS Support on source/target      | Using FW7.7.0-FM SMK (V1 partition cloning protocol) <b>External Storage</b>      | Using FW7.7.0-Primary SMK (V1 partition cloning protocol) <b>External Storage</b> |

### To migrate an older SKS blob:

To insert an SKS blob, for any of the supported scenarios (table above),

1. Insert with the SIMinsert operation as you always have.

The CKDemo Utility, command 106, demonstrates the action - see "[OFFBOARD KEY STORAGE Menu Functions](#)" on page 1.

## Per-Key Authorization (PKA)

---

Per-key authorization or authentication (PKA) is a feature introduced with HSM firmware 7.7.0 to support the eIDAS use case of Remote Signing and Sealing (RSS) and the relevant Protection Profile (PP 419-221.5). PKA introduces data structures to keys that are created and manipulated in the HSM such that keys can be handled in the ways that applications normally handle key material, but under the sole ownership and control of an end-user natural person or legal entity. The attributes are applied to keys that are created with firmware 7.7.0 (or newer). In V0 partitions those attributes are simply ignored. In V1 partitions the attributes are actively used. See more at "[What are "pre-firmware 7.7.0", and V0, and V1 partitions?" on page 126](#).

### Keys for use in eIDAS schemas:

- > have authentication data structures that allow the possibility for an entity to have sole ownership and control
- > can be unassigned, waiting for distribution to eventual owners/Users, or
- > can be assigned to the control of a specific owner/User.

When a key has auth code data attached, then by definition anyone who holds the auth code is a/the key owner. But before it is assigned, the key does not have an owner/User, and might be part of a pool of unassigned keys, waiting for distribution to users. Keys do take some time to generate, so in times of high demand, it could be practical and convenient to have some ready-to-go.

Keys are intended to be used, but they must also be administered. That is, an individual natural person (or a non-natural legal entity) authorizes cryptographic usage of a key, perhaps to sign forms or documents. At the same time, the HSM has roles that perform actions within the HSM, either:

- > *generally* - the eIDAS Administrator role represented by the Crypto Officer (CO) role in the HSM) or
- > *specifically/individually* - the eIDAS User role represented by the Limited Crypto Officer (LCO) role in the HSM.

So, a citizen might log into a service and perform an action that directs the application to retrieve their existing personal key from a database/repository and insert/decrypt the key into an HSM partition, where the citizen authorizes a signing or other operation, and then the copy of the key is deleted from the HSM partition, but the archived, encrypted copy resides safely in the database for future retrieval and use. Alternatively, a citizen might request a single-use key, that is generated 'on-the-spot' in the HSM partition (by the LCO role) and is authorized by that citizen to perform one action (like signing) and then the key is permanently deleted, with no copy existing anywhere.

Generally, these and other operations related to keys are not performed by administrative commands (tools like lunacm); rather, they are performed via the PKA API or REST, while the performing application is logged in as one or the other of the partition roles.

### Example Use Case

For example, an application might be instructed to retrieve a certain key and use it to sign a document on behalf of a citizen. The application acquires the key from a database (in the form of an encrypted blob) and inserts it into an HSM where it is decrypted to reveal the key that is to be used. But the application is able to actually use that key only when the owner/citizen presents her/his unique authentication data, which is part of the key attributes.

---

## New Role and Handling

In order to manage this service, the individual application partition's Crypto Officer role and a new role called Limited Crypto User handle the actions of creating, modifying, and using keys containing auth data.

A key can be created in an assigned state, where it is immediately associated with an entity, or a key can be created in unassigned state and only later assigned to an owner, when convenient.

## No New Administrative Commands

Because the operations around PKA and RSS are handled programmatically, no particular administrative commands are introduced - only a new **-version** option for partition creation and a new partition policy 40, which is off for V0 partitions, and which defaults to on for V1 partitions, but can be turned off if desired.

Everything else about PKA is handled by the ["PKA API" on page 1](#).

## Dependencies and Interactions with Other Features

PKA generally requires HSM firmware 7.7.0 or newer and Luna Client 10.3 or newer, and for the Network HSM Appliance, appliance software 7.7.0 or newer. The feature is ignored by older clients and applications that do not know how to make use of it. Active use of PKA requires a V1 partition, which means that cloning is used for:

- > incoming keys and objects from older firmware, but not outgoing (that is, on V1 partitions, cloning of keys is inbound migration, only)
- > copying (such as for HA), or backing-up/restoring, of the SMK

All other objects are stored, encrypted by the SMK, in external storage using the Scalable Key Storage (SKS) feature.

Stored Data Integrity (SDI) is also mandated by eIDAS and is therefore applied by HSM firmware 7.7.0 and newer.

HA Indirect Login support is constrained differently for V0 and V1 partitions - see section "V0 Partitions" in ["PKA API" on page 1](#).

# CHAPTER 6: Key Cloning

You can clone key material between partitions to back up the keys, or to migrate the keys from one HSM to another. The rules, prerequisites, and procedures for migrating your key material are described in the following topics:

- > ["Domain Planning" on the next page](#)
- > ["Cloning Objects to Another Application Partition" on page 170](#)
- > ["Cloning Keys Between Luna 6, Luna 7, and Luna Cloud HSM" on page 171](#)

## Overview and Key Concepts

---

A Crypto Officer can clone the cryptographic objects (keys) from one user partition to another user partition provided that:

- > The user partitions share the same domain. See ["Domain Planning" on the next page](#).
- > The user partitions use the same authentication method (PED or password).
- > The CO has the required credentials on both user partitions.
- > The capabilities and policies set on the source and target HSM and user partitions allow cloning. See [HSM Capabilities and Policies](#) and ["Partition Capabilities and Policies" on page 272](#).

### Changes introduced with firmware 7.7.0 (and newer)

You can update Luna Client software, and Luna HSM firmware, and Luna Network HSM Appliance software at different times, according to your needs.

When firmware is updated to version 7.7.0 or newer, some changes take place in the partitions and their contents, such that updated Client software is needed to make full use of the updated partitions and their contents. See ["What are "pre-firmware 7.7.0", and V0, and V1 partitions?" on page 126](#) for more detail on behaviors and constraints of the partition types.

In HA groups update the secondary members first, and then the primary member last.

Older client will continue to work with V0 partition for Network HSM.

For PCIe must use Client 10.3 or

Need newer client for V1 partitions when you want to use SKS or PKA.

- Client software must be version 10.3 or newer to support SKS, to work with V1 partitions and HA. See ["What are "pre-firmware 7.7.0", and V0, and V1 partitions?" on page 126](#) for more detail.

**NOTE** The library attempts to perform the individual actions of a cloning operation in sequence on the respective partitions. If the policies and partition types on the source and target partitions are incompatible, the **partition clone** command (or an attempted HA synchronization) can fail with a message like `CKR_DATA_LEN_RANGE` while trying to clone. This can occur if a key object from the source partition is a different size than an equivalent object expected by the target.

### Cloning support when Client is pre-10.3

### Cloning support when Client is version 10.3 or newer

|                                     | to HSM Firmware pre-7.7 | to HSM Firmware 7.7 (or newer) V0 | to HSM Firmware 7.7 (or newer) V1 |
|-------------------------------------|-------------------------|-----------------------------------|-----------------------------------|
| from HSM Firmware pre-7.7           | Yes                     | Yes                               | Yes                               |
| from HSM Firmware 7.7 (or newer) V0 | No                      | Yes                               | Yes                               |
| from HSM Firmware 7.7 (or newer) V1 | No                      | No                                | Yes                               |

## Domain Planning

The cloning or security domain is an element of ["Layered Encryption" on page 1](#).

### What is a security domain or cloning domain?

A security domain or cloning domain is a layer of encryption that is created, during initialization, on an HSM or HSM partition that you control. The domain determines whether a crypto object can leave the HSM, and where it can go if it is allowed to leave.

Cloning is a secure-copy operation by which sensitive HSM objects are copied, while strongly encrypted, from one HSM to another HSM. The security domain, or cloning domain, is a special-purpose secret that is attached to a partition on an HSM. It determines *to* which, and *from* which, other partitions (on the same HSM or on other HSMs) the current partition can clone objects. Partitions that send or receive partition objects by means of the cloning protocol must share identical cloning domain secrets. That is, the protocol verifies that the destination domain matches the source domain; otherwise an error is displayed and the attempted operation fails. This is important for:

- > Cloning in backup and restore operations, and
- > Synchronization in HA groups.

## Only one domain per partition - no copying across domains

An application partition can have one cloning domain. It is not possible to clone objects from two or more different cloning domains to a single partition. By design, there is no provision to change the cloning domain of a partition without initializing it, which destroys any objects in that partition.

## No common domains across Password-authenticated and PED-authenticated HSMs

Password authenticated application partitions, with identical security domains, can clone partition contents one to the other, if the HSM type supports cloning.

Multi-factor authenticated (PED authenticated) application partitions, with identical security domains, can clone partition contents one to the other, if the HSM type supports cloning.

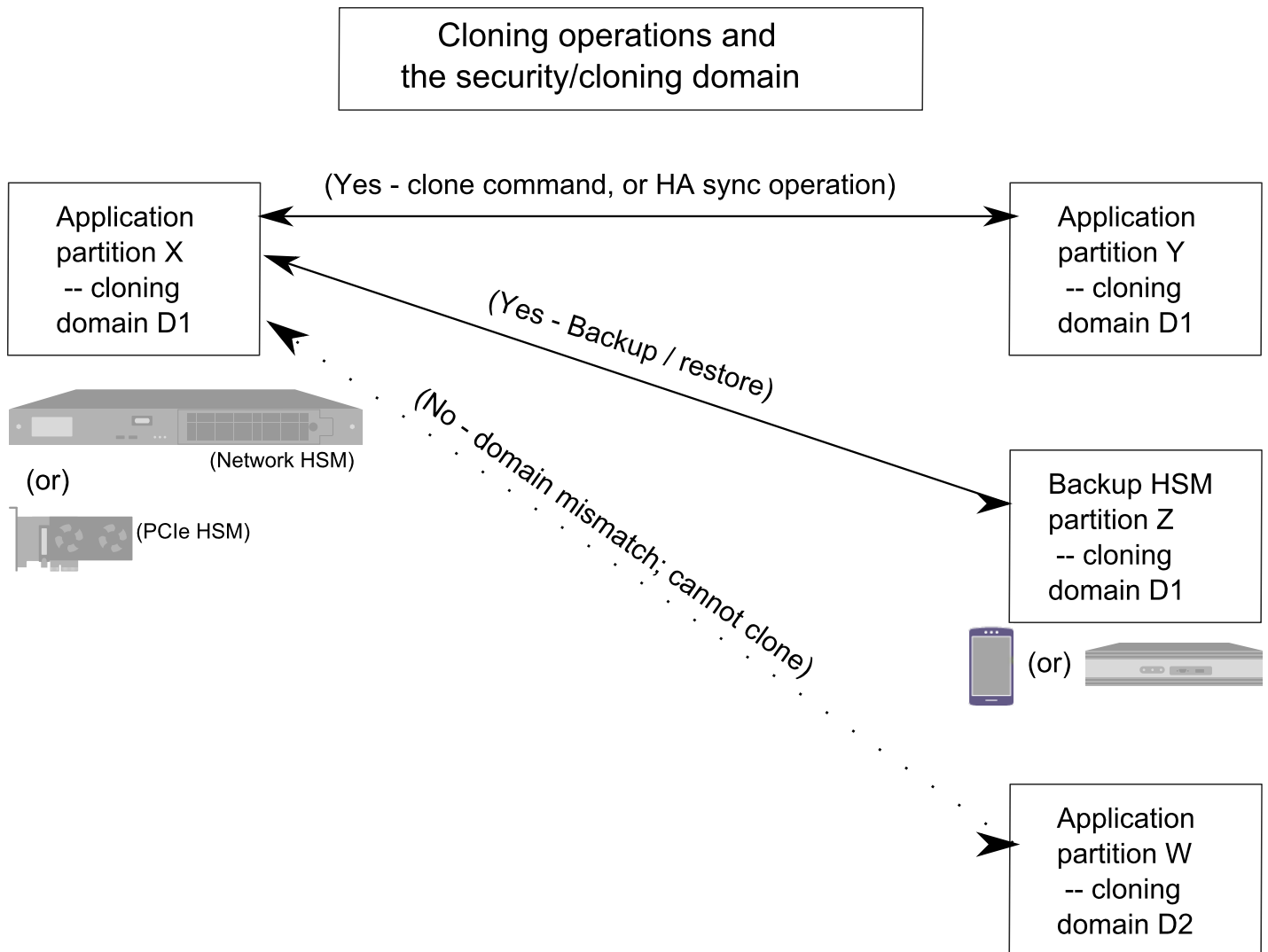
But password authenticated HSM partitions cannot perform cloning with PED-authenticated HSM partitions.

The security design consideration is that, if you have a key or object stored in a multi-factor-authenticated (PED-authenticated) partition:

- > It cannot be altered to a less-secure state and moved outside the protection of its original security/cloning domain.
- > You are assured that the key or object has never been outside its original security/cloning domain, or in any less-secure state.

As of firmware 7.7.0, and any V1 (non-backward-compatible) partitions, backup and HA replication of crypto objects are accomplished with SKS encrypted blobs, and the cloning protocol is reserved for the SMK - the key that encrypts the SKS blobs.





## Characteristics of Cloning Domains

Password authenticated HSMs have text-string cloning domains for the HSM admin partition and for any partitions that are created on the HSM. HSM and Partition domains are typed at the command line of the host computer, when required. Password authentication cloning domains are created by you.

PED authenticated cloning domains are created by a Luna HSM, which could be the current HSM, or it could be a previously initialized HSM that you wish to include in a cloning group with the current HSM. PED authenticated HSMs have cloning domains in the form of encrypted secrets on red PED keys, for the admin partition and for any partitions that are created on the HSM.

The following characteristics are common to security (cloning) domains on all Luna HSMs.

- > The unique admin partition security domain can be created in the HSM at initialization time, or it can be imported, meaning that it is shared with one-or-more other HSMs.
- > The application partition security domain can be created by the current HSM when the partition is initialized, or it can be imported, meaning that it is shared with one-or-more other HSM partitions, and therefore direct

cloning, backup/restore, and HA sync operations can be performed among the partitions that share a given domain.

- > The application partition security domain is usually distinct from the HSM domain, as they are controlled by different people; on multi-partition HSMs, the PSO is usually not the same person as the HSM SO, but on a single-partition HSM the two SOs might be the same person.
- > The application partition security domain can be the same as the domain of another partition on the same HSM (for HSMs that support multiple partitions).

For PED authenticated HSMs, the domain secret for the admin partition or for an application partition can be a single red PED key, or it can be split (by the MofN quorum feature) over several red keys, which are then distributed among trusted personnel such that no single person is able to provide the cloning domain without oversight from other trusted personnel.

In scenarios where multiple HSM partitions are in use, it can be useful to segregate those partitions according to department or business unit, or according to function groups within your organization. This ensures that personnel in a given group are able to clone or backup/restore only the contents of partitions sharing the domain for which they are responsible. The segregation is maintained by physical and procedural control of the relevant PED keys that each group is allowed to handle.

For Password authenticated HSMs, that sort of segregation is maintained entirely by procedure and by trust, as you rely on personnel not to share the domain text strings, just as you rely on them not to share other passwords.

Have your naming conventions and allotments planned out ahead of HSM initialization and partition creation, including a well-thought-out map of who should control cloning domain access for admin partitions and for application partitions. These decisions must be made before you create the partitions.

## Cloning Objects to Another Application Partition

You can back up partition objects from an application partition to any other partition that shares its cloning domain. The Crypto Officer of both partitions can perform this operation using LunaCM.

### Prerequisites

- > **Partition policy 0: Allow private key cloning** must be set to **1 (ON)** on both the source and target partitions.
- > The target partition must be initialized with the same cloning domain as the source partition.
- > You require the Crypto Officer credential for both the source and the target partition.
- > Both partitions must be visible as slots in LunaCM.
- > [Remote PED] This procedure is simpler when both partitions are activated (see "[Activation and Auto-activation on Multi-factor- \(PED-\) Authenticated Partitions](#)" on page 299). If the partitions are not activated, you must connect the source partition to PEDserver before logging in, disconnect it, and then connect the target partition to PEDserver by specifying its slot.

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

```
lunacm:> ped disconnect
```

```
lunacm:> ped connect -slot <target_slot> [-ip <IP>] [-port <port>]
```

**NOTE** The library attempts to perform the individual actions of a cloning operation in sequence on the respective partitions. If the policies and partition types on the source and target partitions are incompatible, the **partition clone** command (or an attempted HA synchronization) can fail with a message like `CKR_DATA_LEN_RANGE` while trying to clone. This can occur if a key object from the source partition is a different size than an equivalent object expected by the target.

### To clone partition objects to another application partition

1. In LunaCM, set the active slot to the source partition and log in as Crypto Officer.

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

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

2. [Optional] View the partition objects and their object handles.

```
lunacm:> partition contents
```

3. Clone objects on the partition to the target partition by specifying the target slot. You can choose which objects to clone by specifying a comma-separated list of object handles, or specify **all** to clone all objects on the partition. Present the target partition's Crypto Officer credential when prompted.

```
lunacm:> partition clone -slot <slotnum> -objects <comma-separated_list/all>
```

The specified objects are cloned to the target partition. Any objects that already exist on the target are not cloned.

## Cloning Keys Between Luna 6, Luna 7, and Luna Cloud HSM

Luna HSM Client allows you to clone keys between Luna 6 partitions, Luna 7 partitions, and Thales Data Protection on Demand (DPoD) Luna Cloud HSM services. This includes creating HA groups made up of different HSM versions. This configuration is useful for:

- > migrating your keys directly from Luna 6 to your new Luna 7 HSMs
- > migrating your keys from Luna Network HSM to the cloud, or vice-versa
- > gradually upgrading your on-premises production environment from Luna 6 to Luna 7 HSMs
- > maintaining a real-time, cloud-based backup of your cryptographic objects

This page contains guidelines and general considerations for cloning keys between the different HSMs, or using mixed-version HA groups. Mixed-version HA groups have all the same requirements of standard HA groups (see ["Planning Your HA Group Deployment" on page 346](#)), in addition to the considerations listed below.

- > ["Luna/Luna Cloud HSM Cloning" on the next page](#)
- > ["Supported Software/Firmware Versions" on the next page](#)
- > ["Mismatched Partition Policies and FIPS Mode" on page 173](#)
- > ["Mismatched Key Types/Cryptographic Mechanisms" on page 173](#)
- > ["Minimum Key Sizes" on page 174](#)
- > ["SafeXcel 1746 Co-Processor" on page 174](#)

- > ["RSA-186 Key Remapping for FIPS Compliance" on page 174](#)
- > ["HA Performance Optimization" on page 175](#)

## Luna/Luna Cloud HSM Cloning

Cloning between Luna partitions and Luna Cloud HSM services require the following special considerations, in addition to the general considerations below.

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

### Authentication

Luna Cloud HSM services use password authentication, and therefore they can clone objects to and from password-authenticated Luna Network HSMs only. It is not possible to clone keys between a Luna Cloud HSM service and a PED-authenticated Luna HSM.

### Network Latency and Luna Cloud HSM as Active HA Member

Requests performed by cloud services like Luna Cloud HSM may experience greater network latency than those sent to on-premise HSMs. Thales recommends using a Luna Cloud HSM service as a standby HA member to achieve the best performance. By default, you can add a Luna Cloud HSM service as a standby HA member only. If all other HA members fail and the Luna Cloud HSM service becomes active, it will revert to standby when another member recovers.

If you prefer to use the Luna Cloud HSM service as an active HA member, you must first edit the following toggle in the **Chrystoki.conf/crystoki.ini** configuration file (see ["Configuration File Summary" on page 70](#)):

```
[Toggles]
lunacm_cv_ha_ui = 0
```

### Cloning Capacity Limitations

The following limitations apply to clients accessing a Luna Cloud HSM service:

- > 100 token objects (or 50 RSA-2048 key pairs) per service.
- > 100 session objects (or 50 RSA-2048 key pairs) per application.
- > 100 simultaneous sessions per application.

Clients which exceed the token object and session object limits can experience slow or failed request responses. The session limit is enforced, and the client receives the error `CKR_MAX_SESSION_COUNT` when the application reaches the limit.

If you exceed the recommended maximum number of objects cloned to/from a Luna Cloud HSM service in a single cloning operation, the operation sometimes fails with `CKR_DEVICE_ERROR`. In the case of HA groups, this could include key creation operations, since objects are then cloned to the Luna Cloud HSM service.

## Supported Software/Firmware Versions

Thales supports cloning between Luna 6/7 partitions and Luna Cloud HSM services using combinations of appliance software/firmware as outlined in the table below.

**NOTE** Luna HSM firmware 7.7.0 is not compatible with older Luna versions or Luna Cloud HSM services.

| Client Software                                                                               | Luna Appliance Software | Luna HSM Firmware |
|-----------------------------------------------------------------------------------------------|-------------------------|-------------------|
| <b>Luna only:</b> 10.3.0 or higher                                                            | 7.7.0 or higher         | 7.7.0 or higher   |
| <b>Luna Cloud HSM service with Luna 6/7:</b> 10.1 or higher<br><b>Luna 6/7:</b> 7.2 or higher | 6.2.1 or higher         | 6.10.9 or higher  |

## Mismatched Partition Policies and FIPS Mode

Partitions in an HA group, and the HSMs on which they reside, must be configured with the same policy settings (see "[HSM and Partition Prerequisites](#)" on page 346). For example, Luna 6 HSMs have certain policies that have been removed from Luna 7 and Luna Cloud HSM, and new policies have been introduced.

Ensure that policies common to Luna 6/7/Luna Cloud HSM members have the same settings, according to your deployment requirements.

lunacm:> [partition showpolicies](#)

**CAUTION!** In particular, FIPS mode must be consistent across all HA members (on or off).

## Mismatched Key Types/Cryptographic Mechanisms

Cloning is limited to key types that are recognized by the firmware on both HSMs. If an HSM does not recognize the type of key being cloned to it, the cloning operation may fail. Ensure that the firmware on the destination HSM is capable of recognizing all cryptographic objects stored on the source HSM.

**NOTE** Luna HSMs comply closely with the relevant FIPS standards and their generally accepted interpretations. These are moving targets, as the crypto and security climate continues to evolve. It is possible for a validated HSM version (firmware) to be fully compliant when its NIST certificate is issued, and for same-model HSMs with newer firmware and more stringent restrictions to refuse to accept "less secure" objects.

Alternatively, the more up-to-date HSM might accept an object from an earlier-firmware HSM, but permit only limited uses of such an object. This can affect the operation of HA groups, and other situations, where applications attempt operations against old keys, or with the use of antiquated mechanisms.

If you are cloning between HSMs operating in FIPS mode, please consult [Supported Mechanisms](#) for the destination HSM's version to determine if all key types can be cloned.

Mixed-version HA groups are limited to functions that are common to all member partitions. Mechanisms are added to/removed from new firmware releases, to provide new functionality and fix vulnerabilities. Operations assigned by load-balancing to a member lacking the correct mechanism will fail. Keys created on one member may fail to replicate to the other group members.

Ensure that your applications use only mechanisms that are available on all HA group members. Use LunaCM to see a list of mechanisms available on each partition/service.

```
lunacm:> partition showmechanism
```

## Minimum Key Sizes

Minimum key sizes are enforced when using certain cryptographic algorithms. These minimums may differ between versions. If a Luna 6 partition creates a key that is smaller than the minimum size required by Luna 7 or Luna Cloud HSM, the key will not be replicated to the other partitions in the HA group.

**NOTE** Minimum key sizes for many mechanisms are larger in FIPS mode, and FIPS minimums may vary among firmware releases.

To avoid this, use LunaCM to check a mechanism's minimum key size. Check the same mechanism on each HA member slot, and always use the highest minimum reported in the HA group.

```
lunacm:> partition showmechanism -m <mechanism_ID>
```

## SafeXcel 1746 Co-Processor

Luna 6 HSMs include the SafeXcel 1746 security co-processor, which is used to offload packet processing and cryptographic computations from the host processor. Applications using this co-processor are not compatible with mixed-version HA groups.

The co-processor is not enabled by default. If you have previously enabled it on your Luna 6 HSMs, you can disable it by editing the **Chrystoki.conf/crystoki.ini** configuration file as follows:

```
[Misc]
PE1746Enabled=0
```

## RSA-186 Key Remapping for FIPS Compliance

Under FIPS 186-3/4, the only RSA methods permitted for generating keys are 186-3 with primes and 186-3 with aux primes. RSA PKCS and X9.31 key generation is not approved in a FIPS-compliant HSM. While Luna 6.10.9 firmware allows these older mechanisms, later firmware does not (and keys created using these mechanisms cannot be replicated to Luna 7 HSMs or Luna Cloud HSM services).

If you have older applications that use RSA PKCS and X9.31 key generation, you can remap these calls to use the newer, secure mechanisms. Add a line to the **Chrystoki.conf/crystoki.ini** configuration file as follows:

```
[Misc]
RSAKeyGenMechRemap=1
```

**NOTE** This setting is intended for older applications that call outdated mechanisms, to redirect calls to FIPS-approved mechanisms. The ideal solution is to update your applications to call the approved mechanisms.

Mechanism remapping is automatic, and ignores the configuration file entry: if you are using Luna HSM Client 10.1 or newer, and HSM firmware is earlier than version 7.7.1 (which introduced the ability for a partition to be FIPS-mode when the HSM is non-FIPS; clients up to, and including, 10.3.0 are unaware of the independent partition setting and do not remap mechanisms).

## HA Performance Optimization

Luna Network HSM 7 provides significant (10x) performance improvements over Luna 6 HSMs. In a mixed-version HA group, operations assigned to Luna 6 member partitions will take longer than those assigned to Luna 7 members. The HA logic does not compensate for these performance differences, and schedules operations on the partition with the shortest queue. Since Luna 7 partitions complete operations more quickly, they will naturally be assigned more operations, but a mixed-version HA group generally does not perform as well as an HA group made up entirely of Luna 7 partitions.

The performance of Luna Cloud HSM services may be limited by network latency, compared to on-premises Luna HSMs. See "[Luna/Luna Cloud HSM Cloning](#)" on page 172.

Thales recommends that you set a Luna 7 partition as the primary HA member (the first member specified when creating the HA group). All key generation takes place on the primary HA member, so this allows you to take advantage of the Luna Network HSM's vastly improved performance for:

- > key generation
- > random number generation

The load-balancing logic is determined by the Luna HSM Client software, so the Luna 7 behavior applies to mixed-version HA (see "[Load Balancing](#)" on page 338).

**NOTE** The primary HA member may not remain the same over time. If the primary member fails, another member takes over all key generation operations. If you notice a significant drop in performance for key generation operations, it could mean that a Luna 6 partition or Luna Cloud HSM service has become the primary member. By default, a Luna Cloud HSM service will revert to standby once another HA member recovers.

# CHAPTER 7: PED Authentication

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

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

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

This chapter contains the following sections about PED authentication:

- > ["PED Authentication Architecture" below](#)
  - ["Comparing Password and PED Authentication" on the next page](#)
- > ["PED Keys" on page 178](#)
  - ["PED Key Types and Roles" on page 178](#)
  - ["Shared PED Key Secrets" on page 180](#)
  - ["Domain PED Keys" on page 181](#)
  - ["PED PINs" on page 181](#)
  - ["M of N Split Secrets \(Quorum\)" on page 182](#)
- > ["Luna PED Received Items" on page 184](#)
- > ["Luna PED Hardware Functions" on page 186](#)
- > ["Updating Luna PED Firmware \(for older-version PED that requires a power-block\)" on page 218](#)
- > ["Local PED Setup" on page 190](#)
- > ["About Remote PED" on page 191](#)
- > [Remote PED Setup](#)
- > ["PED Key Management" on page 224](#)
- > ["PEDserver and PEDclient" on page 238](#)

## PED Authentication Architecture

---

The PED Authentication architecture consists of the following components:



- > **Luna PED:** a PIN Entry Device with a local or remote connection to the HSM. The PED reads authentication secrets from PED keys on behalf of an HSM or partition (see ["Luna PED Hardware Functions" on page 186](#)).
- > **Authentication secrets:** Cryptographic secrets generated by the HSM and stored on PED keys. These secrets serve as login credentials for the various roles on the HSM. They can be shared among roles, HSMs, and partitions according to your security scheme.
- > **PED Keys:** physical USB-connected devices that contain authentication secrets, created by the HSM (see ["PED Keys" on the next page](#)). PED Keys have the following custom authentication features:
  - **Shared Secrets:** PED keys of the same type can be reused or shared among HSMs or partitions, allowing domain sharing (necessary for HA and backup configurations), legacy-style Security Officer authentication, and other custom configurations. See ["Shared PED Key Secrets" on page 180](#).
  - **PED PINs:** optional PINs associated with specific PED keys, set by the owner of the PED key at the time of creation. PED PINs offer an extra layer of security for PED keys which could be lost or stolen. See ["PED PINs" on page 181](#).
  - **M of N Split Key Scheme:** optional configuration which allows a role to split its authentication secret across multiple PED keys, and require a minimum number of those keys for authentication. This scheme can be customized to be as simple or complex as your organization's security policy dictates. See ["M of N Split Secrets \(Quorum\)" on page 182](#).

## Comparing Password and PED Authentication

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

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

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

## PED Keys

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



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





PED keys are created when an HSM, partition, role, or Remote PED vector is initialized. A PED key can contain only one authentication secret at a time, but it can be overwritten with a new authentication secret. See "[PED Key Management](#)" on page 224.




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

## PED Key Types and Roles

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

The PED key colors correspond with the HSM roles described in "[HSM Roles and Procedures](#)" on page 1. The following table describes the keys associated with the various roles:

| Lifecycle                | PED Key                                                                                            | PED Secret                             | Function                                                                                                                                                                                                                                                                     |
|--------------------------|----------------------------------------------------------------------------------------------------|----------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| HSM Administration       | <b>Blue</b>                                                                                        | HSM Security Officer (HSM SO) secret   | Authenticates the HSM SO role. The HSM SO manages provisioning functions and security policies for the HSM.<br><b>Mandatory</b>                                                                                                                                              |
|                          | <b>Red</b><br>    | HSM Domain or Key Cloning Vector       | Cryptographically defines the set of HSMs that can participate in cloning for backup. See " <a href="#">Domain PED Keys</a> " on page 181.<br><b>Mandatory</b>                                                                                                               |
|                          | <b>Orange</b><br> | Remote PED Vector                      | Establishes a connection to a Remote PED server. See * below table.<br><b>Optional</b>                                                                                                                                                                                       |
| HSM Auditing             | <b>White</b><br>  | Auditor (AU) secret                    | Authenticates the Auditor role, responsible for audit log management. This role has no access to other HSM services.<br><b>Optional</b>                                                                                                                                      |
| Partition Administration | <b>Blue</b>                                                                                        | Partition Security Officer (PO) secret | Authenticates the Partition SO role. The PO manages provisioning activities and security policies for the partition.<br><b>NOTE:</b> If you want the HSM SO to also perform Partition SO duties, you can use the same blue key to initialize both roles.<br><b>Mandatory</b> |
|                          | <b>Red</b><br>  | Partition Domain or Key Cloning Vector | Cryptographically defines the set of partitions that can participate in cloning for backup or high-availability. See " <a href="#">Domain PED Keys</a> " on page 181.<br><b>Mandatory</b>                                                                                    |

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

\*

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

\*\*

**NOTE**

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

## Shared PED Key Secrets

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

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

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

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

### Domain PED Keys

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

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

For more information about cloning domains, see ["Domain Planning" on page 167](#).

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

### PED PINs

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

PED PINs can be set only at the time of key creation, and can be changed only by changing the secret on the PED key. Duplicate keys made at the time of creation can have different PED PINs, allowing multiple people access to the role (see ["Creating PED Keys" on page 224](#)). Copies made later are true copies with the same PED PIN, intended as backups for one person (see ["Duplicating Existing PED Keys" on page 234](#)). Duplicates of the PED key all have the same PED PIN.

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

**CAUTION!** Forgetting a PED PIN is equivalent to losing the key entirely; you can no longer authenticate the role, domain, or RPV. See ["Consequences of Losing PED Keys" on page 231](#).

## M of N Split Secrets (Quorum)

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

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

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

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

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

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

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

### Activated Partitions and M of N

For security reasons, the HSM and its servers are often kept in a locked facility, and accessed under specific circumstances, directly or by secure remote channel. To accommodate these security requirements, the Crypto Officer and Crypto User roles can be Activated (to use a secondary, alpha-numeric login credential to authenticate - Partition Policy 22), allowing applications to perform cryptographic functions without having to present a black or gray PED key (see "[Activation and Auto-activation on Multi-factor- \(PED-\) Authenticated Partitions](#)" on page 299). In this case, if the HSM is rebooted for maintenance or loses power due to an outage, the cached PED secret is erased and the role must be reactivated (by logging in the role via LunaCM and presenting the requisite M number, or quorum, of PED keys) before normal operations can resume. A further measure called Auto-Activation (Partition Policy 23) can cache the authenticated state as long as two hours, allowing automatic, hands-off resumption of operation.

## PED-Authenticated HSMs with Firmware 7.7.0 (and newer)

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

### Updated HSMs need updated PEDs

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

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

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

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

### Earlier version HSMs function with updated PEDs

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

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

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

### Orange PED Keys have changed

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

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

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

## New-series PED Behavior Notes

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

- > If a PED is connected via USB to a version 7.x HSM (whether that HSM is installed in a host computer or is embedded in a Network HSM appliance), if the server housing the HSM is booted from a power-off condition, the PED display might come up blank. The PED must be reset.

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

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

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

## Updating or Rolling-back PED-auth HSM Firmware

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

## Luna PED Received Items



This chapter describes the items you received with your Luna PED device. For instructions on setting up the PED, see ["PED Authentication" on page 176](#).

### Required Items

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

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



| Qty | Item                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|-----|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1   | <p data-bbox="245 268 1422 331"><b>PED Power Supply</b> kit with replaceable mains plug modules for international use (employed when the PED is operated in Remote PED mode)</p> <p data-bbox="245 373 1461 436"><b>NOTE:</b> If your PED has firmware 2.8.0 or newer, it contains refreshed internal hardware and is powered by USB connection. Refreshed PEDs are not shipped with the external power supply, as they do not need it.</p>  |
| 1   | <p data-bbox="245 974 1145 1010"><b>Cable, USB 2.0, Type A to Mini B connectors</b> (for Remote PED operation).</p>                                                                                                                                                                                                                                                                                                                        |

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

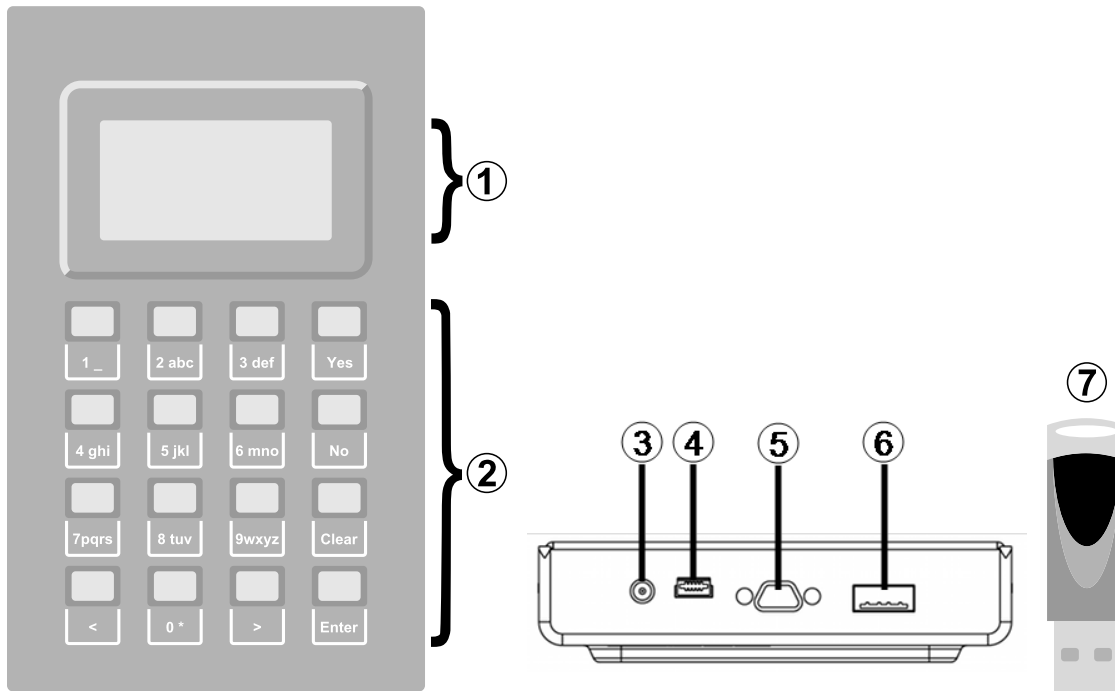
## Luna PED Hardware Functions

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

- > ["Physical Features" below](#)
- > ["Keypad Functions" on the next page](#)
- > ["Modes of Operation" on page 188](#)
- > ["Admin Mode Functions" on page 189](#)
- > ["PED with Newer CPU \(AC Power Block Now Optional\)" on page 189](#)

### Physical Features

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



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

\* PEDs with firmware version 2.8 and above are powered by any USB 2.x or 3.x connection, and do not have an external DC power supply. The PED driver must be installed on the connected computer. If the PED is connected to a hub or to a computer without the driver, then the PED display backlight illuminates, but no PED menu is presented.)

## Keypad Functions

The Luna PED keypad functions are as follows:

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

## Modes of Operation

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

- > **Local PED-SCP:** This mode is reserved for legacy Luna 6.x HSMs that use an MDSM connector between the PED and the HSM. It does not apply to Luna 7.x. Initial HSM configuration must be done in Local PED mode. See "[Local PED Setup](#)" on page 190 for instructions.
- > **Admin:** This mode is for upgrading the PED device firmware, diagnostic tests, and PED key duplication. See "[Admin Mode Functions](#)" on the next page for the functions available in this mode.
- > **Remote PED:** In this mode, the PED is connected to a remote workstation and authenticated to the HSM with an orange PED key containing a Remote PED Vector (RPV) secret. This mode allows the Luna Network HSM to be located in a data center or other location restricting physical access. See "[About Remote PED](#)" on page 191 for more information.
- > **Local PED-USB:** In this mode, the PED is connected directly to the HSM card with a USB mini-B to USB-A connector cable. Initial HSM configuration must be done in Local PED mode.

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

### Changing Modes

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

#### To change the Luna PED's active mode

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

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

PED V.2.7.1-5
```

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

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

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

### Admin Mode Functions

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

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

< EXIT
```

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

### PED with Newer CPU (AC Power Block Now Optional)

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

The older PED was shipped with an AC adapter.

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

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

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

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

## Local PED Setup

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

### Setting Up a Local PED Connection

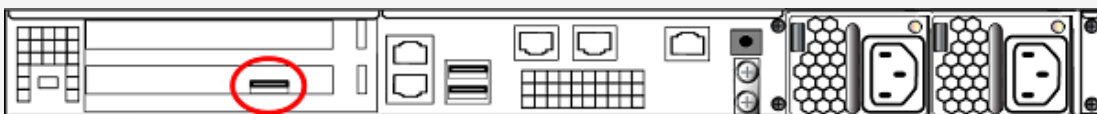
The Luna Network HSM administrator can use these directions to set up a Local PED connection. You require:

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

#### To set up a Local PED connection

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

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



2. PED version 2.8 and above is powered via the USB connection. If you are using PED version 2.7.1, connect it to power using the Luna PED DC power supply.

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

3. If you prefer to set the operation mode to **Local PED-USB** manually, see ["Changing Modes" on page 188](#).

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

## PED Actions

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

- > Wait for a PED authentication prompt in response to a LunaSH or LunaCM command (see ["Performing PED Authentication" on page 229](#))
- > Create copies of your PED keys (see ["Duplicating Existing PED Keys" on page 234](#))
- > Change to the Admin Mode to run tests or update PED software (see ["Changing Modes" on page 188](#))
- > Prepare to set up a Remote PED server (see ["About Remote PED" below](#))

## Secure Local PED

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

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

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

## About Remote PED

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

- > ["Remote PED Architecture" below](#)
- > ["Remote PED Connections" on the next page](#)
- > ["PEDserver-PEDclient Communications" on page 196](#)

## Remote PED Architecture

The Remote PED architecture consists of the following components:

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

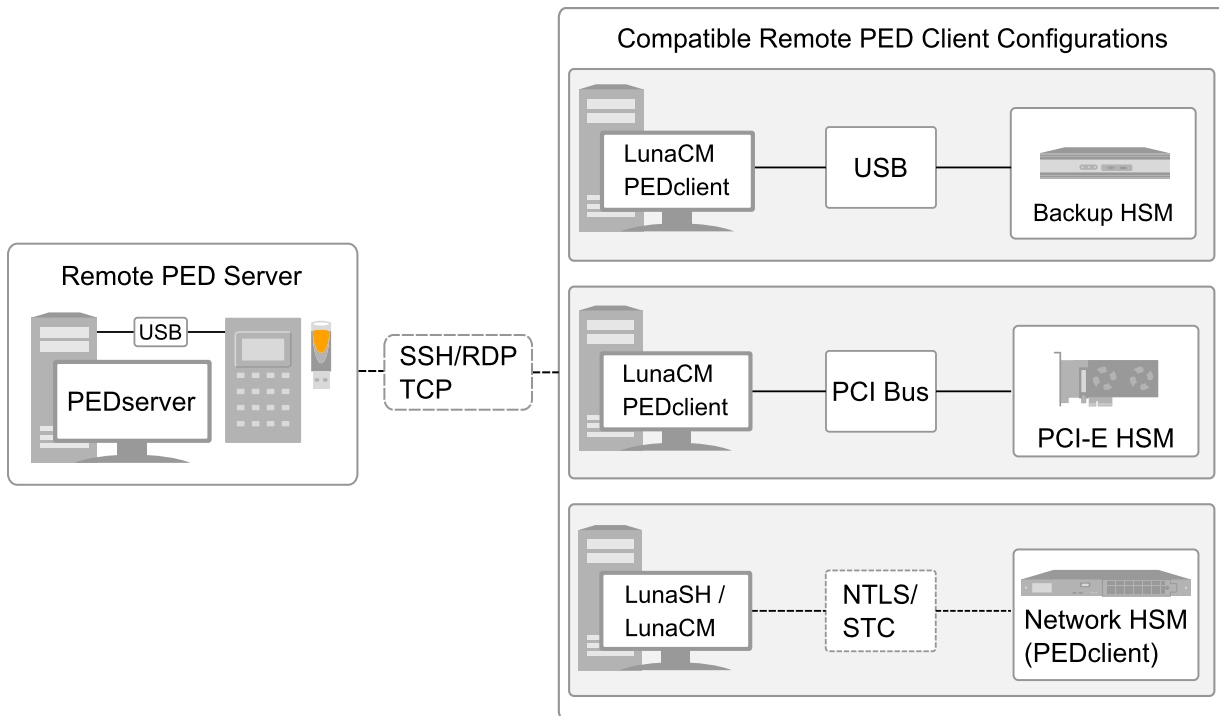
**NOTE** Luna PED firmware versions

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

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

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

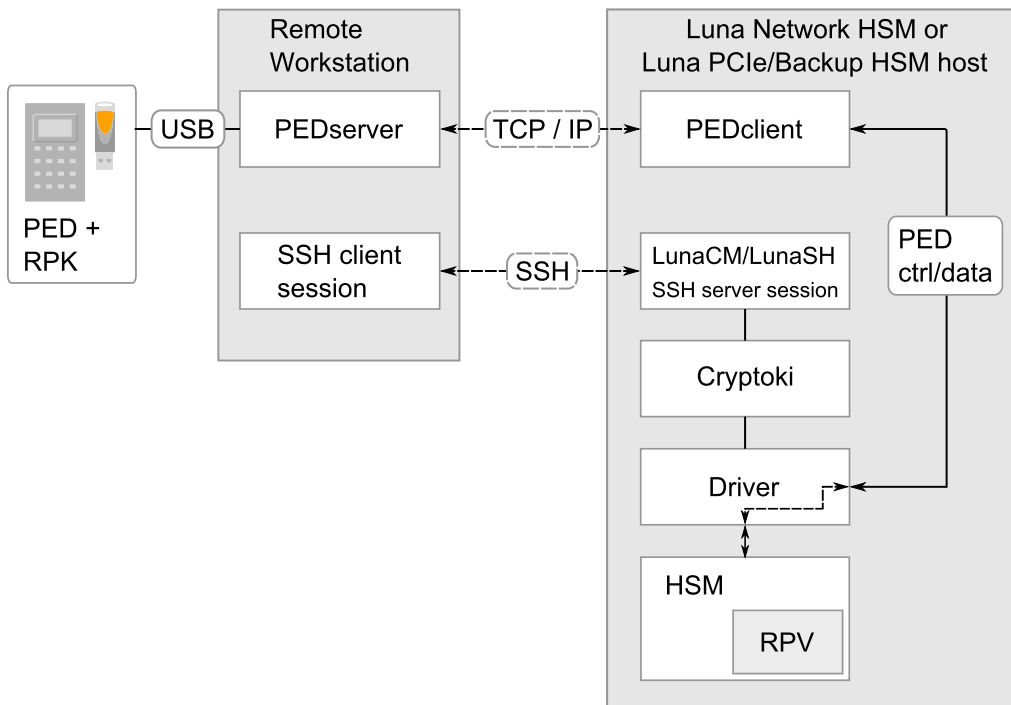




## Remote PED Connections

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

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



### Bi-directionality

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

- > **HSM-initiated:** When the HSM requires authentication, it sends (via PEDclient) a request for PED services to the Remote PED host (which receives the request via PEDserver). This requires that the Luna Network HSM be allowed to initiate external connections, and that the PEDserver IP port remains open. If the Luna Network HSM resides behind a firewall with rules prohibiting these connections, or if your IT policy prohibits opening a port on the Remote PED host, use a PED-initiated connection. See ["HSM-Initiated Remote PED" on page 202](#).
- > **PED-initiated:** The HSM and Remote PED host exchange and register certificates, creating a trusted connection. This allows the Remote PED host (via PEDserver) to initiate the connection to the Luna Network HSM. If you have firewall or other constraints that prevent your HSM from initiating a connection to a Remote PED in the external network, use this connection method. See ["PED-Initiated Remote PED" on page 206](#).

The following constraints apply to PED-initiated connections:

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

## Priority and Lockout

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

When a Remote PED connection is active, the Local PED connection is ignored, and all authentication requests are routed to the Remote PED. Attempts to connect to a different Remote PED server are refused until the current connection times out or is deliberately ended. See ["Ending or Switching the Remote PED Connection" on page 210](#).

## One Connection at a Time

Remote PED can provide PED services to only one HSM at a time. To provide PED service to another HSM, you must first end the original Remote PED connection. See ["Ending or Switching the Remote PED Connection" on page 210](#).

## Timeout

PEDserver and PEDclient both have configurable timeout settings (default: 1800 seconds). See ["pedserver - mode config" on page 245](#) or ["hsm ped timeout" on page 1](#). The utilities are not aware of each other's timeout values, so the briefer value determines the actual timeout duration. Timeout does not apply to PED-initiated Remote PED connections.

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

## Broken Connections

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

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

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

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

## PEDserver-PEDclient Communications

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

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

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

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

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

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

### PEDServer Configuration File

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

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

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

```

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

```

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

```

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

```

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

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

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

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

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

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

- > **Remote RPV Initialization:** The RPV is initialized using a Luna PED connected to a remote workstation running PEDserver. A one-time numeric password is used to authenticate the Remote PED to the HSM before initializing the RPV. This optional method is useful if the HSM SO has only remote SSH access to the appliance. It is available only if the HSM is in a zeroized state (uninitialized) and your firewall settings allow an HSM-initiated Remote PED connection. If you choose this method, you will set up Remote PED before initializing the RPV ("[Remote RPV Initialization](#)" on page 199).

Continue to "[Installing PEDserver and Setting Up the Remote Luna PED](#)" on page 200.

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

### Local RPV Initialization

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

- > Luna PED with firmware 2.7.1 or newer
- > USB mini-B to USB-A connector cable
- > Luna PED DC power supply (if included with your Luna PED)
- > Blank or reusable orange PED key (or multiple keys, if you plan to make extra copies or use an M of N security scheme). See ["Creating PED Keys" on page 224](#) for more information.

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

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

1. If you have not already done so, set up a Local PED connection (see ["Local PED Setup" on page 190](#)).
2. Using a serial or SSH connection, log in to the Luna Network HSM appliance as **admin**.
3. If the HSM is initialized, login as HSM SO (see [Logging In as HSM Security Officer](#)). If not, skip to the next step.

```
lunash:> hsm login
```

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

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

5. Attend to the Luna PED and respond to the on-screen prompts. See ["Creating PED Keys" on page 224](#) for a full description of the key-creation process.

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

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

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

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

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

### Remote RPV Initialization

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

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

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

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

- > A blank or reusable orange PED key (or multiple keys, if you plan to make extra copies or use an M of N security scheme). See ["Creating PED Keys" on page 224](#) for more information.
- > The HSM must be in a zeroized state and the RPV uninitialized.

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

1. Open an HSM-initiated Remote PED connection.

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

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

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

```
Enter PED Password:
```

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

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

```
SLOT
COMPUTE SESSION KEY.

Enter PED Password.

*****█
```

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

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

4. Attend to the Luna PED and respond to the on-screen prompts. See "[Creating PED Keys](#)" on page 224 for a full description of the key-creation process.

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

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

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

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

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

## Installing PEDserver and Setting Up the Remote Luna PED

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

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

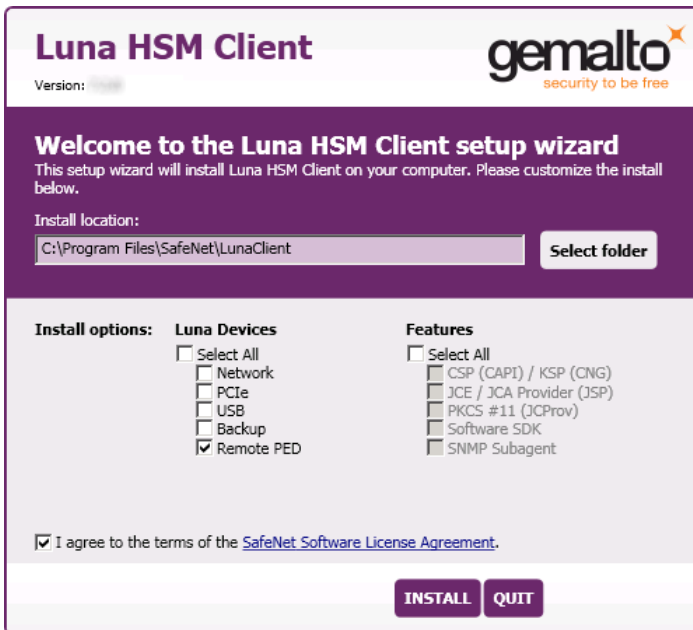
**NOTE** To set up a Remote PED Server on Linux, you require Luna HSM Client 10.1.0 or newer.

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

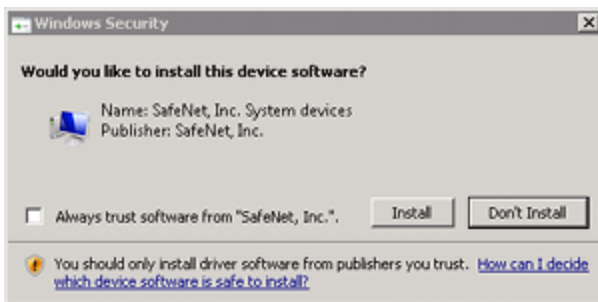
1. Run the Luna HSM Client installer and follow the on-screen instructions, as detailed in "[Luna HSM Client Software Installation](#)" on page 17, and select the **Luna Remote PED** option. Any additional installation



choices are optional, for the purpose of this procedure.



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



3. On Windows, reboot the computer to ensure that the Luna PED driver is accepted by Windows. This step is not required for Linux or Windows Server operating systems.
4. Connect the Luna PED to a USB port on the host system using the supplied USB mini-B to USB-A connector cable.

PED version 2.8 and above is powered via the USB connection. If you are using PED version 2.7.1, connect it to power using the Luna PED DC power supply.

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

To manually set the operation mode to **Remote PED**, see "[Changing Modes](#)" on page 188.

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

- c. Reconnect the Luna PED.

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

## Opening a Remote PED Connection

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

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

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

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

See ["PED-Initiated Remote PED" on page 206](#).

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

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

If you encounter issues, see ["Remote PED Troubleshooting" on page 211](#).

### HSM-Initiated Remote PED

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

- > Administrative access to a network-connected workstation with PEDserver installed and Luna PED connected (see ["Installing PEDserver and Setting Up the Remote Luna PED" on page 200](#))
- > Administrative access to the Luna Network HSM via SSH (if using Remote PED for HSM-level authentication)
- > Administrative access to a Luna HSM Client workstation with an assigned user partition (if using Remote PED for partition-level authentication)
- > One of the following:
  - Orange PED key with the HSM's RPV (see ["Initializing the Remote PED Vector and Creating an Orange Remote PED Key" on page 197](#))
  - Blank orange PED key (or multiple keys, if you plan to use an M of N scheme)

## To launch PEDserver

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

2. Navigate to the Luna HSM Client install directory.

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

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

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

> **"pedserver -mode start" on page 251** [-ip <PEDserver\_IP>]

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

4. Verify that the service has launched successfully.

> **"pedserver -mode show" on page 249**

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

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

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

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

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

Client Information: Not Available

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

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

```

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

```

Show command passed.

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

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

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

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

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

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

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

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

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

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

```
Enter PED Password:
```

See ["Remote RPV Initialization" on page 199](#) for this procedure.

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

```

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

```

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

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

The HSM-initiated Remote PED connection is now open.

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

- If the HSM is already initialized and you have the blue HSM SO key, you can use `lunash:> hsm login`.
- If the HSM is uninitialized, you can initialize it now with `lunash:> hsm init -label <label>`. Have blank or reusable blue and red PED keys ready (or multiple blue and red keys for M of N or to make multiple copies). See ["Creating PED Keys" on page 224](#) for more information.

**NOTE** The HSM-initiated Remote PED connection eventually times out (default: 1800 seconds), and must be re-initiated each time authentication is required. To simplify this process, you can set a default IP address and/or port for LunaSH to use each time you connect. To drop the Remote PED connection manually, see ["Ending or Switching the Remote PED Connection" on page 210](#).

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

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

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

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

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

**NOTE** If you want to use the Remote PED to authenticate a different HSM, you must first drop the current connection. See ["Ending or Switching the Remote PED Connection" on page 210](#).

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

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

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

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

```
Command Result : No Error
```

3. Issue the first command that requires authentication.

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

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

- If the partition is uninitialized, you can initialize it now. Have blank or reusable blue and red PED keys ready (or multiple blue and red keys for MofN or for multiple copies). See ["Creating PED Keys" on page 224](#) for more information on creating PED keys.

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

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

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

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

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

**NOTE** The HSM-initiated Remote PED connection eventually times out (default: 1800 seconds), and must be re-initiated each time authentication is required. To simplify this process, you can set a default IP address and/or port for LunaCM to use each time you connect. To drop the Remote PED connection manually, see ["Ending or Switching the Remote PED Connection" on page 210](#).

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

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

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

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

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

**NOTE** If you want to use the Remote PED to authenticate a different HSM, you must first drop the current connection. See ["Ending or Switching the Remote PED Connection" on page 210](#).

### PED-Initiated Remote PED

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

- > Administrative access to a network-connected workstation with PEDserver installed and Luna PED connected (see ["Installing PEDserver and Setting Up the Remote Luna PED" on page 200](#))

- > Orange PED key with the HSM's RPV (see ["Initializing the Remote PED Vector and Creating an Orange Remote PED Key" on page 197](#))
- > Administrative access to the Luna Network HSM via SSH

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

### To open a PED-initiated Remote PED connection

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

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

#### > **"pedserver -regen" on page 255 -commonname <name>**

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

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

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

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

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

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

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

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

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

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

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

```
>pscp .\cert\client\

```

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

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

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

```
>"pedserver -appliance register" on page 243 -name <appliance_name> -certificate <cert_filename>
-ip <appliance_IP> -port <port>
```

- Open an SSH session to the Luna Network HSM and log in to LunaSH as **admin**.
- Register the PEDserver host certificate.

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

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

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

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

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

```
>"pedserver -mode connect" on page 247 -name <appliance_name>
```

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

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

```
Successfully connected to myLunaHSM.
```

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

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

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

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

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

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

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

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

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



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

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

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

### Workaround when you need PED-initiated Remote PED for Client

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

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

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

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

#### Example:

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

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

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

```
<snip>
```

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

```
Callback Server Information:
```

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

```
Operating Information:
```

```
 Admin Port: 1501
```

```
:
```

```
<snip>
```

```
:
```

```
Show command passed.
```

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

```
lunash:>
```

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

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

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

```
lunacm:> ped connect
```

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

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

```
lunacm:> ped connect
```

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

```
lunacm:> ped connect
```

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

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

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

## Ending or Switching the Remote PED Connection

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

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

1. End the Remote PED connection.

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

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

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

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

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

1. End the Remote PED connection.

```
lunacm:> ped disconnect
```

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

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

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

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

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

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

2. Check the available list of Remote PED servers.

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

If the Remote PED you want to use is not in the list, see ["PED-Initiated Remote PED" on page 206](#).

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

> ["pedserver -mode connect" on page 247](#) -name <appliance\_name>

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

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

## Remote PED Troubleshooting

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

- > ["No Menu Appears on PED Display: Ensure Driver is Properly Installed" on the next page](#)
- > ["RC\\_SOCKET\\_ERROR: PEDserver Requires Administrator Privileges" on the next page](#)

- > ["LUNA\\_RET\\_PED\\_UNPLUGGED: Reconnect HSM-initiated Remote PED Before Issuing Commands" below](#)
- > ["Remote PED Firewall Blocking" on the next page](#)
- > ["Remote PED Blocked Port Access" on page 214](#)
- > ["ped connect Fails if IP is Not Accessible" on page 215](#)
- > ["PEDserver on VPN fails" on page 215](#)

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

If the PED driver is not properly installed before connecting the PED to the workstation's USB port, the PED screen does not display the menu. If you encounter this problem, ensure that you have followed the entire procedure at ["Installing PEDserver and Setting Up the Remote Luna PED" on page 200](#).

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

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

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

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

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

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

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

```
lunash:>hsm login
```

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

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

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

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

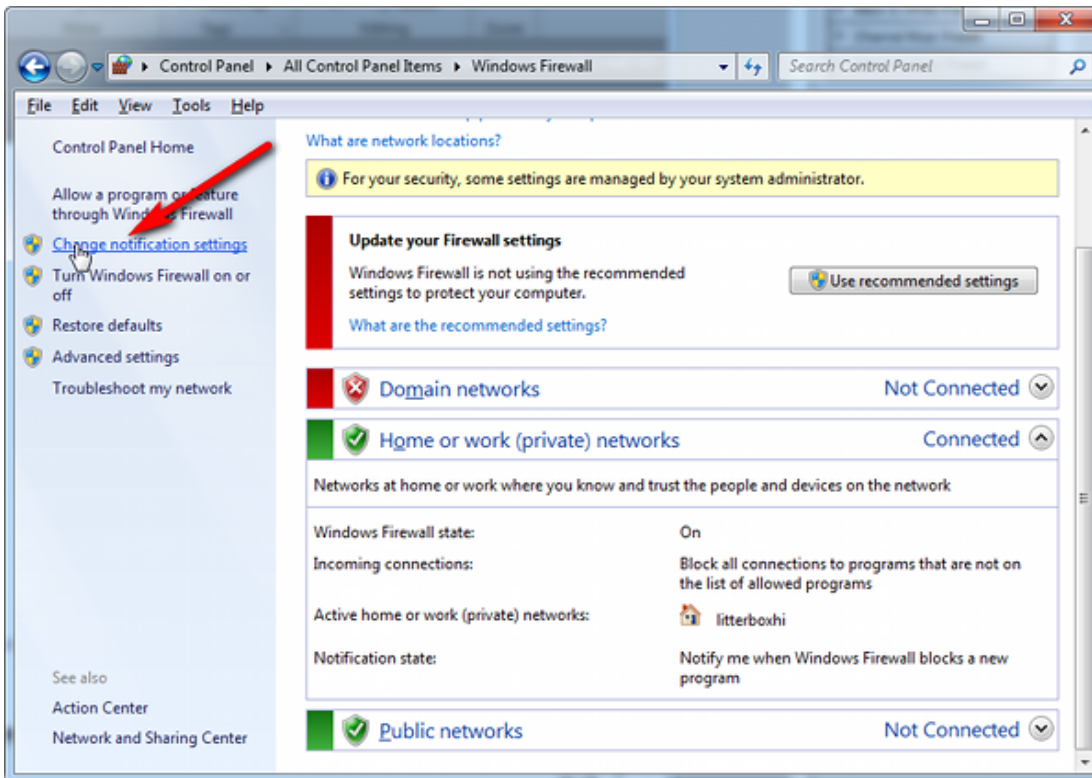
```
lunash:> hsm ped connect -ip <PEDserver_IP> -port <PEDserver_port>
```

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

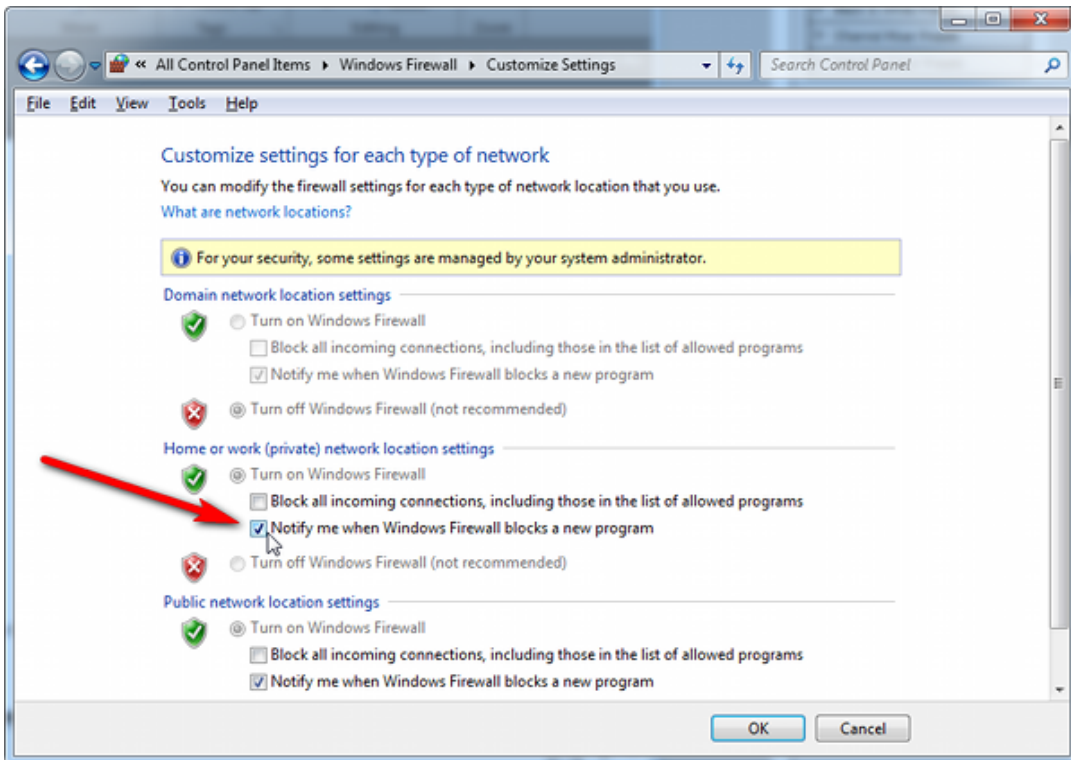
## Remote PED Firewall Blocking

If you experience problems while attempting to configure a SafeNet Remote PED session over VPN, you might need to adjust Windows Firewall settings. If your security policy prohibits changes to Windows Firewall, you can use a PED-initiated connection for HSM SO-level operations. See "[PED-Initiated Remote PED](#)" on page 206.

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



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



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

### Remote PED Blocked Port Access

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

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

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

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

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

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

### **ped connect Fails if IP is Not Accessible**

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

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

### **PEDserver on VPN fails**

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

1. Close the current command prompt window.
2. Open a new Administrator command prompt.
3. Verify the current IP address.  
>**ipconfig**
4. Start PEDserver, specifying the new IP and port number ().  
> "**pedserver -mode start**" on page 251 **-ip** <new\_IP> **-port** <port>

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

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

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

The callback service also restarts when the appliance is rebooted.

## **Migrating the Orange Remote PED Key For Luna 7.7.0 or Newer**

Luna HSM firmware 7.7.0 introduces a new PED protocol for securing local and remote PED connections. In addition to the Luna PED firmware upgrade, any existing orange keys must be migrated to use the new protocol, or you must create a new orange key using a local PED connection after updating the HSM to firmware 7.7.0+ (see "[Initializing the Remote PED Vector and Creating an Orange Remote PED Key](#)" on page 197). If you choose to migrate existing orange key(s), use one of the following procedures:

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

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

## Prerequisites

- > Ensure that you have a backup orange PED key (or M of N set). If you do not have backups, see ["Duplicating Existing PED Keys" on page 234](#) for the procedure.
- > Thales recommends migrating the full M of N set of orange keys at the same time. You must have the full set, and any existing duplicate sets, present at the time of migration. If you do not have all duplicate keysets present, they can be migrated at a later time using this same procedure, or you can create new duplicates from an already-migrated keyset.
- > Depending on your Luna PED hardware, you require the following minimum firmware versions to authenticate with Luna 7.7.0 (see ["Updating Luna PED Firmware \(for older-version PED that requires a power-block\)" on page 218](#)):
  - Luna PED firmware 2.7.4 or newer for older PED
  - Luna PED firmware 2.9.0 or newer for refreshed PED
- > The Luna Network HSM firmware must be at minimum firmware version 7.7.0 (see [Updating the Luna HSM Firmware](#)).
- > The migration process takes about one minute per key. If you are migrating many keys (multiple duplicate copies of M of N splits, for example) you may need to adjust the PED timeouts on your appliance or client to ensure that you can complete the procedure.

For example, if you are migrating an M of N split of 3 keys, with one set of backups, Thales recommends using the following minimum timeout settings under the **Luna** section of the Luna HSM Client configuration file (see ["Configuration File Summary" on page 70](#)). Estimate your actual settings based on the number of keys you are migrating:

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

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

```
lunash:> hsm ped timeout set -type pedk -seconds 600
lunash:> hsm ped timeout set -type pedo -seconds 1220
```

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

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

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

1. Choose LunaSH or LunaCM to initiate the procedure:



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

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

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

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

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

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

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

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

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

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

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

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

If it is possible to gather all your existing orange keys into one place, you can also migrate your orange keys for Luna 7.7.0 using a Luna PED connected directly to the Luna Network HSM (see ["Local PED Setup" on page 190](#)).

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

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

2. Log in to the HSM.

```
lunash:> hsm login
```

3. Ensure that the Luna PED is in **Local-USB** mode (see ["Changing Modes" on page 188](#)).

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

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

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

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

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

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

**NOTE** If your Luna PED is the newer model that is powered by a USB connection (and is not shipped with a power-block), see "[Updating Luna PED Firmware \(for USB-powered PED\)](#)" on page 221.

### Files Included in the Upgrade Package

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

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

### Preparing for the Update

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

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

### To prepare your computer for the update

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

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

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

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

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

## Updating the Luna PED Firmware

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

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

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

## To update the Luna PED firmware

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

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

**NOTE** If you have both older Luna PEDs (that are powered by a power block and addressed on "Updating Luna PED Firmware (for older-version PED that requires a power-block)" on page 218 ), and the newer Luna PEDs (powered by USB connection and addressed on this page), then the LunaPED\_Update.exe files for each are different and not interchangeable.

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

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

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

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

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

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

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

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

```
Software update
Success
Press ENTER
```

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

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

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

## Troubleshooting

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

If your update attempt fails with a Receive error (rx error), check if you have Remote PED services running on the computer to which the PED is connected.

Issue the command **PedServer -m stop** and restart the update to resolve the problem.

### No PED Prompts

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

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

### Files Uploaded in the Wrong Order

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

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

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

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

### Upgrade Failed Message (or Similar)

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

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

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

## Updating Luna PED Firmware (for USB-powered PED)

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

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

If your Luna PED is the older type, that was shipped with a power-block, then do not use these instructions; see ["Updating Luna PED Firmware \(for older-version PED that requires a power-block\)" on page 218](#) instead.

## Preparing for the Upgrade

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

### Prepare your computer for the upgrade

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

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

**NOTE** If you have both older Luna PEDs (that are powered by a power block and addressed on "[Updating Luna PED Firmware \(for older-version PED that requires a power-block\)](#)" on [page 218](#) ), and the newer Luna PEDs (powered by USB connection and addressed on this page), then the LunaPED\_Update.exe files for each are different and *not interchangeable*.

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

### Prepare the Luna PED for the firmware upgrade

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

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

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

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

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

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

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

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

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

### Transfer and confirm the PED FW Update

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

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

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

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

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

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

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

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

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

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

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

## Done

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

## PED Key Management

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

- > ["Creating PED Keys" below](#)
  - ["Stage 1: Reusing Existing PED Keys" on the next page](#)
  - ["Stage 2: Defining M of N" on page 227](#)
  - ["Stage 3: Setting a PED PIN" on page 227](#)
  - ["Stage 4: Duplicating New PED Keys" on page 229](#)
- > ["Performing PED Authentication" on page 229](#)
- > ["Consequences of Losing PED Keys" on page 231](#)
- > ["Identifying a PED Key Secret" on page 233](#)
- > ["Duplicating Existing PED Keys" on page 234](#)
- > ["Changing a PED Key Secret" on page 235](#)

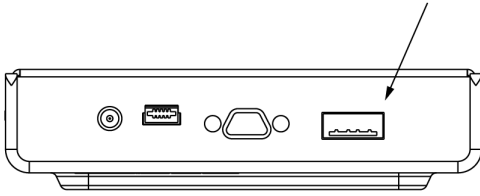
## Creating PED Keys

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

- > If you are reusing an existing PED key or keyset, the owners of those keys must be present with their keys and PED PINs ready.
- > If you plan to use an M of N authentication scheme (quorum, or split-secret), all the parties involved must be present and ready to create their authentication split. It is advisable for each key holder to create backup duplicates, so you must have a sufficient number of blank or rewritable PED keys ready before you begin.
- > If you plan to make backup duplicates of PED keys, you must have a sufficient number of blank or rewritable PED keys ready.
- > If you plan to use PED PINs, ensure that they can be privately entered on the Luna PED and memorized, or written down and securely stored.

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





## To initiate PED key creation

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

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

```
lunash:> hsm init
```

- **Orange Remote PED Key:**

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

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

```
lunacm:> partition init
```

- **Black Crypto Officer Key:**

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

- **Gray Crypto User Key:**

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

- **White Audit User Key:**

```
lunash:> audit init
```

The Luna PED responds, displaying:

```
Remote PED mode
Token found
```

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

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

### Stage 1: Reusing Existing PED Keys

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

- > You want to use the same blue SO key to authenticate multiple HSMs/partitions

- > You want to initialize a partition in an already-existing cloning domain (to be part of an HA group)

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

See "[Shared PED Key Secrets](#)" on page 180 and "[Domain PED Keys](#)" on page 181 for more information.

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

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

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

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

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

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

```

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

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

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

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

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

## Stage 2: Defining M of N

If you chose to create a new keyset, the Luna PED prompts you to define the M of N scheme (quorum and pool of splits) for the role, domain, or vector. See "[M of N Split Secrets \(Quorum\)](#)" on page 182 for more information. If you do not want to use M of N (authentication by one PED key), enter a value of **1** for both M and N.

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

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

>03
```

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

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

>05
```

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

## Stage 3: Setting a PED PIN

If you are creating a new key or M of N split, you have the option of setting a PED PIN that must be entered by the key owner during authentication. PED PINs must be 4-48 digits long. Do not use 0 for the first digit. See "[PED PINs](#)" on page 181 for more information.

**CAUTION!** If you forget your PED PIN, it is the same as losing the PED key entirely; you cannot authenticate the role. See "[Consequences of Losing PED Keys](#)" on page 231.

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

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

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

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

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

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

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

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

3. The PED prompts you for a PIN.

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

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

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

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

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

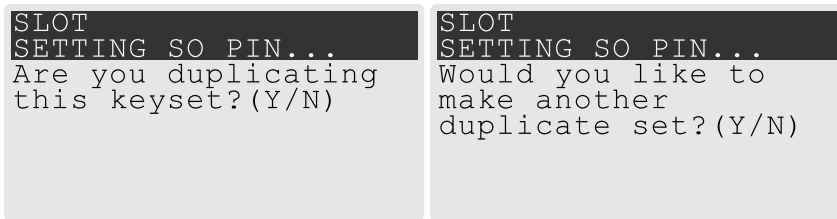
## Stage 4: Duplicating New PED Keys

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

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

You can make backups now or later. See also ["Duplicating Existing PED Keys" on page 234](#).

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



- If you select **No**, the key creation process is complete.
  - If you select **Yes**, complete ["Stage 3: Setting a PED PIN" on page 227](#) for the duplicate keyset. You can set the same PED PIN to create a true copy, or set a different PED PIN for each duplicate.
2. If you specified an M of N scheme, you are prompted to repeat ["Stage 3: Setting a PED PIN" on page 227](#) for each M of N split. Otherwise, the key creation process is complete.

## Performing PED Authentication

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

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

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

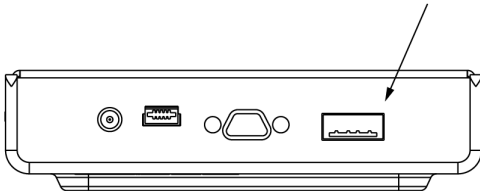
When you issue a command that requires PED interaction, the interface returns a message like the following:

```
lunash:>hsm login
```

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

```
Remote PED mode
Token found
```

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



**CAUTION!** Multiple failed authentication attempts result in zeroization of the HSM or partition, or role lockout, depending on the role. This is a security measure designed to thwart repeated, unauthorized attempts to access cryptographic material. For details, see [Logging In as HSM Security Officer](#) or "Before you can perform administrative tasks on the partition or its stored cryptographic objects, you must log in with the appropriate role:" on page 294.

## To perform PED authentication

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

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

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

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

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

```
Command Result : No Error
```

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

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

```

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

Command Result : No Error

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

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

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

Command Result : No Error

## Consequences of Losing PED Keys

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

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

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

- > ["Blue HSM SO Key" below](#)
- > ["Red HSM Domain Key" on the next page](#)
- > ["Orange Remote PED Key" on the next page](#)
- > ["Blue Partition SO Key" on the next page](#)
- > ["Red Partition Domain Key" on the next page](#)
- > ["Black Crypto Officer Key" on page 233](#)
- > ["Gray Crypto User Key" on page 233](#)
- > ["White Audit User Key" on page 233](#)

### Blue HSM SO Key

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

1. Contact all Crypto Officers and have them immediately make backups of their existing partitions.
2. When all important partitions are backed up, execute a factory reset of the HSM.

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

### Red HSM Domain Key

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

### Orange Remote PED Key

If the Remote PED Vector is lost, create a new one and distribute a copy to the administrator of each Remote PED server. See ["Initializing the Remote PED Vector and Creating an Orange Remote PED Key" on page 197](#).

### Blue Partition SO Key

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

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

### Red Partition Domain Key

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

1. Have the HSM SO create a new partition (or multiple partitions, to replace the entire HA group) and assign it to the same client(s).
2. Initialize the partition(s) with a new cloning domain.



3. Initialize the Crypto Officer role with the original black Crypto Officer key (and Activation password, if applicable).
4. Create objects on the new partition to replace those on the original partition.
5. As soon as possible, change all applications to use the objects on the new partition.
6. When objects on the original partition are no longer in production use, the HSM SO can delete the original partition.

### Black Crypto Officer Key

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

#### > PIN reset by Partition SO:

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

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

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

#### > Partition Activation:

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

#### > Crypto User

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

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

### Gray Crypto User Key

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

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

### White Audit User Key

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

## Identifying a PED Key Secret

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

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

- > who the key belongs to

You require:

- > Luna PED in Admin Mode (see ["Changing Modes" on page 188](#))
- > the key you want to identify

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

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

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

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

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

The PED secret type is identified on-screen.

```
PED Key mode
Found keys:
Domain

Press ENTER.
```

## Duplicating Existing PED Keys

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

- > Luna PED in Admin Mode (see ["Changing Modes" on page 188](#))
- > Enough blank or rewritable keys to make your copies

The PED key is duplicated exactly by this process. If there is a PED PIN assigned, the same PIN is assigned to the duplicate key. If the key is part of an M of N scheme, the duplicates may not be used in the same login process to satisfy the M of N requirements. You must also have copies of the other keys in the M of N keyset. See ["M of N Split Secrets \(Quorum\)" on page 182](#).

### To duplicate an existing PED key

1. Insert the PED key you want to duplicate. Have a blank or rewritable PED key ready.

- From the Admin mode menu, press **1** on the keypad to login to the PED key.

```

PED Key mode
 1 Login
 3 List types

< EXIT

```

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

```

PED Key mode
 2 Logout
 3 List types
 7 Duplicate

< EXIT

```

## Changing a PED Key Secret

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

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

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

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

- > ["Blue HSM SO Key" on the next page](#)
- > ["Red HSM Domain Key" on the next page](#)
- > ["Orange Remote PED Key" on the next page](#)
- > ["Blue Partition SO Key" on the next page](#)
- > ["Red Partition Domain Key" on page 237](#)
- > ["Black Crypto Officer Key" on page 237](#)
- > ["Gray Crypto User Key" on page 237](#)
- > ["White Audit User Key" on page 237](#)

## Blue HSM SO Key

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

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

1. In LunaSH, log in as HSM SO.  
lunash:> **hsm login**
2. Initiate the PED key change.  
lunash:> **hsm changepw**
3. You are prompted to present the original blue key(s) and then to create a new HSM SO keyset. See ["Creating PED Keys" on page 224](#).

## Red HSM Domain Key

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

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

## Orange Remote PED Key

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

### To change the RPV/orange key credential

1. In LunaSH, log in as HSM SO.  
lunash:> **hsm login**
2. Initialize the RPV.  
lunash:> **hsm ped vector init**  
You are prompted to create a new Remote PED key.
3. Distribute a copy of the new orange key to the administrator of each Remote PED server.

## Blue Partition SO Key

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

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

1. In LunaCM, log in as Partition SO.  
lunacm:> **role login -name po**
2. Initiate the PED key change.  
lunacm:> **role changepw -name po**
3. You are prompted to present the original blue key(s) and then to create a new Partition SO keyset.

## Red Partition Domain Key

It is not possible to change a partition's cloning domain. A new partition must be created and initialized with the desired domain. The new partition will not have access to any of the original partition's backups. It cannot be made a member of the same HA group as the original.

## Black Crypto Officer Key

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

---

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

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

## Gray Crypto User Key

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

---

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

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

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

## White Audit User Key

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

---

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

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

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

## PEDserver and PEDclient

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

### The PEDserver Utility

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

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

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

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

### The PEDclient Utility

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

The PEDclient utility performs the following functions:

- > It mediates between the HSM where it is installed and the Luna PED where PEDserver is installed, to provide PED services to the requesting HSM(s).
- > It resides on a computer with RBS and an attached Luna Backup HSM, and it connects with another instance of PEDclient on a distant host of an HSM, to provide the link component for Remote Backup Service. See ["Configuring a Remote Luna Backup HSM \(G5\) Server" on page 406](#) for more information.
- > It acts as the logging daemon for HSM audit logs.

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

Thus, for example, in the case where an administrative workstation or laptop has both a Remote PED and a Remote Backup HSM attached, PEDclient would perform double duty. It would link with a locally-running instance of PEDserver, to convey HSM requests from the locally-connected Backup HSM to the locally-connected PED, and return the PED responses. As well, it would link a locally-running instance of RBS and a distant PEDclient instance to mediate Remote Backup function for that distant HSM's partitions. See ["Configuring a Remote Luna Backup HSM \(G5\) Server" on page 406](#) for more information.

See ["pedclient" on page 255](#).

## pedserver

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

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

### Syntax

#### pedserver

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

Option	Description
<b>-appliance</b>	Registers or deregisters an appliance, or lists the registered appliances. Applies to server-initiated (peer-to-peer) mode only. See <a href="#">"pedserver -appliance" on the next page</a> .
<b>-mode</b>	Specifies the mode that the PED Server will be executed in. See <a href="#">"pedserver mode" on page 244</a> .
<b>-regen</b>	Regenerates the client certificate. Applies to server-initiated (peer-to-peer) mode only. See <a href="#">"pedserver -regen" on page 255</a> .

## pedserver -appliance

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

### Syntax

#### pedserver -appliance

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

Option	Description
<b>delete</b>	Deregisters an appliance. See " <a href="#">pedserver -appliance delete</a> " on the next page.
<b>list</b>	Lists the registered appliances. See " <a href="#">pedserver -appliance list</a> " on page 242.
<b>register</b>	Registers an appliance. See " <a href="#">pedserver -appliance register</a> " on page 243



---

## pedserver -appliance delete

---

Deregister an appliance certificate from PEDserver.

### Syntax

**pedserver -appliance delete -name <unique name> [-force]**

Option	Description
<b>-name</b> <unique name>	Specifies the name of the appliance to be deregistered from PEDserver.
<b>-force</b>	Optional parameter. Suppresses any prompts.

### Example

```
C:\Program Files\Safenet\LunaClient>pedServer -appliance delete -name hello -force
```

---

## pedserver -appliance list

---

Displays a list of appliances registered with PEDserver.

### Syntax

**pedserver -appliance list**

### Example

```
C:\Program Files\Safenet\LunaClient>pedServer -appliance list
```

```
>
```

Server Name	IP Address	Port Number	Certificate Common Name
-------------	------------	-------------	----------------------------

abox	192.20.1.23	9697	test2
bbox	192.20.12.34	9696	test1
hello	192.20.1.34	9876	hellocert

## pedserver -appliance register

Register an appliance certificate with PEDserver.

### Syntax

**pedserver -appliance register -name** <unique name> **-certificate** <appliance certificate file> **-ip** <appliance server IP address> [**-port** <port number>]

Option	Description
<b>-name</b> <unique name>	Specifies the name of the appliance to be registered to PED Server.
<b>-certificate</b> <appliance certificate file>	Specifies the full path and filename of the certificate that was retrieved from the appliance.
<b>-ip</b> <appliance server IP address>	Specifies the IP address of the appliance server.
<b>-port</b> <port number>	Optional field. Specifies the port number used to connect to the appliance (directly or indirectly according to network configuration). <b>Range:</b> 0-65525

### Example

```
C:\Program Files\Safenet\LunaClient>pedServer -appliance register -name hello -certificate the-best-appliance.pem -ip 123.321.123.321 -port 9697
```

## pedserver mode

Specifies the mode that PEDserver will be executed in.

### Syntax

#### pedserver -mode

```

config
connect
disconnect
show
start
stop

```

Option	Description
<b>config</b>	Modifies or shows existing configuration file settings. See " <a href="#">pedserver -mode config</a> " on the next page.
<b>connect</b>	Connects to the appliance. See " <a href="#">pedserver -mode connect</a> " on page 247.
<b>disconnect</b>	Disconnects from the appliance. See " <a href="#">pedserver -mode disconnect</a> " on page 248.
<b>show</b>	Queries if PEDserver is currently running, and gets details about PEDserver. See " <a href="#">pedserver -mode show</a> " on page 249.
<b>start</b>	Starts PEDserver. See " <a href="#">pedserver -mode start</a> " on page 251.
<b>stop</b>	Shuts down PEDserver. See " <a href="#">pedserver -mode stop</a> " on page 253

## pedserver -mode config

Shows and modifies internal PEDserver configuration file settings.

### Syntax

```
pedserver -mode config -name <registered appliance name> -show -set [-port <server port>] [-set][-configfile <filename>] [-admin <admin port number>] [-eserverport <0 or 1>] [-eadmin <0 or 1>] [-idletimeout <int>] [-socketreadtimeout <int>] [-socketwritetimeout <int>] [-internalshutdowntimeout <int>] [-bgprocessstartuptimeout <int>] [-bgprocessshutdowntimeout <int>] [-logfile <filename>] [-loginfo <0 or 1>] [-logwarning <0 or 1>] [-logerror <0 or 1>] [-logtrace <0 or 1>] [-maxlogfilesize <size>] [-pinginterval <int>] [-pingtimeout <int>]
```

Option	Description
<b>-name</b> <registered appliance name>	Specifies the name of the registered appliance to be configured.
<b>-show</b>	Displays the contents of the PEDserver configuration file.
<b>-set</b>	Updates the PEDserver configuration file to be up to date with other supplied options.
<b>-port</b> <server port>	Optional. Specifies the server port number.
<b>-configfile</b> <filename>	Optional. Specifies which PEDserver configuration file to use.
<b>-admin</b> <admin port number>	Optional. Specifies the administration port number.
<b>-eserverport</b> <0 or 1>	Optional. Specifies if the server port is on "localhost" or listening on the external host name.
<b>-eadmin</b> <0 or 1>	Optional. Specifies if the administration is on "localhost" or listening on the external host name.
<b>-idletimeout</b> <int>	Optional. Specifies the idle connection timeout, in seconds.
<b>-socketreadtimeout</b> <int>	Optional. Specifies the socket read timeout, in seconds.
<b>-socketwritetimeout</b> <int>	Optional. Specifies socket write timeout, in seconds.
<b>-internalshutdowntimeout</b> <int>	Optional. Specifies the shutdown timeout for internal services, in seconds.
<b>-bgprocessstartuptimeout</b> <int>	Optional. Specifies the startup timeout for the detached process, in seconds.

Option	Description
<b>-bgprocessshutdowntimeout</b> <int>	Optional. Specifies the shutdown timeout for the detached process, in seconds.
<b>-logfile</b> <filename>	Optional. Specifies the log file name to which the logger should log messages.
<b>-loginfo</b> <0 or 1>	Optional. Specifies if the logger should log "info" messages. Set to 0 for no, 1 for yes.
<b>-logwarning</b> <0 or 1>	Optional. Specifies if the logger should log "warning" messages. Set to 0 for no, 1 for yes.
<b>-logerror</b> <0 or 1>	Optional. Specifies if the logger should log "error" messages. Set to 0 for no, 1 for yes.
<b>-logtrace</b> <0 or 1>	Optional. Specifies if the logger should log "trace" messages. Set to 0 for no, 1 for yes.
<b>-maxlogfilesize</b> <size>	Optional. Specifies the maximum log file size in KB.
<b>-pinginterval</b> <int>	Optional. Specifies the time interval between ping commands, in seconds.
<b>-pingtimeout</b> <int>	Optional. Specifies timeout of the ping response, in seconds.

## Example

```
C:\Program Files\Safenet\LunaClient>pedServer -mode config -name hellohi -show
```

## pedserver -mode connect

Connects to the appliance by retrieving information (IP address, port, PEDserver certificate) from the PEDserver configuration file.

If the running mode is legacy, an error is returned. **pedserver -mode connect** is not a valid command for legacy connections.

The **connect** command will try connecting to PEDclient 20 times before giving up.

### Syntax

**pedserver -mode connect -name** <registered appliance name> [-**configfile** <filename>] [-**logfile** <filename>] [-**loginfo** <0 or 1>] [-**logwarning** <0 or 1>] [-**logerror** <0 or 1>] [-**logtrace** <0 or 1>] [-**maxlogfilesize** <size>]

Option	Description
<b>-name</b> <registered appliance name>	Specifies the name of the registered appliance to be connected to PEDserver.
<b>-configfile</b> <filename>	Optional. Specifies which PEDserver configuration file to use.
<b>-logfile</b> <filename>	Optional. Specifies the log file name to which the logger should log messages.
<b>-loginfo</b> <0 or 1>	Optional. Specifies if the logger should log "info" messages. Set to 0 for no, 1 for yes.
<b>-logwarning</b> <0 or 1>	Optional. Specifies if the logger should log "warning" messages. Set to 0 for no, 1 for yes.
<b>-logerror</b> <0 or 1>	Optional. Specifies if the logger should log "error" messages. Set to 0 for no, 1 for yes.
<b>-logtrace</b> <0 or 1>	Optional. Specifies if the logger should log "trace" messages. Set to 0 for no, 1 for yes.
<b>-maxlogfilesize</b> <size>	Optional. Specifies the maximum log file size in KB.

### Example

```
C:\Program Files\Safenet\LunaClient>pedServer -mode connect -name hellohi
>Connecting to Luna SA. Please wait....
>Successfully connected to Luna SA.
```

## pedserver -mode disconnect

Disconnects PEDserver from the appliance.

If the running mode is legacy, an error is returned. **pedserver -mode disconnect** is not a valid command for legacy connections.

Termination of the connection may take a few minutes.

### Syntax

**pedserver -mode disconnect -name** <registered appliance name> [-**configfile** <filename>] [-**logfile** <filename>] [-**loginfo** <0 or 1>] [-**logwarning** <0 or 1>] [-**logerror** <0 or 1>] [-**logtrace** <0 or 1>] [-**maxlogfilesize** <size>]

Option	Description
<b>-name</b> <registered appliance name>	Specifies the name of the registered appliance to be disconnected from PEDserver.
<b>-configfile</b> <filename>	Optional. Specifies which PEDserver configuration file to use.
<b>-logfile</b> <filename>	Optional. Specifies the log file name to which the logger should log messages.
<b>-loginfo</b> <0 or 1>	Optional. Specifies if the logger should log "info" messages. Set to 0 for no, 1 for yes.
<b>-logwarning</b> <0 or 1>	Optional. Specifies if the logger should log "warning" messages. Set to 0 for no, 1 for yes.
<b>-logerror</b> <0 or 1>	Optional. Specifies if the logger should log "error" messages. Set to 0 for no, 1 for yes.
<b>-logtrace</b> <0 or 1>	Optional. Specifies if the logger should log "trace" messages. Set to 0 for no, 1 for yes.
<b>-maxlogfilesize</b> <size>	Optional. Specifies the maximum log file size in KB.

### Example

```
C:\Program Files\Safenet\LunaClient>pedServer -mode disconnect -name hellohi
>Connection to Luna SA terminated.
```



## pedserver -mode show

Queries if PEDserver is currently running, and gets details about PEDserver.

### Syntax

**pedserver -mode show** [-name <registered appliance name>] [-configfile <filename>] [-logfile <filename>] [-loginfo <0 or 1>] [-logwarning <0 or 1>] [-logerror <0 or 1>] [-logtrace <0 or 1>] [-maxlogfilesize <size>]

Option	Description
-name <registered appliance name>	Specifies the name of the registered appliance to be queried. Applies to server-initiated (peer-to-peer) mode only.
-configfile <filename>	Optional. Specifies which PEDserver configuration file to use.
-logfile <filename>	Optional. Specifies the log file name to which the logger should log messages.
-loginfo <0 or 1>	Optional. Specifies if the logger should log "info" messages. Set to 0 for no, 1 for yes.
-logwarning <0 or 1>	Optional. Specifies if the logger should log "warning" messages. Set to 0 for no, 1 for yes.
-logerror <0 or 1>	Optional. Specifies if the logger should log "error" messages. Set to 0 for no, 1 for yes.
-logtrace <0 or 1>	Optional. Specifies if the logger should log "trace" messages. Set to 0 for no, 1 for yes.
-maxlogfilesize <size>	Optional. Specifies the maximum log file size in KB.

### Example

```
C:\Program Files\Safenet\LunaClient>pedServer -mode show -name hellohi
>Ped Server launched in status mode.
 Server Information:
 Hostname: ABC1-123123
 IP: 192.10.10.123
 Firmware Version: 2.5.0-1
 PedII Protocol Version: 1.0.1-0
 Software Version: 1.0.5 (10005)
 Ped2 Connection Status: Connected
 Ped2 RPK Count 1
 Ped2 RPK Serial Numbers (1a123456789a1234)
 Client Information: Not Available
 Operating Information:
 Server Port: 1234
 External Server Interface: Yes
 Admin Port: 1235
```

```
External Admin Interface: No
Server Up Time: 8 (secs)
Server Idle Time: 8 (secs) (100%)
Idle Timeout Value: 1800 (secs)
Current Connection Time: 0 (secs)
Current Connection Idle Time: 0 (secs)
Current Connection Total Idle Time: 0 (secs) (100%)
Total Connection Time: 0 (secs)
Total Connection Idle Time: 0 (secs) (100%)
>Show command passed.
```

## pedserver -mode start

Starts up PEDserver.

### Syntax

```
pedserver -mode start [-name <registered appliance name>] [-ip <server_IP>] [-port <server port>] [-
configfile <filename>] [-admin <admin port number>] [-eserverport <0 or 1>] [-eadmin <0 or 1>] [-
idletimeout <int>] [-socketreadtimeout <int>] [-socketwritetimeout <int>] [-internalshutdowntimeout
<int>] [-bgprocessstartuptimeout <int>] [-bgprocessshutdowntimeout <int>] [-logfile <filename>]
[-loginfo <0 or 1>] [-logwarning <0 or 1>] [-logerror <0 or 1>] [-logtrace <0 or 1>] [-maxlogfilesize <size>]
[-pinginterval <int>] [-pingtimeout <int>] [-force]
```

Option	Description
<b>-admin</b> <admin port number>	Optional. Specifies the administration port number.
<b>-bgprocessshutdowntimeout</b> <int>	Optional. Specifies the shutdown timeout for the detached process, in seconds.
<b>-bgprocessstartuptimeout</b> <int>	Optional. Specifies the startup timeout for the detached process, in seconds.
<b>-configfile</b> <filename>	Optional. Specifies which PED Server configuration file to use.
<b>-eadmin</b> <0 or 1>	Optional. Specifies if the administration is on "localhost" or listening on the external host name.
<b>-eserverport</b> <0 or 1>	Optional. Specifies if the server port is on "localhost" or listening on the external host name.
<b>-force</b>	Optional parameter. Suppresses any prompts.
<b>-idletimeout</b> <int>	Optional. Specifies the idle connection timeout, in seconds.
<b>-internalshutdowntimeout</b> <int>	Optional. Specifies the shutdown timeout for internal services, in seconds.
<b>-ip</b> <server_IP>	Optional. Specifies the server listening IP address. When <b>running pedserver -mode start</b> on an IPv6 network, you must include this option.
<b>-logerror</b> <0 or 1>	Optional. Specifies if the logger should log "error" messages. Set to 0 for no, 1 for yes.
<b>-logfile</b> <filename>	Optional. Specifies the log file name to which the logger should log messages.
<b>-loginfo</b> <0 or 1>	Optional. Specifies if the logger should log "info" messages. Set to 0 for no, 1 for yes.

Option	Description
<b>-logtrace</b> <0 or 1>	Optional. Specifies if the logger should log "trace" messages. Set to 0 for no, 1 for yes.
<b>-logwarning</b> <0 or 1>	Optional. Specifies if the logger should log "warning" messages. Set to 0 for no, 1 for yes.
<b>-maxlogfilesize</b> <size>	Optional. Specifies the maximum log file size in KB.
<b>-name</b> <registered appliance name>	
<b>-pinginterval</b> <int>	Optional. Specifies the time interval between ping commands, in seconds.
<b>-pingtimeout</b> <int>	Optional. Specifies timeout of the ping response, in seconds.
<b>-port</b> <server port>	Optional. Specifies the server port number.
<b>-socketreadtimeout</b> <int>	Optional. Specifies the socket read timeout, in seconds.
<b>-socketwritetimeout</b> <int>	Optional. Specifies socket write timeout, in seconds.

## Example

```
C:\Program Files\Safenet\LunaClient>pedServer -mode start -name hellohi -force
>Ped Server launched in startup mode.
>Starting background process
>Background process started
>Ped Server Process created, exiting this process.
```

## pedserver -mode stop

Stops PEDserver.

### Syntax

```
pedserver -mode stop [-name <registered appliance name>] [-configfile <filename>] [-socketwritetimeout <int>] [-internalshutdowntimeout <int>] [-bgprocessstartuptimeout <int>] [-bgprocessshutdowntimeout <int>] [-logfile <filename>] [-loginfo <0 or 1>] [-logwarning <0 or 1>] [-logerror <0 or 1>] [-logtrace <0 or 1>] [-maxlogfilesize <size>]
```

Option	Description
<b>-name</b> <registered appliance name>	Specifies the name of the registered appliance to be on which PEDserver will be stopped. Applies to server-initiated (peer-to-peer) mode only.
<b>-configfile</b> <filename>	Optional. Specifies which PEDserver configuration file to use.
<b>-socketreadtimeout</b> <int>	Optional. Specifies the socket read timeout, in seconds.
<b>-socketwritetimeout</b> <int>	Optional. Specifies socket write timeout, in seconds.
<b>-internalshutdowntimeout</b> <int>	Optional. Specifies the shutdown timeout for internal services, in seconds.
<b>-bgprocessstartuptimeout</b> <int>	Optional. Specifies the startup timeout for the detached process, in seconds.
<b>-bgprocessshutdowntimeout</b> <int>	Optional. Specifies the shutdown timeout for the detached process, in seconds.
<b>-logfile</b> <filename>	Optional. Specifies the log file name to which the logger should log messages.
<b>-loginfo</b> <0 or 1>	Optional. Specifies if the logger should log "info" messages. Set to 0 for no, 1 for yes.
<b>-logwarning</b> <0 or 1>	Optional. Specifies if the logger should log "warning" messages. Set to 0 for no, 1 for yes.
<b>-logerror</b> <0 or 1>	Optional. Specifies if the logger should log "error" messages. Set to 0 for no, 1 for yes.
<b>-logtrace</b> <0 or 1>	Optional. Specifies if the logger should log "trace" messages. Set to 0 for no, 1 for yes.
<b>-maxlogfilesize</b> <size>	Optional. Specifies the maximum log file size in KB.

## Example

```
C:\Program Files\Safenet\LunaClient>pedServer -mode stop -name hellohi
```

## pedserver -regen

Regenerates the client certificate. This command is available in server-initiated (peer-to-peer) mode only. Existing links (PEDserver, NTLS or STC) will not be affected until they are terminated. Afterward, the user is required to re-register the client certificate to NTLS and PEDserver.

**NOTE** The **pedserver -regen** command should be used only when there is no Luna HSM Client installed. When Luna HSM Client is installed on the host computer, use the LunaCM command **clientconfig deploy** with the **-regen** option or, if necessary, **vtl createCert**.

### Syntax

**pedserver -regen -commonname <commonname> [-force]**

Option	Description
<b>-commonname</b> <commonname>	The client's common name (CN).
<b>-force</b>	Optional parameter. Suppresses any prompts.

### Example

```
C:\Program Files\SafeNet\LunaClient>pedServer -regen -commonname win2016_server -force
Ped Server Version 1.0.6 (10006)
```

```
Private Key created and written to: C:\Program Files\SafeNet\LunaClient\cert\client\win2016_serverKey.pem
```

```
Certificate created and written to: C:\Program Files\SafeNet\LunaClient\cert\client\win2016_server.pem
```

```
Successfully regenerated the client certificate.
```

## pedclient

Use the **pedclient** commands to start, stop, and configure the PEDclient service.

### Syntax

**pedclient -mode**

```
assignid
config
deleteid
releaseid
setid
show
```

**start**  
**stop**  
**testid**

Option	Description
<b>assignid</b>	Assigns a PED ID mapping to an HSM. See <a href="#">"pedclient -mode assignid" on the next page.</a>
<b>config</b>	Modifies or shows existing configuration file settings. See <a href="#">"pedclient -mode config" on page 258.</a>
<b>deleteid</b>	Deletes a PED ID mapping. See <a href="#">"pedclient -mode deleteid" on page 260.</a>
<b>releaseid</b>	Releases a PED ID mapping from an HSM. See <a href="#">"pedclient -mode releaseid" on page 261.</a>
<b>setid</b>	Creates a PED ID mapping. See <a href="#">"pedclient -mode setid" on page 262.</a>
<b>show</b>	Queries if PEDclient is currently running and gets details about PEDclient. See <a href="#">"pedclient -mode show" on page 263.</a>
<b>start</b>	Starts up PEDclient. See <a href="#">"pedclient -mode start" on page 264.</a>
<b>stop</b>	Shuts down PEDclient. See <a href="#">"pedclient -mode stop" on page 266.</a>
<b>testid</b>	Tests a PED ID mapping. See <a href="#">"pedclient -mode testid" on page 267.</a>



## pedclient -mode assignid

Assigns a PED ID mapping to a specified HSM.

### Syntax

**pedclient -mode assignid -id** <pedid> **-id\_serialnumber** <serial> [**-logfile** <filename>] [**-loginfo** <0 or 1>] [**-logwarning** <0 or 1>] [**-logerror** <0 or 1>] [**-logtrace** <0 or 1>] [**-maxlogfilesize** <size>] [**-locallogger**]

Option	Description
<b>-id</b> <pedid>	Specifies the ID of the PED to be assigned.
<b>-id_serialnumber</b> <serial>	Specifies the serial number of the HSM to be linked to the specified PED ID.
<b>-logfile</b> <filename>	Optional. Specifies the log file name to which the logger should log messages.
<b>-loginfo</b> <0 or 1>	Optional. Specifies if the logger should log "info" messages. Set to 0 for no, 1 for yes.
<b>-logwarning</b> <0 or 1>	Optional. Specifies if the logger should log "warning" messages. Set to 0 for no, 1 for yes.
<b>-logerror</b> <0 or 1>	Optional. Specifies if the logger should log "error" messages. Set to 0 for no, 1 for yes.
<b>-logtrace</b> <0 or 1>	Optional. Specifies if the logger should log "trace" messages. Set to 0 for no, 1 for yes.
<b>-maxlogfilesize</b> <size>	Optional. Specifies the maximum log file size in KB.
<b>-locallogger</b>	Optional. Specifies that the Remote PED logger should be used, not the IS logging system.

### Example

```
C:\Program Files\Safenet\LunaClient>pedClient -mode assignid -id 1234 -id_serialnumber 123456789
```

## pedclient -mode config

Modifies or shows existing configuration file settings.

### Syntax

```
pedclient -mode config -show -set [-eadmin <0 or 1>] [-idletimeout <int>] [-ignoreidletimeout] [-socketreadtimeout <int>] [-socketwritetimeout <int>] [-shutdowntimeout <int>] [-pstartuptimeout <int>] [-pshutdowntimeout <int>] [-logfilename <filename>] [-loginfo <0 or 1>] [-logwarning <0 or 1>] [-logtrace <0 or 1>] [-maxlogfilesize <size>] [-locallogger]
```

Option	Description
<b>-show</b>	Displays the contents of the configuration file.
<b>-set</b>	Updates the configuration file to be up to date with other supplied options.
<b>-eadmin &lt;0 or 1&gt;</b>	Optional. Specifies if the administration port is on "localhost" or on the external host name.
<b>-idletimeout &lt;int&gt;</b>	Optional. Specifies the idle connection timeout, in seconds.
<b>-ignoreidletimeout</b>	Optional. Specifies that the idle connection timeout should not apply to the connection established between the PED and HSM during their assignment.
<b>-socketreadtimeout &lt;int&gt;</b>	Optional. Specifies the socket read timeout, in seconds.
<b>-socketwritetimeout &lt;int&gt;</b>	Optional. Specifies the socket write timeout, in seconds.
<b>-shutdowntimeout &lt;int&gt;</b>	Optional. Specifies the shutdown timeout for internal services, in seconds.
<b>-pstartuptimeout &lt;int&gt;</b>	Optional. Specifies the startup timeout for the detached process, in seconds.
<b>-pshutdowntimeout &lt;int&gt;</b>	Optional. Specifies the shutdown timeout for the detached process, in seconds.
<b>-logfilename &lt;filename&gt;</b>	Optional. Specifies the log file name to which the logger should log messages.
<b>-loginfo &lt;0 or 1&gt;</b>	Optional. Specifies if the logger should log "info" messages. Set to 0 for no, 1 for yes.
<b>-logwarning &lt;0 or 1&gt;</b>	Optional. Specifies if the logger should log "warning" messages. Set to 0 for no, 1 for yes.
<b>-logerror &lt;0 or 1&gt;</b>	Optional. Specifies if the logger should log "error" messages. Set to 0 for no, 1 for yes.
<b>-logtrace &lt;0 or 1&gt;</b>	Optional. Specifies if the logger should log "trace" messages. Set to 0 for no, 1 for yes.

Option	Description
<b>-maxlogfilesize</b> <size>	Optional. Specifies the maximum log file size in KB.
<b>-locallogger</b>	Optional. Specifies that the Remote PED logger should be used, not the IS logging system.

## Example

```
C:\Program Files\Safenet\LunaClient>pedClient -mode config -show
```

## pedclient -mode deleteid

Deletes a PED ID mapping between a specified PED and PEDserver.

### Syntax

**pedclient -mode deleteid -id <PED\_ID> [-logfilename <filename>] [-loginfo <0 or 1>] [-logwarning <0 or 1>] [-logerror <0 or 1>] [-logtrace <0 or 1>] [-maxlogfilesize <size>] [-locallogger]**

Option	Description
<b>-id &lt;PED_ID&gt;</b>	Specifies the ID of the PED to be deleted from the map.
<b>-logfilename &lt;filename&gt;</b>	Optional. Specifies the log file name to which the logger should log messages.
<b>-loginfo &lt;0 or 1&gt;</b>	Optional. Specifies if the logger should log "info" messages. Set to 0 for no, 1 for yes.
<b>-logwarning &lt;0 or 1&gt;</b>	Optional. Specifies if the logger should log "warning" messages. Set to 0 for no, 1 for yes.
<b>-logerror &lt;0 or 1&gt;</b>	Optional. Specifies if the logger should log "error" messages. Set to 0 for no, 1 for yes.
<b>-logtrace &lt;0 or 1&gt;</b>	Optional. Specifies if the logger should log "trace" messages. Set to 0 for no, 1 for yes.
<b>-maxlogfilesize &lt;size&gt;</b>	Optional. Specifies the maximum log file size in KB.
<b>-locallogger</b>	Optional. Specifies that the Remote PED logger should be used, not the IS logging system.

### Example

```
C:\Program Files\Safenet\LunaClient>pedClient -mode deleteid -id 1234
```

## pedclient -mode releaseid

Releases a PED ID mapping from the HSM it was assigned to.

### Syntax

**pedclient -mode releaseid -id <PED\_ID> [-logfilename <filename>] [-loginfo <0 or 1>] [-logwarning <0 or 1>] [-logerror <0 or 1>] [-logtrace <0 or 1>] [-maxlogfilesize <size>] [-locallogger]**

Option	Description
<b>-id &lt;PED_ID&gt;</b>	Specifies the ID of the PED to be released.
<b>-logfilename &lt;filename&gt;</b>	Optional. Specifies the log file name to which the logger should log messages.
<b>-loginfo &lt;0 or 1&gt;</b>	Optional. Specifies if the logger should log "info" messages. Set to 0 for no, 1 for yes.
<b>-logwarning &lt;0 or 1&gt;</b>	Optional. Specifies if the logger should log "warning" messages. Set to 0 for no, 1 for yes.
<b>-logerror &lt;0 or 1&gt;</b>	Optional. Specifies if the logger should log "error" messages. Set to 0 for no, 1 for yes.
<b>-logtrace &lt;0 or 1&gt;</b>	Optional. Specifies if the logger should log "trace" messages. Set to 0 for no, 1 for yes.
<b>-maxlogfilesize &lt;size&gt;</b>	Optional. Specifies the maximum log file size in KB.
<b>-locallogger</b>	Optional. Specifies that the Remote PED logger should be used, not the IS logging system.

### Example

```
C:\Program Files\Safenet\LunaClient>pedClient -mode releaseid -id 1234
```

## pedclient -mode setid

Creates a PED ID mapping between a specified PED and PEDserver.

### Syntax

**pedclient -mode setid -id <PED\_ID> -id\_ip <hostname> -id\_port <port> [-logfile <filename>] [-loginfo <0 or 1>] [-logwarning <0 or 1>] [-logerror <0 or 1>] [-logtrace <0 or 1>] [-maxlogfilesize <size>] [-locallogger]**

Option	Description
<b>-id &lt;PED_ID&gt;</b>	Specifies the ID of the PED to be mapped.
<b>-id_ip &lt;hostname&gt;</b>	Specifies the IP address or hostname of the PED Server to be linked with the PED ID.
<b>-id_port &lt;port&gt;</b>	Specifies the PED Server port to be linked with the PED ID.
<b>-logfile &lt;filename&gt;</b>	Optional. Specifies the log file name to which the logger should log messages.
<b>-loginfo &lt;0 or 1&gt;</b>	Optional. Specifies if the logger should log "info" messages. Set to 0 for no, 1 for yes.
<b>-logwarning &lt;0 or 1&gt;</b>	Optional. Specifies if the logger should log "warning" messages. Set to 0 for no, 1 for yes.
<b>-logerror &lt;0 or 1&gt;</b>	Optional. Specifies if the logger should log "error" messages. Set to 0 for no, 1 for yes.
<b>-logtrace &lt;0 or 1&gt;</b>	Optional. Specifies if the logger should log "trace" messages. Set to 0 for no, 1 for yes.
<b>-maxlogfilesize &lt;size&gt;</b>	Optional. Specifies the maximum log file size in KB.
<b>-locallogger</b>	Optional. Specifies that the Remote PED logger should be used, not the IS logging system.

### Example

```
C:\Program Files\Safenet\LunaClient>pedClient -mode setid -id 1234 -id_ip myhostname -id_port 3456
```

## pedclient -mode show

Queries if PEDclient is currently running and gets details about PEDclient.

### Syntax

**pedclient -mode show** [-admin <admin port number>] [-eadmin <0 or 1>] [-socketreadtimeout <int>] [-socketwritetimeout <int>] [-logfile <filename>] [-loginfo <0 or 1>] [-logwarning <0 or 1>] [-logtrace <0 or 1>] [-maxlogfilesize <size>] [-locallogger]

Option	Description
<b>-admin</b> <admin port number>	Optional. Specifies the administration port number to use.
<b>-eadmin</b> <0 or 1>	Optional. Specifies if the administration port is on "localhost" or on the external host name.
<b>-socketreadtimeout</b> <int>	Optional. Specifies the socket read timeout, in seconds.
<b>-socketwritetimeout</b> <int>	Optional. Specifies the socket write timeout, in seconds.
<b>-logfile</b> <filename>	Optional. Specifies the log file name to which the logger should log messages.
<b>-loginfo</b> <0 or 1>	Optional. Specifies if the logger should log "info" messages. Set to 0 for no, 1 for yes.
<b>-logwarning</b> <0 or 1>	Optional. Specifies if the logger should log "warning" messages. Set to 0 for no, 1 for yes.
<b>-logerror</b> <0 or 1>	Optional. Specifies if the logger should log "error" messages. Set to 0 for no, 1 for yes.
<b>-logtrace</b> <0 or 1>	Optional. Specifies if the logger should log "trace" messages. Set to 0 for no, 1 for yes.
<b>-maxlogfilesize</b> <size>	Optional. Specifies the maximum log file size in KB.
<b>-locallogger</b>	Optional. Specifies that the Remote PED logger should be used, not the IS logging system.

### Example

```
C:\Program Files\Safenet\LunaClient>pedClient -mode show
```

## pedclient -mode start

Starts up the PED Client.

### Syntax

```
pedclient -mode start [-winservice] [-eadmin <0 or 1>] [-idletimeout <int>] [-socketreadtimeout <int>] [-socketwritetimeout <int>] [-shutdowntimeout <int>] [-pstartuptimeout <int>][-pshutdowntimeout <int>] [-logfilename <filename>] [-loginfo <0 or 1>] [-logwarning <0 or 1>] [-logtrace <0 or 1>] [-maxlogfilesize <size>] [-locallogger]
```

Option	Description
<b>-winservice</b>	Starts PEDclient for Windows service. The standard parameters used for <b>pedclient mode start</b> can be used for <b>pedclient mode start -winservice</b> as well.
<b>-eadmin</b> <0 or 1>	Optional. Specifies if the administration port is on "localhost" or on the external host name.
<b>-idletimeout</b> <int>	Optional. Specifies the idle connection timeout, in seconds.
<b>-socketreadtimeout</b> <int>	Optional. Specifies the socket read timeout, in seconds.
<b>-socketwritetimeout</b> <int>	Optional. Specifies the socket write timeout, in seconds.
<b>-shutdowntimeout</b> <int>	Optional. Specifies the shutdown timeout for internal services, in seconds.
<b>-pstartuptimeout</b> <int>	Optional. Specifies the startup timeout for the detached process, in seconds.
<b>-pshutdowntimeout</b> <int>	Optional. Specifies the shutdown timeout for the detached process, in seconds.
<b>-logfilename</b> <filename>	Optional. Specifies the log file name to which the logger should log messages.
<b>-loginfo</b> <0 or 1>	Optional. Specifies if the logger should log "info" messages. Set to 0 for no, 1 for yes.
<b>-logwarning</b> <0 or 1>	Optional. Specifies if the logger should log "warning" messages. Set to 0 for no, 1 for yes.
<b>-logerror</b> <0 or 1>	Optional. Specifies if the logger should log "error" messages. Set to 0 for no, 1 for yes.
<b>-logtrace</b> <0 or 1>	Optional. Specifies if the logger should log "trace" messages. Set to 0 for no, 1 for yes.
<b>-maxlogfilesize</b> <size>	Optional. Specifies the maximum log file size in KB.
<b>-locallogger</b>	Optional. Specifies that the Remote PED logger should be used, not the IS logging system.



## Example

```
C:\Program Files\Safenet\LunaClient>pedClient -mode start
```

## pedclient -mode stop

Shuts down PEDclient.

### Syntax

**pedclient -mode stop** [-eadmin <0 or 1>] [-socketreadtimeout <int>] [-socketwritetimeout <int>] [-shutdowntimeout <int>] [-pstartuptimeout <int>] [-pshutdowntimeout <int>] [-logfilename <filename>] [-loginfo <0 or 1>] [-logwarning <0 or 1>] [-logtrace <0 or 1>] [-maxlogfilesize <size>] [-locallogger]

Option	Description
<b>-eadmin</b> <0 or 1>	Optional. Specifies if the administration port is on "localhost" or on the external host name.
<b>-socketreadtimeout</b> <int>	Optional. Specifies the socket read timeout, in seconds.
<b>-socketwritetimeout</b> <int>	Optional. Specifies the socket write timeout, in seconds.
<b>-shutdowntimeout</b> <int>	Optional. Specifies the shutdown timeout for internal services, in seconds.
<b>-pstartuptimeout</b> <int>	Optional. Specifies the startup timeout for the detached process, in seconds.
<b>-pshutdowntimeout</b> <int>	Optional. Specifies the shutdown timeout for the detached process, in seconds.
<b>-logfilename</b> <filename>	Optional. Specifies the log file name to which the logger should log messages.
<b>-loginfo</b> <0 or 1>	Optional. Specifies if the logger should log "info" messages. Set to 0 for no, 1 for yes.
<b>-logwarning</b> <0 or 1>	Optional. Specifies if the logger should log "warning" messages. Set to 0 for no, 1 for yes.
<b>-logerror</b> <0 or 1>	Optional. Specifies if the logger should log "error" messages. Set to 0 for no, 1 for yes.
<b>-logtrace</b> <0 or 1>	Optional. Specifies if the logger should log "trace" messages. Set to 0 for no, 1 for yes.
<b>-maxlogfilesize</b> <size>	Optional. Specifies the maximum log file size in KB.
<b>-locallogger</b>	Optional. Specifies that the Remote PED logger should be used, not the IS logging system.

### Example

```
C:\Program Files\Safenet\LunaClient>pedClient -mode stop
```

## pedclient -mode testid

Tests a PED ID mapping between a specified PED and PEDserver.

### Syntax

**pedclient -mode testid -id <PED\_ID> [-logfilename <filename>] [-loginfo <0 or 1>] [-logwarning <0 or 1>] [-logerror <0 or 1>] [-logtrace <0 or 1>] [-maxlogfilesize <size>] [-locallogger]**

Option	Description
<b>-id &lt;PED_ID&gt;</b>	Specifies the ID of the PED to be tested.
<b>-logfilename &lt;filename&gt;</b>	Optional. Specifies the log file name to which the logger should log messages.
<b>-loginfo &lt;0 or 1&gt;</b>	Optional. Specifies if the logger should log "info" messages. Set to 0 for no, 1 for yes.
<b>-logwarning &lt;0 or 1&gt;</b>	Optional. Specifies if the logger should log "warning" messages. Set to 0 for no, 1 for yes.
<b>-logerror &lt;0 or 1&gt;</b>	Optional. Specifies if the logger should log "error" messages. Set to 0 for no, 1 for yes.
<b>-logtrace &lt;0 or 1&gt;</b>	Optional. Specifies if the logger should log "trace" messages. Set to 0 for no, 1 for yes.
<b>-maxlogfilesize &lt;size&gt;</b>	Optional. Specifies the maximum log file size in KB.
<b>-locallogger</b>	Optional. Specifies that the Remote PED logger should be used, not the IS logging system.

### Example

```
C:\Program Files\Safenet\LunaClient>pedClient -mode testid -id 1234
```

# CHAPTER 8: Initializing an Application Partition

Before it can be used to store cryptographic objects or perform operations, an application partition must be initialized. Initialization is performed by the Partition Security Officer and sets the authentication credential. There are two scenarios where the Partition SO would initialize the partition:

- > **Preparing a new partition:** On a new partition, initialization sets the Partition SO authentication credential, an identifying label for the partition, and the partition's cloning domain (see "[Initializing a New Partition](#)" below).
- > **Erasing an existing partition:** The Partition SO can re-initialize a partition to erase all cryptographic objects and the Crypto Officer/Crypto User roles, and select a new partition label. The Partition SO credential and the cloning domain remain the same (see "[Re-initializing an Existing Partition](#)" on page 270).

## Initializing a New Partition

Initializing an application partition for the first time establishes you as the Partition SO and sets a cloning domain for the partition. This procedure can be performed

- > from an administrative connection to the network HSM appliance (via SSH) using Luna Shell (lunash) commands
  - (beginning with Network appliance software 7.7.1 [and newer] the administrator (HSM SO) can initialize the newly created partition, creating the PSO role
  - and then use the new PSO credential on that partition to initialize the Crypto Officer role), or
- > from a registered client, with an NTLS or STC connection, using LunaCM commands.

The Crypto User role is created from the client side, via lunacm.

Any subsequent *re*-initialization of an application partition is performed from the client.

### Prerequisites

- > The new partition must be created and visible in Luna Shell if it is to be initialized on the Network appliance, in lunash (appliance software 7.7.1 and later - see "[partition init \[ LUNA-16119 \]](#)" on page 1).
- > The new partition must be assigned to the client and visible in LunaCM if it is to be initialized from that client, in lunacm (see "[Client-Partition Connections](#)" on page 86).
- > If you want to configure the partition's policies with a policy template using lunacm, the template file must be available on the client (see "[Setting Partition Policies Using a Template](#)" on page 284).
- > If you want to configure the partition's policies with a policy template using lunash on the appliance, the pre-edited template file must be uploaded to the appliance.
- > PED authentication: A local or remote PED connection must be established (see "[Local PED Setup](#)" on page 190 or "[Remote PED Setup](#)"). Ensure that you have enough blue (Partition SO) and red (Domain) PED keys for your planned authentication scheme (see "[Creating PED Keys](#)" on page 224).

## To initialize a new application partition in LunaSH on the Network HSM appliance

The following steps assume that the Network HSM administrator has created the partition ( "[partition create](#)" on page 1 ).

1. In Lunash, log in to the HSM as SO if you are not already logged in.

```
lunash:> "hsm login" on page 1
```

2. Create the partition, if it has not already been created

```
lunash:> "partition create" on page 1 -partition <partition name>
```

3. Initialize the partition by specifying its partition name. To initialize the partition using a policy template, specify the path to the template file.

Partition names created in LunaSH must be 1-32 characters in length. The following characters are allowed:

```
abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ 0123456789!@#%&^*()-_+{}[]:;./?~
```

Spaces are allowed; enclose the partition name in double quotes if it includes spaces.

The following characters are not allowed: &\|;<>`'?"

No two partitions can have the same name.

- **Password authentication:** You can specify a Partition SO password and/or a domain string with the initialization command, or enter them when prompted.

In LunaSH, the SO or CO password must be 7-255 characters in length. The following characters are allowed:

```
abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789 !@#%&^*()-_+[]{} /: ', . ~
```

The following characters are invalid or problematic and must not be used in the HSM SO password:

```
"&;<>\`|
```

Spaces are allowed; to specify a password with spaces, enclose the password in double quotation marks.

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.

```
lunash:> "partition init [LUNA-16119] " on page 1 -partition <name> [-applytemplate <template_file>] [-password <password>] [-domain <domain_string>]
```

- **PED authentication:**

```
lunash:> "partition init [LUNA-16119] " on page 1-partition <name> [-applytemplate <template_file>]
```

Respond to the Luna PED prompts to create the blue Partition SO key and the red domain key (see "[Creating PED Keys](#)" on page 224).

4. After the partition is initialized and the PSO created, you can create the Crypto Officer role via lunash on the appliance or with lunacm on a registered client see "[The following procedures will allow you to initialize the Crypto Officer \(CO\) and Crypto User \(CU\) roles and set an initial credential.](#)" on page 295

## To initialize a new application partition in LunaCM on the Client

1. Launch LunaCM on the client workstation.

- Set the active slot to the partition you want to initialize.

```
lunacm:> slot set -slot <slot_number>
```

- Initialize the partition by specifying an identifying label. To initialize the partition using a policy template, specify the path to the template file.

The partition label created during initialization must be 1-32 characters in length. If you specify a longer label, it will automatically be truncated to 32 characters. The following characters are allowed:

```
abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789 !@#$%^&* () -_ =+ [] {} \ | / ; : ' , . < > ` ~
```

Question marks (?) and double quotation marks (") are not allowed.

Spaces are allowed; enclose the label in double quotation marks if it includes spaces.

- Password authentication:** You can specify a Partition SO password and/or a domain string with the initialization command, or enter them when prompted.

In LunaCM, passwords and activation challenge secrets must be 7-255 characters in length (**NOTE:** If you are using firmware version 7.0.x, 7.3.3, or 7.4.2, activation challenge secrets must be 7-16 characters in length). The following characters are allowed:

```
abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789 !@#$%^&* () -_ =+ [] {} \ | / ; : ' , . < > ` ~
```

Double quotation marks (") are problematic and should not be used within passwords.

Spaces are allowed; to specify a password with spaces using the **-password** option, enclose the password in double quotation marks.

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.

```
lunacm:> partition init -label <label> [-applytemplate <template_file>] [-password <password>] [-domain <domain_string>]
```

- PED authentication:**

```
lunacm:> partition init -label <label> [-applytemplate <template_file>]
```

Respond to the Luna PED prompts to create the blue Partition SO key and the red domain key (see ["Creating PED Keys" on page 224](#)).

## Re-initializing an Existing Partition

The Partition SO can re-initialize an existing partition at any time. Re-initialization erases all cryptographic objects on the partition, and the login credentials for the Crypto Officer and Limited Crypto Officer and Crypto User roles. The Partition SO login credential and cloning domain are retained.

### Prerequisites

- > The partition must be already initialized.
- > Back up any important cryptographic objects stored on the partition.
- > [PED authentication] A local or remote PED connection must be established (see ["Local PED Setup" on page 190](#) or ["Remote PED Setup" on page 1](#)).

**To re-initialize an existing application partition**

1. Launch LunaCM on the client workstation.
2. Set the active slot to the partition you want to re-initialize.  
lunacm:> **slot set -slot** <slot\_number>
3. Initialize the partition by specifying an identifying label. You must specify a label for the partition (the same label or a new one). You are prompted for the current Partition SO credential.  
lunacm:> **partition init -label** <label>

# CHAPTER 9: Partition Capabilities and Policies

An application partition can be configured to provide a range of different functions. The Partition Security Officer can customize this functionality using partition policies. This configuration is governed by the following settings:

- > **Partition Capabilities** are features of partition functionality that are inherited from the parent HSM policies (see [HSM Capabilities and Policies](#)). The HSM SO can configure HSM policies to allow or disallow partition capabilities. Some capabilities have corresponding modifiable partition policies.
- > **Partition Policies** are configurable settings that allow the Partition Security Officer to modify the function of their corresponding capabilities.

The table below describes all partition capabilities, their corresponding policies, and the results of changing their settings. This section contains the following procedures:

- > ["Setting Partition Policies Manually" on page 283](#)
- > ["Setting Partition Policies Using a Template" on page 284](#)

## Destructive Policies

As a security measure, changing some partition policies forces deletion of all cryptographic objects on the partition. These policies are listed as **destructive** in the table below. Some policy changes are destructive in either direction (**OFF-to-ON** and **ON-to-OFF**), while others are destructive only in the direction resulting in lowered partition security.

Use `lunacm:> partition showpolicies -verbose` to check whether the policy you want to enable/disable is destructive.



#	Partition Capability	Partition Policy
0	<p><b>Enable private key cloning</b></p> <p>Always <b>1</b>. This capability allows private keys to be cloned to another Luna HSM partition (required for backup and HA).</p> <div data-bbox="276 415 759 674" style="border: 1px solid #ccc; padding: 5px;"> <p><b>NOTE</b> The HSM SO can disable cloning for all partitions on the HSM by turning off HSM policy 7 (see <a href="#">HSM Capabilities and Policies</a>). In this case, cloning is not possible on the partition, regardless of this capability/policy's setting.</p> </div>	<p><b>Allow private key cloning (destructive OFF-to-ON)</b></p> <ul style="list-style-type: none"> <li>&gt; <b>1</b> (default): The partition is capable of cloning private keys to another partition. This policy must be enabled to back up partitions or create HA groups. Public keys and objects can always be cloned, regardless of this policy's setting.</li> <li>&gt; <b>0</b>: Private keys can never be cloned to another application partition.</li> </ul> <p>Partition policies <b>0</b> and <b>1</b> may not be set to <b>1</b> (ON) at the same time.</p> <div data-bbox="919 667 1393 995" style="border: 1px solid #ccc; padding: 5px;"> <p><b>NOTE</b> Key attributes can be set modifiable, and a key can then be set with (for example) attribute - extractable (see "<a href="#">cmu generatekeypair</a>" on page 1 ), but Partition Policies overrule object attributes; Cloning ON and Private Key Wrapping OFF would prevent export despite the attribute settings.</p> </div>
1	<p><b>Enable private key wrapping</b></p> <p>Always <b>1</b>. This capability allows private keys to be encrypted (wrapped) and exported off the partition.</p>	<p><b>Allow private key wrapping (destructive OFF-to-ON)</b></p> <ul style="list-style-type: none"> <li>&gt; <b>1</b>: Private keys may be wrapped and saved to an encrypted file off the partition. Public keys and objects can always be wrapped and exported, regardless of this policy's setting.</li> <li>&gt; <b>0</b> (default): Private keys can never be wrapped and exported off the partition.</li> </ul> <p>Partition policies <b>0</b> and <b>1</b> may not be set to <b>1</b> (ON) at the same time.</p> <div data-bbox="919 1434 1393 1761" style="border: 1px solid #ccc; padding: 5px;"> <p><b>NOTE</b> Key attributes can be set modifiable, and a key can then be set with (for example) attribute - extractable (see "<a href="#">cmu generatekeypair</a>" on page 1 ), but Partition Policies overrule object attributes; Cloning ON and Private Key Wrapping OFF would prevent export despite the attribute settings.</p> </div>

#	Partition Capability	Partition Policy
2	<p><b>Enable private key unwrapping</b></p> <p>Always <b>1</b>. This capability allows wrapped private keys to be imported to the partition.</p>	<p><b>Allow private key unwrapping</b></p> <ul style="list-style-type: none"> <li>&gt; <b>1</b> (default): Private keys can be unwrapped and stored on the partition.</li> <li>&gt; <b>0</b>: Private keys cannot be unwrapped onto the partition.</li> </ul>
3	<p><b>Enable private key masking</b></p> <p>Private keys can be masked off the partition.</p>	<p><b>Allow private key masking</b></p> <ul style="list-style-type: none"> <li>&gt; <b>1</b> (default for V1 partitions): Private keys can be masked off the partition.</li> <li>&gt; <b>0</b> (default for V0 partitions): Private keys cannot be masked off the partition.</li> </ul>
4	<p><b>Enable secret key cloning</b></p> <p>Always <b>1</b>. This capability allows secret keys to be cloned to another Luna HSM partition (required for backup and HA).</p> <div style="border: 1px solid black; padding: 5px; margin-top: 10px;"> <p><b>NOTE</b> The HSM SO can disable cloning for all partitions on the HSM by turning off HSM policy 7 (see <a href="#">HSM Capabilities and Policies</a>). In this case, cloning is not possible on the partition, regardless of this capability/policy's setting.</p> </div>	<p><b>Allow secret key cloning (destructive OFF-to-ON)</b></p> <ul style="list-style-type: none"> <li>&gt; <b>1</b> (default): Secret keys on the partition can be cloned to another partition. This is required for partition backup and HA groups.</li> <li>&gt; <b>0</b>: Secret keys cannot be backed up, and will not be cloned to other HA group members.</li> </ul>
5	<p><b>Enable secret key wrapping</b></p> <p>Always <b>1</b>. This capability allows secret keys to be encrypted (wrapped) and exported off the partition.</p>	<p><b>Allow secret key wrapping (destructive OFF-to-ON)</b></p> <ul style="list-style-type: none"> <li>&gt; <b>1</b> (default): Secret keys can be wrapped and saved to an encrypted file off the partition.</li> <li>&gt; <b>0</b>: Secret keys can never be wrapped and exported off the partition.</li> </ul>
6	<p><b>Enable secret key unwrapping</b></p> <p>Always <b>1</b>. This capability allows wrapped secret keys to be imported to the partition.</p>	<p><b>Allow secret key unwrapping</b></p> <ul style="list-style-type: none"> <li>&gt; <b>1</b> (default): Secret keys can be unwrapped and stored on the partition.</li> <li>&gt; <b>0</b>: Secret keys cannot be unwrapped onto the partition.</li> </ul>
7	<p><b>Enable secret key masking</b></p> <p>Enable masking secret keys off the partition.</p>	<p><b>Allow secret key masking</b></p> <ul style="list-style-type: none"> <li>&gt; <b>1</b> (default for V1 partitions): Secret keys can be masked and stored off the partition.</li> <li>&gt; <b>0</b> (default for V0 partitions): Secret keys cannot be masked off the partition.</li> </ul>

#	Partition Capability	Partition Policy
10	<p><b>Enable multipurpose keys</b></p> <p>Always <b>1</b>. This capability allows keys that are created or unwrapped on the partition to have more than one of the following attributes enabled (set to <b>1</b>), and can therefore be used for multiple types of operation:</p> <ul style="list-style-type: none"> <li>• Encrypt/Decrypt</li> <li>• Sign/Verify</li> <li>• Wrap/Unwrap</li> <li>• Derive</li> </ul>	<p><b>Allow multipurpose keys (destructive OFF-to-ON)</b></p> <ul style="list-style-type: none"> <li>&gt; <b>1</b> (default): Keys that are created or unwrapped on the partition may be used for multiple operations.</li> <li>&gt; <b>0</b>: Keys that are created or unwrapped on the partition may have only one of the affected attributes enabled. Thales recommends that you create keys with only the attributes required for their intended purpose. Disabling this policy enforces this rule on the partition.</li> </ul> <div style="border: 1px solid black; padding: 5px; margin-top: 10px;"> <p><b>NOTE</b> This policy does not affect Diffie-Hellman keys, which are always created with only Derive set to <b>1</b>.</p> </div>
11	<p><b>Enable changing key attributes</b></p> <p>Always <b>1</b>. This capability allows the Crypto Officer to modify the following non-sensitive attributes of keys on the partition, changing key functions:</p> <ul style="list-style-type: none"> <li>&gt; CKA_ENCRYPT</li> <li>&gt; CKA_DECRYPT</li> <li>&gt; CKA_WRAP</li> <li>&gt; CKA_UNWRAP</li> <li>&gt; CKA_SIGN</li> <li>&gt; CKA_SIGN_RECOVER</li> <li>&gt; CKA_VERIFY</li> <li>&gt; CKA_VERIFY_RECOVER</li> <li>&gt; CKA_DERIVE</li> <li>&gt; CKA_EXTRACTABLE</li> </ul>	<p><b>Allow changing key attributes (destructive OFF-to-ON)</b></p> <ul style="list-style-type: none"> <li>&gt; <b>1</b> (default): The Crypto Officer can modify the non-sensitive attributes of keys on the partition.</li> <li>&gt; <b>0</b>: Keys created on the partition cannot be modified.</li> </ul>

#	Partition Capability	Partition Policy
15	<p><b>Allow failed challenge responses</b></p> <p>Always <b>1</b>. This capability/policy applies to PED-authenticated Luna Network HSM only. It determines whether failed login attempts using a challenge secret count towards a partition lockout.</p>	<p><b>Ignore failed challenge responses (destructive OFF-to-ON)</b></p> <ul style="list-style-type: none"> <li>&gt; <b>1</b> (default): Failed challenge secret login attempts are not counted towards a partition lockout. Only failed PED key authentication attempts increment the counter.</li> <li>&gt; <b>0</b>: Failed login attempts using either a PED key or a challenge secret will count towards a partition lockout.</li> </ul> <p>See <a href="#">"Activation and Auto-activation on Multi-factor-(PED-) Authenticated Partitions"</a> on page 299 and <a href="#">"Before you can perform administrative tasks on the partition or its stored cryptographic objects, you must log in with the appropriate role:"</a> on page 294 for more information.</p>
16	<p><b>Enable operation without RSA blinding</b></p> <p>Always <b>1</b>. RSA blinding is a technique that introduces random elements into the signature process to prevent timing attacks on the RSA private key. Some security policies may require this technique, but it does affect performance.</p>	<p><b>Operate without RSA blinding (destructive OFF-to-ON)</b></p> <ul style="list-style-type: none"> <li>&gt; <b>1</b> (default): The partition does not use RSA blinding.</li> <li>&gt; <b>0</b>: The partition uses RSA blinding. Performance will be affected.</li> </ul>
17	<p><b>Enable signing with non-local keys</b></p> <p>Always <b>1</b>. Keys generated on the HSM have the attribute CKA_LOCAL=1. Keys that are imported (unwrapped) to the HSM have CKA_LOCAL=0. These attributes are maintained if keys are backed up or cloned to another HSM partition.</p>	<p><b>Allow signing with non-local keys</b></p> <ul style="list-style-type: none"> <li>&gt; <b>1</b> (default): Only keys with attribute CKA_LOCAL=1 can be used to sign data on the partition.</li> <li>&gt; <b>0</b>: Keys with attribute CKA_LOCAL=0 can be used for signing, and their trust history is not assured.</li> </ul>
18	<p><b>Enable raw RSA operations</b></p> <p>Always <b>1</b>. This capability enables the RSA mechanism <a href="#">CKM_RSA_X_509</a> on the partition, which allows weak signatures and weak encryption.</p>	<p><b>Allow raw RSA operations (destructive OFF-to-ON)</b></p> <ul style="list-style-type: none"> <li>&gt; <b>1</b> (default): The partition allows operations using the RSA mechanism <a href="#">CKM_RSA_X_509</a>.</li> <li>&gt; <b>0</b>: Operations using <a href="#">CKM_RSA_X_509</a> are blocked on the partition.</li> </ul>
20	<p><b>Max failed user logins allowed</b></p> <p>Displays the maximum number of failed partition login attempts (<b>10</b>) before the partition is locked out (see <a href="#">"Before you can perform administrative tasks on the partition or its stored cryptographic objects, you must log in with the appropriate role:"</a> on page 294).</p>	<p><b>Max failed user logins allowed</b></p> <p>The Partition SO can lower the effective number of failed logins below the maximum if desired. Default: <b>10</b></p>

#	Partition Capability	Partition Policy
21	<p><b>Enable high availability recovery</b></p> <p>Always <b>1</b>. This capability enables the RecoveryLogin feature on the partition. This feature allows other HA group members to restore the login state of the partition in the event of a power outage or other such deactivation.</p>	<p><b>Allow high availability recovery</b></p> <ul style="list-style-type: none"> <li>&gt; <b>1</b> (default): RecoveryLogin is enabled on the partition. This feature must be configured in advance (see <a href="#">role recoveryinit</a> and <a href="#">role recoverylogin</a>).</li> <li>&gt; <b>0</b>: RecoveryLogin is disabled on the partition.</li> </ul>
22	<p><b>Enable activation</b></p> <p>This capability allows the partition to be activated. See "<a href="#">Activation and Auto-activation on Multi-factor- (PED-) Authenticated Partitions</a>" on page 299.</p> <ul style="list-style-type: none"> <li>&gt; <b>1</b>: Always enabled on PED-authenticated HSMs.</li> <li>&gt; <b>0</b>: Always disabled on password-authenticated HSMs.</li> </ul>	<p><b>Allow activation</b></p> <ul style="list-style-type: none"> <li>&gt; <b>1</b>: The black and/or gray PED key secrets can be encrypted and cached, so that only a keyboard-entered challenge secret is required to log in.</li> <li>&gt; <b>0</b> (default): PED keys must be presented at each login, whether via LunaCM or a client application.</li> </ul> <p>This policy is overridden and activation is disabled if a tamper event occurs, or if an uncleared tamper event is detected on reboot. See <a href="#">Tamper Events</a> for more information.</p>
23	<p><b>Enable auto-activation</b></p> <p>This capability allows the partition to remain activated for up to two hours if the Luna Network HSM loses power. See "<a href="#">Activation and Auto-activation on Multi-factor- (PED-) Authenticated Partitions</a>" on page 299.</p> <ul style="list-style-type: none"> <li>&gt; <b>1</b>: Always enabled on PED-authenticated HSMs.</li> <li>&gt; <b>0</b>: Always disabled on password-authenticated HSMs.</li> </ul>	<p><b>Allow auto-activation</b></p> <ul style="list-style-type: none"> <li>&gt; <b>1</b>: Partition activation (see policy 22 above) is maintained after an HSM power loss of up to two hours.</li> <li>&gt; <b>0</b> (default): The partition is deactivated in the event of a power loss. When power is restored, the black and/or gray PED keys must be presented to re-activate the partition.</li> </ul>
25	<p><b>Minimum PIN length</b></p> <p>Always <b>248 (7 characters)</b>.</p> <p>The absolute minimum length for a role password/challenge secret is 7 characters. This is displayed as a value subtracted from 255.</p> <p>The reason for this inversion is that a policy can only be set to a value equal to or lower than the value set by its capability. If the absolute minimum length was set to 7, the Partition SO would be able to set the preferred minimum to 2, a less-secure policy. The Partition SO may only change the minimum length to increase security by forcing stronger passwords.</p>	<p><b>Minimum PIN length</b></p> <p>The Partition SO can choose to increase the effective minimum length of a role password/challenge secret by setting this policy. The policy value is determined as follows:</p> <p>Subtract the desired minimum length from 255 (the absolute maximum length), and set policy 25 to that value.</p> <p><b>255 - (desired length) = (policy value)</b></p> <p>For example, to set the minimum length to 10 characters, set the value of this policy to 245:</p> <p><b>255 - 10 = 245</b></p> <p>Default: <b>248 (7 characters)</b></p>

#	Partition Capability	Partition Policy
26	<p><b>Maximum PIN length</b></p> <p>Always <b>255</b>. The absolute maximum length for a role password/challenge secret is 255 characters.</p>	<p><b>Maximum PIN length</b></p> <p>The effective maximum role password/challenge secret length may be changed by the Partition SO. It must always be greater than or equal to the effective minimum length, determined by the formula described in policy 25 (above).</p> <p>Default: <b>255</b></p>
28	<p><b>Enable Key Management Functions</b></p> <p>Always <b>1</b>. This capability allows cryptographic objects to be created or deleted on the partition.</p>	<p><b>Allow Key Management Functions (destructive OFF-to-ON)</b></p> <ul style="list-style-type: none"> <li>&gt; <b>1</b> (default): The Crypto Officer can manage (create/delete) objects on the partition. The Crypto User is restricted to read-only operations.</li> <li>&gt; <b>0</b>: Partition objects are read-only for both the CO and CU roles.</li> </ul>
29	<p><b>Enable RSA signing without confirmation</b></p> <p>Always <b>1</b>. This capability governs the HSM's internal signing verification.</p>	<p><b>Perform RSA signing without confirmation (destructive OFF-to-ON)</b></p> <ul style="list-style-type: none"> <li>&gt; <b>1</b> (default): No internal signing verification is performed.</li> <li>&gt; <b>0</b>: The HSM performs an internal verification of signing operations to validate the signature. This has a performance impact on signature operations.</li> </ul>
31	<p><b>Enable private key unmasking</b></p> <p>Always <b>1</b>. Private keys can be unmasked onto the partition.</p>	<p><b>Allow private key unmasking</b></p> <ul style="list-style-type: none"> <li>&gt; <b>1</b> (default for V1 partitions): Private keys can be unmasked onto the partition (meaning they also can be migrated from legacy Luna HSMs that used SIM).</li> <li>&gt; <b>0</b> (default for V0 partitions): Private keys cannot be unmasked onto the partition (meaning that migration of private keys from legacy HSMs using SIM is also not possible).</li> </ul>
32	<p><b>Enable secret key unmasking</b></p> <p>Enable unmasking of a secret key onto the partition.</p>	<p><b>Allow secret key unmasking</b></p> <ul style="list-style-type: none"> <li>&gt; <b>1</b> (default for V1 partitions): Secret keys can be masked and stored onto the partition.</li> <li>&gt; <b>0</b> (default for V0 partitions): Secret keys cannot be masked onto the partition.</li> </ul>

#	Partition Capability	Partition Policy
33	<p><b>Enable RSA PKCS mechanism</b></p> <p>Always <b>1</b>. The mechanism <a href="#">CKM_RSA_PKCS</a> has known weaknesses, which you can address in your applications. If you are not prepared to address these issues, you can choose to disable the mechanism entirely.</p>	<p><b>Allow RSA PKCS mechanism (destructive OFF-to-ON)</b></p> <ul style="list-style-type: none"> <li>&gt; <b>1</b> (default): <a href="#">CKM_RSA_PKCS</a> is enabled on the partition.</li> <li>&gt; <b>0</b>: <a href="#">CKM_RSA_PKCS</a> is disabled on the partition.</li> </ul>
34	<p><b>Enable CBC-PAD (un)wrap keys of any size</b></p> <p>Always <b>1</b>. There are known vulnerabilities using small keys wrapped/unwrapped with CBC_PAD mechanisms (and with small keys in general). You can choose to enforce a size restriction so that small weak keys cannot be unwrapped onto the partition. The following mechanisms are affected:</p> <ul style="list-style-type: none"> <li>&gt; <a href="#">CKM_AES_CBC_PAD</a></li> <li>&gt; <a href="#">CKM_AES_CBC_PAD_IPSEC</a></li> <li>&gt; <a href="#">CKM_ARIA_CBC_PAD</a></li> <li>&gt; <a href="#">CKM_ARIA_L_CBC_PAD</a></li> <li>&gt; <a href="#">CKM_CAST3_CBC_PAD</a></li> <li>&gt; <a href="#">CKM_CAST5_CBC_PAD</a></li> <li>&gt; <a href="#">CKM_DES_CBC_PAD</a></li> <li>&gt; <a href="#">CKM_DES3_CBC_PAD</a></li> <li>&gt; <a href="#">CKM_DES3_CBC_PAD_IPSEC</a></li> <li>&gt; <a href="#">CKM_RC2_CBC_PAD</a></li> <li>&gt; <a href="#">CKM_RC5_CBC_PAD</a></li> <li>&gt; <a href="#">CKM_SEED_CBC_PAD</a></li> <li>&gt; <a href="#">CKM_SM4_CBC_PAD</a></li> </ul>	<p><b>Allow CBC-PAD (un)wrap keys of any size</b></p> <ul style="list-style-type: none"> <li>&gt; <b>1</b> (default): All keys can be wrapped or unwrapped using CBC_PAD mechanisms.</li> <li>&gt; <b>0</b>: Small keys cannot be wrapped or unwrapped using CBC_PAD mechanisms.</li> </ul>
37	<p><b>Enable Secure Trusted Channel</b></p> <p>Always <b>1</b>. This capability allows the partition to use STC for client access.</p> <div style="border: 1px solid black; padding: 5px; margin-top: 10px;"> <p><b>NOTE</b> The HSM SO must first enable STC by turning on HSM policy 39.</p> </div>	<p><b>Force Secure Trusted Channel (destructive ON-to-OFF)</b></p> <ul style="list-style-type: none"> <li>&gt; <b>1</b>: If this policy is set, STC is used for all client access to this partition. You must first set up and register the STC identities (see "<a href="#">Creating an STC Connection</a>" on page 104).</li> <li>&gt; <b>0</b> (default): NTLS is used by default for client access to this partition , but STC can be used if desired.</li> </ul>

#	Partition Capability	Partition Policy
39	<p><b>Enable Start/End Date Attributes</b></p> <p>Always <b>1</b>. This capability allows you to enforce the CKA_START_DATE and CKA_END_DATE attributes of partition objects.</p>	<p><b>Allow Start/End Date Attributes (destructive ON-to-OFF)</b></p> <ul style="list-style-type: none"> <li>&gt; <b>1</b>: CKA_START_DATE and CKA_END_DATE attributes are enforced for all partition objects.</li> <li>&gt; <b>0</b> (default): These attributes can be set for partition objects, but their values are ignored.</li> </ul>
40	<p><b>Enable Per-Key Authorization Data</b></p> <p>Both assigned and unassigned secret keys ( symmetric or private) are given per-key authorization attributes in the form of CKA_AUTH_DATA, in any newly created or upgraded firmware 7.7.0 (or newer) partition. For V0 partitions PKA is ignored and applications can use the pre-existing APIs as before. For V1 partitions it is actively used, for eIDAS compliance with newer API.</p>	<p><b>Require Per-Key Authorization Data</b></p> <ul style="list-style-type: none"> <li>&gt; <b>1</b> (default for V1 partitions): Per-Key-Authorization is on by default, but can be turned off for performance.</li> <li>&gt; <b>0</b> (default for V0 partitions): Per-Key-Authorization is off by default, and cannot be turned on - V0 partitions do not allow policy changes that would require new clients.</li> </ul>
41	<p><b>Enable Partition Version</b></p> <p>Always <b>1</b>. This capability is visible for any partition at firmware version 7.7.0 or newer, and allows you to switch a partition between version V0 and V1.</p>	<p><b>Partition Version (destructive ON-to-OFF)</b></p> <ul style="list-style-type: none"> <li>&gt; <b>1</b> : Version 1 (V1) partition supports all features of firmware 7.7.0 (or newer). <ul style="list-style-type: none"> <li>• cloning is used/permitted only for SMKs</li> <li>• key objects are transferred using SKS</li> <li>• only HA Login version 2 is supported.</li> </ul> </li> <li>&gt; <b>0</b> (default): Version 0 (V0) supports older API and your pre-existing applications (used with f/w &lt; 7.7), enhanced by fixes and security updates of firmware 7.7.0 (or newer), but Per Key Authorization, SKS, and other V1-dependent features are not available. Pre-7.7.0 version of HA Login can be used (full use of v1.1 or version 2.0 , while v1.0 HA Login for use as primary only)</li> </ul>



#	Partition Capability	Partition Policy
42	<p><b>Enable CPv1</b></p> <p>This capability is visible for any partition at firmware version 7.7.1 or newer, and allows the partition to use the cloning protocol needed for HA with older partitions.</p>	<p><b>Allow CPv1 (destructive OFF-to-ON)</b></p> <p>For V0 partitions created while the HSM is at firmware version 7.7.1 or newer</p> <p>When the HSM is in non-FIPS mode (where HSM policy 12 is set to ON)</p> <ul style="list-style-type: none"> <li>&gt; <b>1</b> (default): Cloning (CPv1) can be used by the partition for key objects.</li> <li>&gt; <b>0</b> (default): Cloning (CPv1) is not allowed by the partition for key objects. When the HSM is in FIPS mode (where HSM policy 12 is set to OFF), this policy setting cannot be changed. Cloning (CPv1) is not allowed, by the partition, for key objects.</li> </ul> <p>For firmware 7.7.0 V0 partitions, "Allow CPv1" is OFF after firmware update from version 7.7.0 to version 7.7.1 or newer.</p> <p>For firmware 7.7.0 V1 partitions, "Allow CPv1" is always OFF.</p> <p>For pre-7.7.0 firmware partitions, CPv1 is turned ON after update, if the HSM is not in FIPS mode, OFF if the HSM is in FIPS mode.</p> <p>The Luna Backup HSM (G7) with firmware 7.7.1 cannot restore keys to a partition with CPv1 enabled if they were backed up from a partition with CPv1 disabled. This limitation is restricted to the Backup HSM. You can still use direct slot-to-slot cloning (see <a href="#">"Cloning Objects to Another Application Partition" on page 170</a>).</p>

#	Partition Capability	Partition Policy
43	<p><b>Enable non-FIPS algorithms</b></p> <p>This capability is visible for any partition at firmware version 7.7.1 or newer, and allows the use of algorithms that are FIPS non-compliant, within the current partition. Requires that HSM policy 12 be set to ON (i.e., HSM is in non-FIPS mode).</p>	<p><b>Allow non-FIPS algorithms (destructive OFF-to-ON)</b></p> <p>For V0 partitions created while the HSM is at firmware version 7.7.1 or newer</p> <p>When the HSM is in non-FIPS mode (where HSM policy 12 is set to ON)</p> <ul style="list-style-type: none"> <li>&gt; <b>1</b> (default): Non-FIPS-compliant algorithms can be used by the partition.</li> <li>&gt; <b>0</b> (default): Non-FIPS-compliant algorithms are not permitted.</li> </ul> <p>When the HSM is in FIPS mode (where HSM policy 12 is set to OFF), this policy setting cannot be changed; non-FIPS-compliant algorithms are not permitted on any partition on the HSM.</p> <p>For firmware 7.7.0 V0 partitions, "Allow CPv1" is OFF after firmware update from version 7.7.0 to version 7.7.1 or newer.</p> <p>For firmware 7.7.0 V1 partitions, "Allow non-FIPS" follows the HSM policy (on if on, off if off).</p> <p>For pre-7.7.0 firmware partitions, this partition policy follows the HSM policy.</p>

A number of partition capabilities are linked to the corresponding HSM capabilities and policies including:

- > Partition Policy (0) Enable private key cloning is dependent on HSM Policy (7) Allow cloning;
- > Partition Policy (3) Enable private key masking is dependent on HSM Policy (6) Allow Masking;
- > Partition Policy (4) Enable secret key cloning is dependent on HSM Policy (7) Allow cloning;
- > Partition Policy (7) Enable secret key masking is dependent on HSM Policy (6) Allow Masking;
- > Partition Policy (22) Enable Activation and Partition Policy (23) Enable Auto-Activation are dependent on HSM Policy (1) Allow PED-based authentication;
- > Partition Policy (31) Enable private key unmasking is dependent on HSM Policy (6) Allow Masking; and
- > Partition Policy (32) Enable secret key unmasking is dependent on HSM Policy (6) Allow Masking.

In addition – the following dependencies within the partition level policies are observed:

- > Partition Policy (7) Allow cloning cannot be enabled at the same time as Partition Policy (1) Allow private key wrapping;
- > Partition Policy (1) Allow private key wrapping cannot be enabled at the same time as either one of the policies, Partition Policy (0) Enable private key cloning, Partition Policy (3) Allow private key masking, Partition Policy (31) Enable private key unmasking;
- > Partition Policy (23) Allow Activation is dependent on Partition Policy (22) Allow Activation being enabled;
- > Partition Policies related to 'Masking' (3, 7, 31 and 32) can only be enabled when Partition Policy (41) Partition Version is '0'; and

- > Partition Policy (41) Partition Version cannot be set to '1' at the same time as either Partition Policy (40) Enable Per-Key Authorisation Data or any of the Partition Policies covering key masking (3, 7, 31 and 32).
- > Partition Policy (40) Enable Per-Key Authorisation Data is enabled by default but is disabled if Partition Policy (41) Partition Version is set to '0'.

**NOTE** With the HSM in FIPS mode, then at partition level

- you are never allowed cloning (CPV1) and
- you can never to turn FIPS mode off per partition.

This is to prevent keys/objects in a more secure container from being transferred to a less-secure container.

## Setting Partition Policies Manually

The Partition Security Officer can change available policies to customize partition functionality. Policy settings apply to all roles/objects on the partition. Refer to ["Partition Capabilities and Policies" on page 272](#) for a complete list of partition policies and their effects.

In most cases, partition policies are either enabled (**1**) or disabled (**0**), but some allow a range of values.

To change multiple policy settings during partition initialization, see ["Setting Partition Policies Using a Template" on the next page](#).

See also ["Configuring the Partition for Cloning or Export of Private/Secret Keys" on page 287](#).

### Prerequisites

- > The partition must be initialized (see ["Initializing an Application Partition" on page 268](#)).
- > If you are changing a destructive policy, back up any important cryptographic objects (see ["Backup and Restore Using a Luna Backup HSM \(G5\)" on page 379](#) or ["Backup and Restore Using a Luna Backup HSM \(G7\)" on page 408](#)).

**NOTE** If you are running more than one LunaCM session against the same partition, and change a partition policy in one LunaCM session, the new policy setting is visible in that session only (although it is in effect). You must exit and restart the other LunaCM sessions to display the new policy setting.

### To manually set or change a partition policy

1. Launch LunaCM and set the active slot to the partition.

```
lunacm:> slot set -slot <slotnum>
```

2. [Optional] Display the existing partition policy settings.

```
lunacm:> partition showpolicies
```

3. Log in as Partition SO (see ["Before you can perform administrative tasks on the partition or its stored cryptographic objects, you must log in with the appropriate role:" on page 294](#)).

```
lunacm:> role login -name po
```

- 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). You can specify multiple policy changes in the same command by using comma-separated lists (for example, **-policy 33,37,40 -value 0,1,1**).

```
lunacm:> partition changepolicy -policy <policy_ID> -value <value>
```

If you are changing a destructive policy, you are prompted to enter **proceed** to continue the operation.

## Setting Partition Policies Using a Template

A partition policy template is a file containing a set of preferred partition policy settings, used to initialize partitions with those settings. You can use the same file to initialize multiple partitions, rather than changing policies manually after initialization. This can save time and effort when initializing partitions that are to function as 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 HSM Policies Using a Policy Template](#).

**NOTE** This feature requires minimum firmware version 7.1.0 and client 7.1. See [Version Dependencies by Feature](#) for more information.

You can create a partition policy template file from an initialized or uninitialized partition, and edit it using a standard text editor. Partition policy templates have additional customization options.

Policy templates cannot be used to alter settings for an initialized partition. Once a partition has been initialized, the Partition SO must change individual policies manually (see "[Setting Partition Policies Manually](#)" on the [previous page](#)).

This section provides instructions for the following procedures, and some general guidelines and restrictions:

- > "[Creating a Partition Policy Template](#)" below
- > "[Editing a Partition Policy Template](#)" on the next page
- > "[Applying a Partition Policy Template](#)" on page 286

### Creating a Partition Policy Template

The following procedure describes how to create a policy template for a partition. This can be done optionally at two points in the partition setup process:

- > before the partition is initialized: this produces a template file containing the default policy settings, which can then be edited
- > after initializing and setting the partition policies manually: this produces a template file with the current policy settings, which can then be used to initialize other partitions with the same settings. The Partition SO must complete the procedure.

#### To create a partition policy template

- Launch LunaCM and set the active slot to the partition. If you are creating a template from an initialized partition, you must log in as Partition SO.

```
lunacm:> slot set -slot <slotnum>
```

```
lunacm:> role login -name po
```

2. Create the partition policy template file. Specify an existing save directory and original filename. No file extension is required. If a template file with the same name exists in the specified directory, it is overwritten.

```
lunacm:> partition showpolicies -exporttemplate <filepath/filename>
```

```
lunacm:> partition showpolicies -exporttemplate /usr/safenet/lunaclient/templates/ParPT
```

```
Partition policies for Partition: myPartition1 written to
/usr/safenet/lunaclient/templates/ParPT
```

```
Command Result : No Error
```

## Editing a Partition Policy Template

Use a standard text editor to manually edit policy templates for custom configurations. This section provides template examples and customization guidelines.

### Partition Policy Template Example

This example shows the contents of a partition policy template created using the factory default policy settings. Use a standard text editor to change the policy and/or destructiveness values (0=OFF, 1=ON, or the desired value 0-255).

Partition policy template entries have two additional fields: **Off to on destructive** and **On to off destructive** (see example below). Change these values to **0** or **1** to determine whether cryptographic objects on the partition should be deleted when this policy is changed in the future. Policies that lower the security level of the objects stored on the partition are normally destructive, but it may be useful to customize this behavior for your own security strategy. See "[Partition Capabilities and Policies](#)" on page 272 for more information.

**CAUTION!** Setting policy destructiveness to **0** (OFF) makes partitions less secure. Use this feature only if your security strategy demands it.

If you export a policy template from an uninitialized partition, the **Sourced from partition** header field remains blank. This field is informational and you can still apply the template.

The **Policy Description** field is included in the template for user readability only. Policies are verified by the number in the **Policy ID** field.

```
Policy template FW Version 7.1.0
Field format - Policy ID:Policy Description:Policy Value:Off to on destructive:On to off
destructive
Sourced from partition: myPartition1, SN: 154438865290

0:"Allow private key cloning":1:1:0
1:"Allow private key wrapping":0:1:0
2:"Allow private key unwrapping":1:0:0
3:"Allow private key masking":0:1:0
4:"Allow secret key cloning":1:1:0
5:"Allow secret key wrapping":1:1:0
6:"Allow secret key unwrapping":1:0:0
7:"Allow secret key masking":0:1:0
10:"Allow multipurpose keys":1:1:0
11:"Allow changing key attributes":1:1:0
```

```

15:"Ignore failed challenge responses":1:1:0
16:"Operate without RSA blinding":1:1:0
17:"Allow signing with non-local keys":1:0:0
18:"Allow raw RSA operations":1:1:0
20:"Max failed user logins allowed":10:0:0
21:"Allow high availability recovery":1:0:0
22:"Allow activation":0:0:0
23:"Allow auto-activation":0:0:0
25:"Minimum pin length (inverted 255 - min)":248:0:0
26:"Maximum pin length":255:0:0
28:"Allow Key Management Functions":1:1:0
29:"Perform RSA signing without confirmation":1:1:0
31:"Allow private key unmasking":1:0:0
32:"Allow secret key unmasking":1:0:0
33:"Allow RSA PKCS mechanism":1:1:0
34:"Allow CBC-PAD (un)wrap keys of any size":1:1:0
39:"Allow Start/End Date Attributes":0:1:0
40:"Require Per-Key Authorization Data":0:1:0
41:"Partition Version":0:0:1

```

## Editing Guidelines and Restrictions

When creating or editing partition 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 partition will use the default values for that policy.
- > Partition policy templates from older Luna versions (6.x or earlier) cannot be applied to Luna 7.x partitions.
- > This version of the partition policy template feature is available on Luna 7.x application partitions only. When the active slot is set to a Luna 6.x partition, the **-exporttemplate** option is not available.
- > If you are using Secure Trusted Channel (STC) client connections, you cannot use partition policy templates.
- > The following restrictions apply when configuring partitions for Cloning or Key Export (see ["Configuring the Partition for Cloning or Export of Private/Secret Keys" on the next page](#) for more information):
  - **Partition policy 0: Allow private key cloning** and **partition policy 1: Allow private key wrapping** can never be set to **1** (ON) at the same time. Initialization fails if the template contains a value of **1** for both policies.
  - **Partition policy 1: Allow private key wrapping** must always have **Off-to-on** destructiveness set to **1** (ON). Initialization fails if the template contains a value of **0** in this field.
- > You may not use invalid policy values (outside the acceptable range), or values that conflict with your HSM or partition's capabilities. For example, **Partition capability 3: Enable private key masking** is always **0**, so you cannot set the corresponding partition policy to **1**. If you attempt to initialize a partition with a template containing invalid policy values, an error is returned and initialization fails.

If there is a mismatch between template policies and the default values of newer or dependent policies, then the attempt to apply the old policy would fail with **CKR\_FAILED\_DEPENDENCIES**.

You have the option to edit a policy file before applying it, to add newer policies.

## Applying a Partition Policy Template

The following procedure describes how to initialize a partition using a policy template.

### To apply a policy template to a new partition

1. Ensure that the template file is saved on the client workstation.
2. Launch LunaCM and set the active slot to the new partition.  
 lunacm:> **slot set -slot** <slotnum>
3. Initialize the partition, specifying a label and the policy template file. If the template file is not in the same directory as LunaCM, include the correct filepath.  
 lunacm:> **partition init -label** <label> **-applytemplate** <filepath/filename>
4. [Optional] Verify that the template has been applied correctly by checking the partition's policy settings. Include the **-verbose** option to view the destructiveness settings.  
 lunacm:> **partition showpolicies [-verbose]**

## Configuring the Partition for Cloning or Export of Private/Secret Keys

By default, the Luna Network HSM stores all keys in hardware, allowing private asymmetric and secret keys to be copied only to another Luna HSM (cloning). Cloning allows you to move or copy key material from a partition to a backup HSM or to another partition in the same HA group. You might, however, want to export private or secret keys to an encrypted file for off-board storage or use. Individual partitions can be configured in one of three modes for handling private keys.

**NOTE** This feature requires minimum firmware version 7.1.0. See [Version Dependencies by Feature](#) for more information.

The Partition SO can set the mode by changing the following policies (see ["Partition Capabilities and Policies" on page 272](#) for more information):

- > **Partition policy 0: Allow private key cloning** (default: **1**)
- > **Partition policy 1: Allow private key wrapping** (default: **0**)

**NOTE** These partition policies can never be set to **1** (ON) at the same time. An error will result (CKR\_CONFIG\_FAILS\_DEPENDENCIES) if it is attempted.

The policies can be set at the time of initialization, using a policy template (see ["Setting Partition Policies Using a Template" on page 284](#)) or by following the procedures described below:

- > ["Cloning Mode" on the next page](#)
- > ["Key Export Mode" on page 289](#)
- > ["No Backup Mode" on page 289](#)

**NOTE** Partition configurations are listed in LunaCM as "Key Export With Cloning Mode". This indicates that the partition is *capable* of being configured for either Key Export or Cloning, with the mode of operation defined by the policies listed above. You can never configure a partition to allow both export and cloning of private keys at once.

## Cloning Mode

A partition in Cloning mode has the following capabilities and restrictions:

- > All keys/objects can be cloned to another partition or Luna Backup HSM in the same cloning domain.
- > All keys/objects are replicated within the partition's HA group.
- > Private asymmetric and secret keys cannot be wrapped off the HSM (cannot be exported to a file encrypted with a wrapping key).

In this mode, private and secret keys are never allowed to exist outside of a trusted Luna HSM in the designated cloning domain. Cloning mode is the default setting for new partitions.

### Setting Cloning Mode on a Partition

Cloning mode is the default setting on new partitions. If another mode was set previously, the Partition SO can use the following procedure to set Cloning mode. Use `lunacm:> partition showpolicies` to see the current policy settings.

**CAUTION!** Partition policy 0: Allow private key cloning is Off-to-On destructive by default. Back up any important cryptographic material on the partition before continuing. This destructiveness setting can be customized by initializing the partition with a policy template (see "Editing a Partition Policy Template" on page 285).

### To manually set Cloning mode on a partition

1. Log in to the partition as Partition SO.  
`lunacm:> slot set -slot <slotnum>`  
`lunacm:> role login -name po`
2. Set partition policy 1: Allow private key wrapping to 0 (OFF).  
`lunacm:> partition changepolicy -policy 1 -value 0`
3. Set partition policy 0: Allow private key cloning to 1 (ON).  
`lunacm:> partition changepolicy -policy 0 -value 1`

### To initialize a partition in Cloning mode using a policy template

Use a standard text editor to include the following lines in the policy template file (see "Editing a Partition Policy Template" on page 285):

```
0:"Allow private key cloning":1:1:0
1:"Allow private key wrapping":0:1:0
```



## Key Export Mode

A partition in Key Export mode has the following capabilities and restrictions:

- > Private asymmetric and secret keys cannot be cloned to other partitions nor to a Luna Backup HSM.
- > The partition cannot be part of an HA group (private keys will not be replicated).
- > All keys/objects, including private keys, can be wrapped off the HSM (can be exported to a file encrypted with a wrapping key).

This mode is useful when generating key pairs for identity issuance, where transient key-pairs are generated, wrapped off, and embedded on a device. They are not used on the HSM, but generated and issued securely, and then deleted from the HSM.

### Setting Key Export Mode on a Partition

The Partition SO can use the following procedure to set Key Export mode. Use `lunacm:> partition showpolicies` to see the current policy settings.

**CAUTION!** **Partition policy 1: Allow private key wrapping** is always Off-to-On destructive. Back up any important cryptographic material on the partition before continuing. This destructiveness setting cannot be changed with a policy template (see "[Editing Guidelines and Restrictions](#)" on page 286).

### To manually set Key Export mode on a partition

1. Launch LunaCM and log in to the partition as Partition SO.
 

```
lunacm:> slot set -slot <slotnum>
lunacm:> role login-name po
```
2. Set **partition policy 0: Allow private key cloning** to **0** (OFF).
 

```
lunacm:> partition changepolicy -policy 0 -value 0
```
3. Set **partition policy 1: Allow private key wrapping** to **1** (ON).
 

```
lunacm:> partition changepolicy -policy 1 -value 1
```

### To initialize a partition in Key Export mode using a policy template

Use a standard text editor to include the following lines in the policy template file (see "[Editing a Partition Policy Template](#)" on page 285):

```
0:"Allow private key cloning":0:1:0
1:"Allow private key wrapping":1:1:0
```

## No Backup Mode

A partition in No Backup mode has the following restrictions:

- > Private asymmetric and secret keys cannot be cloned to other partitions or to a Luna Backup HSM. All other objects can still be cloned.
- > Private asymmetric and secret keys cannot be wrapped off the HSM (exported to a file encrypted with a wrapping key). All other objects can still be wrapped off.

Without backup capability, private keys can never leave the HSM. This mode is useful when keys are intended to have short lifespans, and are easily replaced.

### Setting No Backup Mode on a Partition

The Partition SO can use the following procedure to set No Backup mode. Use `lunacm:> partition showpolicies` to see the current policy settings.

---

#### To manually set No Backup mode on a partition

1. Launch LunaCM and log in to the partition as Partition SO.  
`lunacm:> slot set -slot <slotnum>`  
`lunacm:> role login -name po`
2. If **partition policy 0: Allow private key cloning** is set to **1** (ON), set it to **0** (OFF).  
`lunacm:> partition changepolicy -policy 0 -value 0`
3. If **partition policy 1: Allow private key wrapping** is set to **1** (ON), set it to **0** (OFF).  
`lunacm:> partition changepolicy -policy 1 -value 0`

---

#### To initialize a partition in No Backup mode using a policy template

Use a standard text editor to include the following lines in the policy template file (see "[Editing a Partition Policy Template](#)" on page 285):

```
0:"Allow private key cloning":0:1:0
1:"Allow private key wrapping":0:1:0
```

# CHAPTER 10: Partition Roles

The security of an HSM and its cryptographic contents depends on well-controlled access to that HSM. A controlled access policy is defined by:

- > the set of users with valid login credentials for the appliance, the HSM and the application partition
- > the actions each user is allowed to perform when logged in (the user's role)

For example, an access policy that adheres to the PKCS#11 standard requires two roles: the security officer (SO), who administers the user account(s), and the standard user, who performs cryptographic operations. When a user logs in to the HSM, they can perform only those functions that are permitted for their role.

All cryptographic operations take place on an application partition. This partition is created on the HSM by the HSM SO and assigned to a registered client over a network (see [Application Partitions](#)). Partition roles allow the partition to function as an independent virtual HSM, with its own Security Officer and users. This design provides more flexibility in meeting the security needs of your organization. Personnel holding the roles described below must have administrative access to a client workstation with a partition assigned to it and Luna HSM Client installed. They do not require SSH access to LunaSH on the Luna Network HSM appliance.

The partition-level roles are as follows:

## Partition Security Officer (PO)

The Partition SO handles all administrative and configuration tasks on the application partition, including:

- > Initializing the partition, setting the PO credential, and setting a cloning domain for the partition (see ["Initializing an Application Partition" on page 268](#))
- > Configuring partition policies (see ["Partition Capabilities and Policies" on page 272](#))
- > Initializing the Crypto Officer role (see ["Initializing the Crypto Officer Role " on page 295](#))
- > Activating the partition (see ["Activation and Auto-activation on Multi-factor- \(PED-\) Authenticated Partitions" on page 299](#))

## Managing the Partition SO Role

Refer also to the following procedures to manage the PO role:

- > ["Before you can perform administrative tasks on the partition or its stored cryptographic objects, you must log in with the appropriate role:" on page 294](#)
- > ["Changing a Partition Role Credential" on page 297](#)

## Crypto Officer (CO)

The Crypto Officer is the primary user of the application partition and the cryptographic objects stored on it. The Crypto Officer has the following responsibilities:

- > Creating, deleting, and modifying cryptographic objects via user applications
- > Performing cryptographic operations via user applications

- > Managing backup and restore operations for partition objects:
  - ["Backup and Restore Using a Luna Backup HSM \(G5\)" on page 379](#)
  - ["Backup and Restore Using a Luna Backup HSM \(G7\)" on page 408](#)
- > Create and configure HA groups (see ["Setting Up an HA Group" on page 350](#))
- > Initializing the Crypto User role (see ["Initializing the Crypto User Role" on page 297](#))
- > The CO can modify keys - must provide per-key authorisation (PKA) data for unassigned keys
- > The CO can unblock blocked (due to per-key auth failures) PKA keys
- > The CO can increment usage counters and change/set the limit
- > The CO can perform SMK rollover

### Managing the Crypto Officer Role

Refer also to the following procedures to manage the CO role:

- > ["Before you can perform administrative tasks on the partition or its stored cryptographic objects, you must log in with the appropriate role:" on page 294](#)
- > ["Changing a Partition Role Credential" on page 297](#)

### Limited Crypto Officer (LCO)

The Limited Crypto Officer is a role needed for eIDAS compliance and the performance of Per Key Authorization functions, with a subset of the abilities and responsibilities of the Crypto Officer, but wider authority and ability than the Crypto User. The LCO is created by the partition CO. The LCO role is visible and accessible in V1 partitions if the Client software version is 10.3 or newer. The Limited Crypto Officer has the following abilities and responsibilities:

- > Creating, deleting, and modifying cryptographic objects via user applications
- > Performing cryptographic operations via user applications
  - The LCO can copy and modify keys and private objects- must provide per-key authorisation (PKA) data for unassigned keys
  - The LCO can increment usage counters, but cannot change/set the limit
  - The LCO cannot unblock blocked (due to per-key auth failures) PKA keys
  - The LCO can wrap/unwrap keys - must specify the per-key auth data for both the wrapping/unwrapping keys and the wrapped/unwrapped keys
  - The LCO can derive keys - must provide the per-key auth data for the key used for derivation and specify the per-key auth data for the key being derived in the template
  - The LCO can derive-and-wrap - must provide per-key auth data as above
  - The LCO can perform SKS operations (SIMExtract / SIMInsert)
  - The LCO cannot perform SMK rollover
- > Creating and configuring HA groups (see ["Setting Up an HA Group" on page 350](#))
- > Initializing the Crypto User role (see ["Initializing the Crypto User Role" on page 297](#))

## Managing the Limited Crypto Officer Role

Refer also to the following procedures to manage the LCO role:

- > ["Before you can perform administrative tasks on the partition or its stored cryptographic objects, you must log in with the appropriate role:" on the next page](#)
- > ["Changing a Partition Role Credential" on page 297](#)
- > The LCO role does not support cloning
- > The LCO role is not visible for V0 partitions.
- > The LCO role is subject to role-affecting partition policies like
  - Minimum PIN length [25]
  - Maximum PIN length [26]
  - Maximum failed challenge responses [15]
  - Maximum failed user logins allowed [20]
    - Upon reaching the limit, the LCO is locked out; CO and CU remain operational
    - Partition CO can unlock a locked LCO by resetting its credentials
- > The LCO can create and destroy private objects
- > The LCO can generate keys assigned or unassigned, but cannot assign a key after it is generated.
- > The LCO can delete keys
  - Unlike CO role, LCO must provide per-key authorization (PKA) data
  - LCO supports the “single-use signing keys” scenario where a user generates a key, signs with that key, and deletes the key
- > The LCO can modify keys - must provide per-key authorisation (PKA) data for unassigned keys
- > The LCO can increment usage counters but, unlike CO, cannot change/set the limit
- > The LCO can wrap/unwrap
  - PKA behaviour for wrap: must provide the per-key auth data for both the wrapping and the wrapped keys
  - PKA behaviour for unwrap: must provide the per-key auth data for unwrapping key and specify the per-key auth data for the unwrapped key in the template
- > For PKA operation
  - The LCO can derive keys
  - The LCO can derive-and-wrap
- > The LCO can extract/insert in all scenarios
  - Including SKS key migration (old SKS: Insert; no Extract)
  - Including new SKS (Extract and Insert)
- > The LCO cannot clone/replicate in any scenario - this means that LCO is not self-sufficient for HA; the CO is needed to clone SMK(s)
- > Unlike the CO, the LCO cannot perform SMK rollover

## Crypto User (CU)

The Crypto User is an optional role that can perform cryptographic operations using partition objects in a read-only capacity, but can create only public objects. This role is useful in that it provides limited access; the Crypto Officer is the only role that can make significant changes to the contents of the partition. The Crypto User has the following capabilities:

- > Performing operations like encrypt/decrypt and sign/verify using objects on the partition
- > Creating and backing up public objects:
  - ["Backup and Restore Using a Luna Backup HSM \(G5\)" on page 379](#)
  - ["Backup and Restore Using a Luna Backup HSM \(G7\)" on page 408](#)
- > The CU can increment usage counters but, unlike CO, cannot change/set the limit

### Managing the Crypto User Role

Refer also to the following procedures to manage the CU role:

- > ["Before you can perform administrative tasks on the partition or its stored cryptographic objects, you must log in with the appropriate role:" below](#)
- > ["Changing a Partition Role Credential" on page 297](#)

Before you can perform administrative tasks on the partition or its stored cryptographic objects, you must log in with the appropriate role:

- > Partition Security Officer (specify **po** for <role>)
- > Crypto Officer (specify **co** for <role>)
- > Crypto User (specify **cu** for <role>)

### To log in to the application partition

1. Launch LunaCM on the Luna Network HSM client workstation.
2. Set the active slot to the desired partition.
3. Log in by specifying your role on the partition.

```
lunacm:> slot set -slot <slotnum>
```

```
lunacm:> role login -name <role>
```

You are prompted for the role's credential.

## Failed Partition Login Attempts

The consequences of multiple failed login attempts vary by role, depending on the severity of the security risk posed by that role being compromised. This is a security feature meant to thwart repeated, unauthorized attempts to access your cryptographic material.

**NOTE** The system must actually receive some erroneous/false information before it logs a failed attempt; if you merely forget to insert a PED key, or insert the wrong color key, that is not counted as a failed attempt. You must insert an incorrect PED key of the correct type, or enter an incorrect PED PIN or challenge secret, to fail a login attempt.

## Partition Security Officer

If you fail ten consecutive Partition SO login attempts, the partition is zeroized and all cryptographic objects are destroyed. The Partition SO must re-initialize the partition and Crypto Officer role, who can restore key material from a backup device.

## Crypto Officer

If you fail ten consecutive Crypto Officer login attempts, the CO and CU roles are locked out. The default lockout threshold of 10 is governed by partition policy 20: Max failed user logins allowed, and the Partition SO can set this threshold lower if desired (see ["Partition Capabilities and Policies" on page 272](#)). Recovery depends on the setting of **HSM policy 15: Enable SO reset of partition PIN**:

- > If HSM policy 15 is set to **1** (enabled), the CO and CU roles are locked out. The Partition SO must unlock the CO role and reset the credential (see ["If necessary, the Crypto Officer can reset the Crypto User credential at any time, without providing the current credential. This is useful in cases where the Crypto User credential has been lost or otherwise compromised." on page 298](#)).
- > If HSM policy 15 is set to **0** (disabled), the CO and CU roles are permanently locked out and the partition contents are no longer accessible. The Partition SO must re-initialize the partition and the Crypto Officer role, who can restore key material from a backup. This is the default setting.

**CAUTION!** If this is not the desired outcome, ensure that the HSM SO enables this destructive policy before creating and assigning partitions to clients.

## Crypto User

If you fail ten consecutive Crypto User login attempts, the CU role is locked out. The default lockout threshold of 10 is governed by partition policy **20: Max failed user logins allowed**, and the Partition SO can set this threshold lower if desired (see ["Partition Capabilities and Policies" on page 272](#)). The CO must unlock the CU role and reset the credential (see ["If necessary, the Crypto Officer can reset the Crypto User credential at any time, without providing the current credential. This is useful in cases where the Crypto User credential has been lost or otherwise compromised." on page 298](#)).

The following procedures will allow you to initialize the Crypto Officer (CO) and Crypto User (CU) roles and set an initial credential.

As of Network appliance software 7.7.1 (and newer), in addition to creating an application partition, the administrator (HSM SO) can also initialize the partition, creating the PSO role. The administrator can then use the new PSO credential on that partition to initialize the Crypto Officer role. The Crypto User role is still created from the client side, via lunacm.

## Initializing the Crypto Officer Role

The Crypto Officer (CO) is the primary user of the application partition and the cryptographic objects stored on it. The Partition Security Officer (PO) must initialize the CO role and assign an initial credential.

### To initialize the Crypto Officer role from the Client via lunacm

1. In LunaCM, log in to the partition as Partition SO (see ["Before you can perform administrative tasks on the partition or its stored cryptographic objects, you must log in with the appropriate role:" on the previous page](#)).

```
lunacm:> role login -name po
```

- Initialize the Crypto Officer role. If you are using a password-authenticated partition, specify a CO password. If you are using a PED-authenticated partition, ensure that you have a blank or rewritable black PED key available. Refer to ["Creating PED Keys" on page 224](#) for details on creating PED keys.

In LunaCM, passwords and activation challenge secrets must be 7-255 characters in length (**NOTE:** If you are using firmware version 7.0.x, 7.3.3, or 7.4.2, activation challenge secrets must be 7-16 characters in length). The following characters are allowed:

abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789 !@#\$%^&\* ()\_-+[]{}|\|/;:'.<>?`~

Double quotation marks (") are problematic and should not be used within passwords.

Spaces are allowed; to specify a password with spaces using the **-password** option, enclose the password in double quotation marks.

```
lunacm:> role init -name co
```

- Provide the CO credential to your designated Crypto Officer.

**NOTE** If **HSM policy 21: Force user PIN change after set/reset** is enabled (this is the default setting), the CO must change the credential before any other actions are permitted. See ["Changing a Partition Role Credential" on the next page](#).

### To initialize the Crypto Officer role from the Network appliance via lunash

The following steps assume that the Network HSM administrator has created the partition ( ["partition create" on page 1](#) ) and has initialized the partition ( ["partition init " on page 1](#) ), thus initializing the PSO role for that partition.

- In LunaSH, log in to the HSM as SO if you are not already logged in.

```
lunash:> "hsm login" on page 1
```

- Initialize the Crypto Officer role, providing the partition name, the PSO credential (already created) for that partition, and the credential for the CO that is being created. If you are using a password-authenticated partition, specify a CO password. If you are using a PED-authenticated partition, ensure that you have a blank or rewritable black PED key available. Refer to ["Creating PED Keys" on page 224](#) for details on creating PED keys.

In LunaSH, the SO or CO password must be 7-255 characters in length. The following characters are allowed:

abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789 !@#\$%^&\* ()\_-+[]{}|/;:'.<>?`~

The following characters are invalid or problematic and must not be used in the HSM SO password:

"&;<>`|

Spaces are allowed; to specify a password with spaces, enclose the password in double quotation marks.

```
lunash:> "partition init co [LUNA-16119]" on page 1 -partition <partition name> -psopin
<PSO'spassword> -copin <CO's password>
```

(Text credentials presented at the command line are ignored for PED-authenticated HSMs.)

- Provide the CO credential to your designated Crypto Officer.



**NOTE** If **HSM policy 21: Force user PIN change after set/reset** is enabled (this is the default setting), the CO must change the credential before any other actions are permitted. This is done from a registered client, via lunacm commands -- see ["Changing a Partition Role Credential" below](#).

Any crypto operations, as well as initialization of the Crypto User role, performed by the CO, are done from a registered client via a suitable API, or lunacm commands, respectively.

### Initializing the Crypto User Role

The Crypto User (CU) is an optional role that can perform cryptographic operations using partition objects in a read-only capacity, but can only create public objects. The Crypto Officer must initialize the CU role and assign an initial credential.

#### To initialize the Crypto User role

1. In LunaCM, log in to the partition as Crypto Officer (see ["Before you can perform administrative tasks on the partition or its stored cryptographic objects, you must log in with the appropriate role:"](#) on page 294).

```
lunacm:> role login -name co
```

2. Initialize the Crypto User role. If you are using a password-authenticated partition, specify a CU password. If you are using a PED-authenticated partition, ensure that you have a blank or rewritable gray PED key available. Follow the instructions on the Luna PED screen. Refer to ["Creating PED Keys" on page 224](#) for details on creating PED keys.

In LunaCM, passwords and activation challenge secrets must be 7-255 characters in length (**NOTE:** If you are using firmware version 7.0.x, 7.3.3, or 7.4.2, activation challenge secrets must be 7-16 characters in length). The following characters are allowed:

```
abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789 !@#$%^&* () - _ = + [] { } \ | / ; : ' , . < > ? ` ~
```

Double quotation marks (") are problematic and should not be used within passwords.

Spaces are allowed; to specify a password with spaces using the **-password** option, enclose the password in double quotation marks.

```
lunacm:> role init -name cu
```

3. Provide the CU credential to your designated Crypto User.

**NOTE** If **HSM policy 21: Force user PIN change after set/reset** is enabled (this is the default setting), the CU must change the credential before any other actions are permitted. See ["Changing a Partition Role Credential" below](#).

## Changing a Partition 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 partition role (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 partition role credential

1. In LunaCM, log in using the role's current credential (see ["Before you can perform administrative tasks on the partition or its stored cryptographic objects, you must log in with the appropriate role:"](#) on page 294).

```
lunacm:> role login -name <role>
```

2. Change the credential for the logged-in role. If you are using a password-authenticated partition, specify a new password. If you are using a PED-authenticated partition, ensure that you have a blank or rewritable PED key available. Refer to ["Creating PED Keys"](#) on page 224 for details on creating PED keys.

In LunaCM, passwords and activation challenge secrets must be 7-255 characters in length (**NOTE:** If you are using firmware version 7.0.x, 7.3.3, or 7.4.2, activation challenge secrets must be 7-16 characters in length). The following characters are allowed:

```
abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789 !@#$%^&* () -_ =+ [] {} \ | / ; : ' , . < > ? ` ~
```

Double quotation marks (") are problematic and should not be used within passwords.

Spaces are allowed; to specify a password with spaces using the **-password** option, enclose the password in double quotation marks.

```
lunacm:> role changepw -name <role>
```

3. To change the CO or CU challenge secret for an activated PED-authenticated partition, specify the **-oldpw** and/or **-newpw** options.

```
lunacm:> role changepw -name <role> -oldpw <oldpassword> -newpw <newpassword>
```

**TIP** Where you have an HA Indirect Login setup (see ["HA Indirect Login \(firmware 7.7.0 and newer\)"](#) on page 1), your HSM is made accessible by other HSMs.

Adding a challenge secret to your role, that is unknown to other parties, does not prevent other parties from logging into your HSM.

Rather it prevents other parties from using your particular role without that extra credential.

To prevent other parties accessing your HSM, change the PIN.

If necessary, the Crypto Officer can reset the Crypto User credential at any time, without providing the current credential. This is useful in cases where the Crypto User credential has been lost or otherwise compromised.

### Prerequisites for Crypto Officer Reset

The Partition SO can also reset the Crypto Officer's credential, if **HSM policy 15: Enable SO reset of partition PIN** is enabled. By default, this policy is not enabled, and changing it is destructive. If you want the Partition SO to be able to reset the CO's credential, the HSM SO must enable this policy before creating the application partition (see ["Partition Capabilities and Policies"](#) on page 272).

**CAUTION!** HSM policy 15 is destructive when turned on. All partitions on the HSM and their contents will be erased.

## To reset the Crypto Officer , Limited Crypto Officer, or Crypto User credential

1. Log in with the appropriate role (see ["Before you can perform administrative tasks on the partition or its stored cryptographic objects, you must log in with the appropriate role:" on page 294](#)).
2. Reset the desired role's credential.

In LunaCM, passwords and activation challenge secrets must be 7-255 characters in length (**NOTE:** If you are using firmware version 7.0.x, 7.3.3, or 7.4.2, activation challenge secrets must be 7-16 characters in length). The following characters are allowed:

abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNopqrstuvwxyz0123456789 !@#\$%^&\* () -\_ =+ [] {} \ | / ; : ' , . < > ? ` ~

Double quotation marks (") are problematic and should not be used within passwords.

Spaces are allowed; to specify a password with spaces using the **-password** option, enclose the password in double quotation marks.

lunacm:> **role resetpw -name** <role>

You are prompted to set a new credential for the role.

3. Provide the new credential to the Crypto Officer , Limited Crypto Officer(\*), or Crypto User.

**NOTE** If **HSM policy 21: Force user PIN change after set/reset** is enabled, the user must change the credential before any other actions are permitted. See ["Changing a Partition Role Credential" on page 297](#).

The CO can reset the LCO's primary credentials (lunacm:> **role resetpw**) regardless of the status of "Enable SO reset of a partition PIN" policy 15.

(\*LCO is applicable to firmware 7.7.0 and newer.)

## Activation and Auto-activation on Multi-factor- (PED-) Authenticated Partitions

A multi-factor-authenticated partition (also known as PED-authenticated) requires a PED key each time a role (Partition SO, Crypto Officer, Limited Crypto Officer, Crypto User) logs in. For some use cases, such as key vaulting, this physical key requirement is desirable. For many applications, however, it is impractical to require the full PED interaction every time.

For these use cases, the Partition SO can activate the partition and set a secondary password referred to as a challenge secret. When a partition is activated, the HSM caches the Crypto Officer and Limited Crypto Officer and Crypto User PED secrets upon first login, and subsequent logins require the challenge secret only. The PED key secret remains cached until the role is explicitly deactivated or the HSM loses power due to a reboot or power outage.

Activation does not provide much advantage for clients that log in to the partition and remain logged in. It is an indispensable advantage in cases where the client application repeatedly logs in to perform a task, and then logs out or closes the cryptographic session after the task is completed.

### Auto-activation

Auto-activation allows PED key credentials to remain cached even in the event of a reboot or a brief power outage (up to 2 hours).

## Tamper events and activation/auto-activation

When a tamper event occurs, or if an uncleared tamper event is detected on reboot, the cached PED key data is zeroized, and activation/auto-activation is disabled. See [Tamper Events](#) and ["Partition Capabilities and Policies" on page 272](#) for more information.

This section contains instructions for the following procedures:

- > ["Enabling Activation on a Partition" below](#)
- > ["Activating a Role" below](#)
- > ["Enabling Auto-activation" on the next page](#)
- > ["Deactivating a Role" on page 302](#)

## Enabling Activation on a Partition

The Partition SO can enable activation on a partition by setting **partition policy 22: Allow activation** to 1 (on). This setting enables activation for the Crypto Officer and Limited Crypto Officer and Crypto User roles. When partition policy 22 is enabled, the Partition SO can set an initial challenge secret for the Crypto Officer.

### Prerequisites

- > The partition must be initialized (see ["Initializing an Application Partition" on page 268](#)).

---

### To enable activation on a partition

1. Log in to the partition as Partition SO (see ["Before you can perform administrative tasks on the partition or its stored cryptographic objects, you must log in with the appropriate role:" on page 294](#)).

```
lunacm:> role login -name po
```

2. Enable partition policy 22.

```
lunacm:> partition changepolicy -policy 22 -value 1
```

## Activating a Role

After enabling partition policy 22, activate the CO or LCO or CU roles on the partition. You must set a PED challenge password for each role you want to activate. The Partition SO must set the initial challenge secret for the Crypto Officer, who must set it for the Limited Crypto Officer or Crypto User. The role becomes activated the first time the user logs in to the partition.

### Prerequisites

- > **Partition policy 22: Allow activation** must be enabled on the partition (see ["Enabling Activation on a Partition" above](#)).
- > The role you wish to activate must be initialized on the partition (see ["The following procedures will allow you to initialize the Crypto Officer \(CO\) and Crypto User \(CU\) roles and set an initial credential." on page 295](#)).

## To activate a role

- Log in to the partition using the appropriate role (see ["Before you can perform administrative tasks on the partition or its stored cryptographic objects, you must log in with the appropriate role:"](#) on page 294):
  - If you are activating the Crypto Officer role, log in as Partition SO.
  - If you are activating the Crypto User or Limited Crypto Officer role, log in as Crypto Officer.

```
lunacm:> role login -name <role>
```

- Set an initial challenge secret for the role you wish to activate. The length of the challenge secret is configurable by the Partition SO (see ["Partition Capabilities and Policies"](#) on page 272).

In LunaCM, passwords and activation challenge secrets must be 7-255 characters in length (**NOTE:** If you are using firmware version 7.0.x, 7.3.3, or 7.4.2, activation challenge secrets must be 7-16 characters in length). The following characters are allowed:

```
abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789 !@#$%^&*()-_+[]{}|/;:'.<>?`~
```

Double quotation marks (") are problematic and should not be used within passwords.

Spaces are allowed; to specify a password with spaces using the **-password** option, enclose the password in double quotation marks.

```
lunacm:> role createchallenge -name <role>
```

**NOTE** Activation requires that a challenge secret is set for the specified role. If the role does not have a challenge secret, you are prompted for the PED key, regardless of the policy setting.

- Log out of the partition.

```
lunacm:> role logout
```

- Provide the initial challenge secret to the designated CO or CU by secure means. The PED secret is cached when they log in for the first time. The CO or CU can store the black or gray PED key in a safe place. The cached PED secret allows their application(s) to open and close sessions and perform operations within those sessions.

**NOTE** If **HSM policy 21: Force user PIN change after set/reset** is enabled (this is the default setting), the CO or CU must change the challenge secret before any other actions are permitted. See ["Changing a Partition Role Credential"](#) on page 297.

**NOTE** The PED screen prompts for a Black PED Key for any of "User", "Crypto Officer", "Limited Crypto Officer", "Crypto User". The PED is not aware that the key you present has a black or a gray sticker on it. The colored stickers are visual identifiers for your convenience in keeping track of your PED Keys. You differentiate by how you label, and how you use, a given physical key that the PED sees as "black" (once it has been imprinted with a secret).

## Enabling Auto-activation

Auto-activation allows PED key credentials to be cached even in the event of a reboot or a brief power outage (up to 2 hours). Clients can re-connect and continue using the application partition without needing to re-authenticate using a PED key.

The Partition SO can enable auto-activation on a partition by setting **partition policy 23: Allow auto-activation**.

### Prerequisites

- > **Partition policy 22: Allow activation** must be enabled on the partition (see ["Enabling Activation on a Partition" on page 300](#)).

### To enable auto-activation on a partition

1. Log in to the partition as Partition SO (see ["Before you can perform administrative tasks on the partition or its stored cryptographic objects, you must log in with the appropriate role:" on page 294](#)).  
 lunacm:> **role login -name po**
2. Enable partition policy 23.  
 lunacm:> **partition changepolicy -policy 23 -value 1**  
 Auto-activation takes effect for each affected role (CO and/or CU) the next time the role is authenticated.
3. [Optional] For optimal reliability, the Luna Network HSM **admin** or **operator** can set the appliance to reboot automatically if it fails to complete a normal shutdown. Log in to LunaSH to change this setting.  
 lunash:> **sysconf appliance rebootonpanic enable**

## Deactivating a Role

An activated role on a partition remains activated until it is explicitly deactivated, or the HSM loses power due to a reboot or power outage (with auto-activation disabled). This deletes the cached PED secret for the role.

### Prerequisites

- > You must be authorized to deactivate the role. The CO and CU can manually deactivate their own or each other's roles. The Partition SO can deactivate both the CO and CU roles.

### To deactivate a role on a partition

1. Log in to the partition with the appropriate role (see ["Before you can perform administrative tasks on the partition or its stored cryptographic objects, you must log in with the appropriate role:" on page 294](#)).  
 lunacm:> **role login -name <role>**
2. Specify the role you wish to deactivate.  
 lunacm:> **role deactivate -name <role>**  
 This deletes the cached authentication credential for the role. The next time the role logs in, the credential is re-cached.
3. If you wish to disable activation entirely, so that credentials are not re-cached at the next login, the Partition SO can disable **partition policy 22: Allow activation**.  
 lunacm:> **partition changepolicy -policy 22 -value 0**
4. If partition policy 22 is disabled, auto-activation is also disabled (even though **partition policy 23: Allow auto-activation** is set to **1**). When partition policy 22 is enabled again, auto-activation resumes. To turn off auto-activation, you must disable partition policy 23.

```
lunacm:> partition changepolicy -policy 23 -value 0
```

## Security of Your Partition Challenge

For Luna Network HSMs with Password Authentication, the partition password used for administrative access by the Crypto Officer is also the partition challenge secret or password used by client applications.

For Luna Network HSMs with PED Authentication, the partition authentication used for administrative access by the Crypto Officer is the secret on the black PED key(s) for that partition. The partition challenge secret or password used by client applications is a separate character string, set by the Partition SO and then changed by the Crypto Officer (mandatory) for the CO's use. This is one way in which we implement separation of roles in the Luna HSM security paradigm.

### How Secure Is the Challenge Secret or Password?

The underlying concern is that a password-harvesting attack might eventually crack the secret that protects the partition. Layers of protection are in place, to minimize or eliminate such a risk.

**First**, such an attack must be run from a Luna HSM Client computer. For interaction with HSM partitions on a Luna Network appliance, like Luna Network HSM, a Luna HSM Client computer is one with Luna software installed, on which you have performed the exchange of certificates to create a Network Trust Link (NTL). That exchange requires the knowledge and participation of the appliance administrator and the Partition SO (who might, or might not, be the same person). It is not possible to secretly turn a computer into a Client of a Luna HSM partition - an authorized person within your organization must participate.

**Second**, for Luna HSMs with password authentication, you set the partition password directly when you create the partition, so you can make it as secure as you wish (for an example of guidance on password strength, see <http://howsecureismypassword.net/> or <http://xkcd.com/936/>)

For Luna HSMs with PED authentication, an optional partition password (also called a challenge secret) may be added for the initialized Crypto Officer (CO) and/or Crypto User (CU) roles. See [role createchallenge](#) for the proper command syntax.

Using LunaCM or LunaSH, you can change the partition password (or challenge secret) if you suspect it has been compromised, or if you are complying with a security policy that dictates regular password changes.

As long as you replace any password/challenge secret with one that is equally secure, the possible vulnerability is extremely small.

Conversely, you can choose to replace a secure, random password/challenge-secret with one that is shorter or more memorable, but less secure - you assume the risks inherent in such a tradeoff.

**Third**, Luna HSM **partition policy 15: Ignore failed challenge responses** can be set to **0** (off). When that policy is off, the HSM stops ignoring bad challenge responses (that is, attempts to submit the partition secret) and begins treating them as failed login attempts. Each bad login attempt is counted. **Partition policy 20: Max failed user logins allowed** determines how high that count can go before the partition is locked out.

Once a partition is locked by bad login attempts, it cannot be accessed until the HSM Security Officer (SO) unlocks it. This defeats an automated harvesting attack that relies on millions of attempts occurring at computer-generated speeds. As well, after one or two lockout cycles, the HSM SO would realize that an attack was under way and would rescind the NTL registration of the attacking computer. That computer would no longer exist as far as the HSM partition was concerned. The SO or your security organization would then investigate how the client computer had been compromised, and would correct the problem before allowing

any new NTL registration from that source. See ["Before you can perform administrative tasks on the partition or its stored cryptographic objects, you must log in with the appropriate role:"](#) on page 294 for more information.

As the owner/administrator of the HSM, you determine any tradeoffs with respect to security, convenience, and other operational parameters.

## Name, Label, and Password Requirements

This page describes length and character requirements for setting names, labels, domains, passwords, and challenge secrets on the Luna Network HSM. This information can also be found in relevant sections throughout the documentation. Refer to the applicable section below:

- > ["Custom Appliance User Accounts" below](#)
- > ["Custom Appliance Roles" below](#)
- > ["Appliance User Passwords" below](#)
- > ["HSM Labels" on the next page](#)
- > ["Cloning Domains" on the next page](#)
- > ["Partition Names" on the next page](#)
- > ["Partition Labels" on the next page](#)
- > ["HSM/Partition Role Passwords or Challenge Secrets" on the next page](#)

### Custom Appliance User Accounts

LunaSH user names can be 1-32 characters in length, chosen from letters a-z, or A-Z, numbers 0-9, the dash, the dot, or the underscore:

abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNopQRSTUVWXYZ0123456789-.\_

No spaces are allowed. User names cannot begin with a dot, dash, or number. As with any secure system, no two users (regardless of role) can have the same name.

### Custom Appliance Roles

LunaSH role names can be 1-64 characters in length. The following characters are allowed:

abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNopQRSTUVWXYZ0123456789-.\_

No spaces are allowed. Role names cannot start with a dot or dash. Creating a role name that begins with a number is not recommended. As with any secure system, no two roles can have the same name.

### Appliance User Passwords

LunaSH passwords must be at least eight characters in length, and include characters from at least three of the following four groups:

- > lowercase alphabetic: abcdefghijklmnopqrstuvwxyz
- > uppercase alphabetic: ABCDEFGHIJKLMNOPQRSTUVWXYZ



- > numeric: 0123456789
- > special (spaces allowed): !@#\$%^&\*()-\_+=[]{}|/;:'",.<>?`~

## 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. Only alphanumeric characters and the underscore are allowed:

```
abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789_
```

## Cloning Domains

The domain string must be 1-128 characters in length. The following characters are allowed:

```
abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789 !@#$%^&*-_+=[]{}/:'",.~
```

The following characters are problematic or invalid and must not be used in a domain string: "&;<>\`|()

Spaces are allowed, as long as the leading character is not a space; to specify a domain string with spaces using the **-domain** option, enclose the string in double quotation marks.

## Partition Names

Partition names created in LunaSH must be 1-32 characters in length. The following characters are allowed:

```
abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ 0123456789!@#$%^&*()-_+=[]{}[:;./?~
```

Spaces are allowed; enclose the partition name in double quotes if it includes spaces.

The following characters are not allowed: &\|;<>`'?"

No two partitions can have the same name.

## Partition Labels

The partition label created during initialization must be 1-32 characters in length. If you specify a longer label, it will automatically be truncated to 32 characters. The following characters are allowed:

```
abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789 !@#$%^&*()-_+=[]{}|/;:'",.<>`~
```

Question marks (?) and double quotation marks (") are not allowed.

Spaces are allowed; enclose the label in double quotation marks if it includes spaces.

## HSM/Partition Role Passwords or Challenge Secrets

In LunaSH, the SO or CO password must be 7-255 characters in length. The following characters are allowed:

```
abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789 !@#$%^&*()-_+=[]{}/:'",.~
```

The following characters are invalid or problematic and must not be used in the HSM SO password: "&;<>\`|()

Spaces are allowed; to specify a password with spaces, enclose the password in double quotation marks.

In LunaCM, passwords and activation challenge secrets must be 7-255 characters in length (**NOTE:** If you are using firmware version 7.0.x, 7.3.3, or 7.4.2, activation challenge secrets must be 7-16 characters in length).

The following characters are allowed:

```
abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789 !@#$%^&*()-_+=[]{}|/;:'",.<>?`~
```

Double quotation marks (") are problematic and should not be used within passwords.

Spaces are allowed; to specify a password with spaces using the **-password** option, enclose the password in double quotation marks.

# CHAPTER 11: Verifying the HSM's Authenticity

Hardware Security Modules have traditionally been deployed in the corporate data center's most secure zone. Establishing trust with the HSM is, in part, achieved by physical access control. In cases of remote client usage (such as cloud cryptography), the client needs a way to verify the authenticity of the device protecting their most valued cryptographic keys.

## Public Key Confirmations

Thales's Luna HSMs include factory-issued device identities certified by a Thales authority. The root of this authority is maintained by Thales in HSMs locked in a vault with layered physical and logical access controls. These certificates are used as the root of trust for the issuance of "public key confirmations" (PKCs), certificates issued by the HSM attesting to the life cycle of a specific private key. A Luna HSM will issue confirmations only for private keys that were created by the HSM and that can never exist outside of the HSM. A valid confirmation is cryptographic proof that a specific key is inside the identified HSM. The confirmation is also proof that that the identified HSM is real.

The key pair within the HSM that signs the confirmation is called a Hardware Origin Key (HOK). It is protected inside the HSM's FIPS 140-2 Level 3 security boundary. Each HOK is unique and there is no way to extract or replace it. The HOK is created in the HSM at the time of manufacture and certified by Thales's secure manufacturing authority, which is certified by Thales's root authority.

Public key confirmations are automatically generated for RSA key pairs in the HSM. A user can get a confirmation through the PKCS #11 API or the Luna **cmu** utility, and use it to verify that any RSA key is protected and has always been protected by a Luna HSM. A PKC bundle contains the following certificates:

- > **MIC:** Manufacturing Integrity Certificate; corresponds to the Manufacturing Integrity Private Key (MIK), signed by the SafeNet Root.
- > **HOC:** Hardware Origin Certificate; corresponds to the Hardware Origin Private Key (HOK). Unique to each HSM. Signed by MIK.
- > **DAC:** Device Authentication Certificate; corresponds to the Device Authentication Private Key (DAK). Unique to each HSM. Signed by HOK.
- > **PKC:** Public Key Confirmation Certificate; certificate for a private key on the HSM. Signed by DAK.

Public key confirmations are delivered as PKCS #7 files containing a certificate chain. The PKCS #7 files can be viewed using tools like OpenSSL and Microsoft's Certificates snap-in for MMC.

**NOTE** While third-party tools are capable of cryptographically validating the certificate signature chain, they may display some certificate errors, since they do not recognize some SafeNet-specific key usage attributes included in the certificates.

## Chains of Trust

The chain of trust available via the **cmu** utility included with the Luna HSM Client, **Chrysalis-ITS**, is built in by default, and originates from Thales's root certificate authority. It uses the MIC, HOC, DAC, and the PKC.

**NOTE** Since the introduction of Functionality Modules, HSMs are shipped from the factory with FM-ready hardware. This means that they contain, and use, the HOK and the HOC, but they also have the FM-HOK and FM-HOC on standby. If FMs are enabled on the HSM, the original HOK and HOC are deleted, and the chain-of-trust, thereafter, proceeds through the FM-HOC.

## Verifying the HSM's Authenticity

The **cmu** utility also includes a command, **cmu verifyhsm**, that tests an HSM's authenticity by creating and verifying a confirmation on a temporary key created in the HSM. The test includes a proof of possession that asks the HSM to sign a user-entered string as proof the associated private key is present within the target HSM.

**NOTE** This confirmation procedure is currently not supported on FM-enabled HSMs. Refer to [FM Deployment Constraints](#) for details.

The test requires the SafeNet root certificate, provided below:



**safenet-root.pem**

**NOTE** The current certificate is valid until 2031-12-31, but it might change before this date at Thales's discretion. Ensure that you have the most recent version of this documentation.

### To verify the HSM's authenticity

1. Right-click the link above and save the root certificate to the Luna HSM Client directory.
2. Open a command line and navigate to the Luna HSM Client directory.
3. Use the **cmu** utility to authenticate the HSM. You must specify a challenge string for the HSM to sign, and the root certificate file:

```
cmu verifyhsm -challenge <string> -rootcert safenet-root.pem
```

When prompted, specify the partition you wish to use and the Crypto Officer credential for that partition.

```
>cmu verifyhsm -challenge "1234567890" -rootcert safenet-root.pem
Select token
[0] Token Label: mypartition-1
[1] Token Label: mypartition-2
```

```
Enter choice: 0
Please enter password for token in slot 0 : *****
Reading rootcert from file "safenet-root.pem"... ok.
Generating temporary RSA keypair in HSM... ok.
Extracting PKC bundle from HSM... ok.
Verifying PKC certificate... ok.
Verifying DAC certificate... ok.
Verifying HOC certificate... ok.
Verifying MIC certificate... ok.
Verifying MIC against rootcert... ok.
Signing and verifying challenge... ok.
Verifying HSM serial number... ok.
Overall status: Success.
```

If this test fails, contact the HSM SO.

# CHAPTER 12: Migrating Keys to Your New HSM

This chapter describes how to migrate your keys and configuration from a Luna HSM 5.x or 6.x partition to a Luna HSM 7.x partition by using one of three methods; backup and restore, cloning, or cloning using a temporary HA group:

- > ["Luna Network HSM \(5.x or 6.x\) to Luna Network HSM \(7.x\)" on the next page](#)
- > ["Luna USB HSM \(5.x or 6.x\) to Luna Network HSM \(7.x\)" on page 318](#)
- > ["Luna PCIe HSM \(5.x or 6.x\) to Luna Network HSM \(7.x\)" on page 322](#)
- > ["Luna PCIe HSM or Luna USB HSM \(5.x or 6.x\) to Luna PCIe HSM \(7.x\)" on page 327](#)
- > ["Moving from Pre-7.7.0 to Firmware 7.7.0 or Newer" on page 334](#)

Refer also to the chapter on ["Key Cloning" on page 166](#), particularly ["Cloning Keys Between Luna 6, Luna 7, and Luna Cloud HSM" on page 171](#).

This document guides you through several migration scenarios consisting of older and newer Luna HSMs, using each applicable migration method. Before migrating, preconditions are provided for each scenario that must be met. There are specific user roles that are identified for performing the migration. In addition, both authentication methods (password and PED-authenticated) are supported.

## Supported Luna HSMs

This document describes key migration for these Luna HSMs:

- > Luna Network HSM, version 5.x or 6.x to 7.x
- > Luna USB HSM, version 5.x or 6.x to 7.x
- > Luna PCIe HSM, version 5.x or 6.x to 7.x

## Migration methods

The three migration methods used in this guide are:

- > Backup and restore

The backup and restore method uses the LunaCM **partition archive backup** command to backup key material on an HSM (5.x or 6.x) partition and the Restore command to then restore this material to an HSM 7.x partition.
- > Cloning

The cloning method uses the LunaCM **partition clone** command to clone from an HSM (5.x or 6.x) partition to an HSM 7.x partition. It is also referred to as slot-to slot cloning.
- > Cloning using an HA group

The HA group method uses the LunaCM **ha synchronize** command on members of a temporary HA group consisting of a 5.x or 6.x HSM and a 7.x HSM, set up solely for the purpose of migration. After migration, this group should be removed since the members are not using the same software version.

## Preconditions

Each migration procedure in this document is prefaced by a "Preconditions" section that specifies the hardware and software requirements along with any assumptions the procedure is using to perform the migration steps. Examples are a 5.x or 6.x HSM, a 7.x HSM, 5.x, 6.x or 7.x client software, user roles and the slot #s used in the procedure.

## Roles required for migration

The following partition roles are needed to migrate key material:

- > Partition Security Officer. The partition security officer role is needed to perform LunaCM HA operations and to create the Crypto Officer role.
- > Partition Crypto Officer. The partition Crypto Officer role is needed to perform LunaCM backup/restore and cloning operations.

**NOTE** When logging in to a partition, be mindful of whether you're working with pre-PPSO or PPSO firmware. Use the **partition login** command if your HSM has pre-PPSO firmware (version 6.21.2 and earlier). Use the **role login** command if your HSM has PPSO firmware (version 6.22.0 and later). Also, with PPSO firmware 6.22.0 and later (up to but not including firmware 7.x), be careful with user names; that is, type **Crypto Officer** in full (is case sensitive) and not the abbreviation **co**.

In firmware version release 7.x, partition login name requirements allow for abbreviations. That is, you can log in using **po** for Partition Security Officer or **co** for Crypto Officer.

## Luna Network HSM (5.x or 6.x) to Luna Network HSM (7.x)

This chapter describes how to migrate your key material from a release 5.x or 6.x Luna Network HSM partition to a release 7.x Luna Network HSM partition. You can migrate your key material using one of the following three methods:

- > ["Backup and Restore" below](#)
- > ["Cloning" on page 314](#)
- > ["Cloning Using an HA Group" on page 316](#)

## Backup and Restore

Cryptographic key material can be backed up and then restored to a release 7.x Luna Network HSM partition using a Luna Backup HSM.

The new configuration's operating system must be compatible with both the new 7.x and the old 5.x/6.x hardware. Consult the 5.x/6.x CRN for a list of compatible operating systems.

To backup and restore cryptographic keys from one HSM to another, the HSMs must share the same cloning domain. For password-authenticated HSMs, this domain should have been specified when the partition was initialized. For PED-authenticated HSMs, the red key determines the cloning domain. You will need the same red key that was imprinted during 5.x/6.x partition creation to initialize the 7.x partition (see ["Initializing an Application Partition" on page 268](#)).

The 7.x client software should be installed, and the connection to both the source and destination partitions verified, before attempting this procedure (see ["Luna HSM Client Software Installation" on page 17](#) for details). The source and destination partitions must both be assigned to the client machine issuing the backup and restore commands (see ["Client-Partition Connections" on page 86](#) for details). Use **slot list** to ensure both partitions are visible to the client.

### Preconditions

The following instructions assume that:

- > the 10.x client software has been installed
- > an uninitialized partition has been created on the 7.x HSM
- > the source and destination partitions are both registered with the client (visible)
- > the source partition's security policy allows cloning of private and secret keys

In the following example:

- > Slot 0: the source 5.x/6.x partition
- > Slot 1: the destination 7.x partition
- > Slot 2: the Backup HSM partition

**NOTE** Partition login name requirements have changed with the hardware versions. With release 7.x, you can log in using the abbreviated **po** (Partition Security Officer) or **co** (Crypto Officer).

### To migrate cryptographic keys from a 5.x/6.x partition to a 7.x partition using a Backup HSM

Follow these steps to back up all cryptographic material on a 5.x/6.x partition to a Backup HSM, and restore to a new 7.x partition.

1. Run LunaCM, set the current slot to the 7.x partition, and initialize the partition and the Partition SO role.

**slot set -slot 0**

**partition init -label <7.x\_partition\_label>**

- a. If you are backing up a PED-authenticated 5.x/6.x partition, use the 5.x/6.x partition's red key when prompted.
- b. If you are backing up a password-authenticated 5.x/6.x partition, enter the same cloning domain when prompted.

2. Log in as the **po** (Partition Security Officer) and initialize the **co** (Crypto Officer) role.

**role login -name po**

**role init -name co**



If you are backing up a PED-authenticated 5.x/6.x partition, you can create an optional challenge secret for the Crypto Officer.

**role createchallenge -name co -challengeSecret <password>**

3. Connect your backup HSM and make sure it is visible to the client, along with the 5.x/6.x and 7.x HSMs.
4. Set the current slot to the source 5.x/6.x slot.

**slot list**

**slot set -slot 0**

5. Log in as the Crypto Officer.

**NOTE** Be mindful of whether you're working with pre-PPSO or PPSO firmware and use the **partition login** or **role login** commands as specified below. Also, with PPSO firmware 6.22.0 and up, be careful with user names, i.e., type **Crypto Officer** in full (is case sensitive) and not **co**.

- a. If you are cloning a release 5.x or 6.x pre-PPSO partition (up to and including Firmware 6.21.2), use:

**partition login**

- b. If you are cloning a release 6.x PPSO partition (Firmware 6.22.0 and up), use:

**role login -name Crypto Officer**

6. Optional: To verify the objects in the 5.x/6.x partition to be cloned, issue the "partition contents" command.

**partition contents**

7. Back up the 5.x/6.x partition contents to the Backup HSM.

**partition archive backup -slot 2 -partition <backup\_label>**

- a. If you are backing up a PED-authenticated 5.x/6.x partition, use the 5.x/6.x partition's red key when prompted.
- b. If you are backing up a password-authenticated 5.x/6.x partition, enter the same cloning domain when prompted.

Optionally, verify that all objects were backed up successfully on the Backup HSM by checking the partition contents.

8. Set the current slot to the 7.x partition, log in as the Crypto Officer, and restore from backup.

**slot set -slot 1**

**role login -name co**

**partition archive restore -slot 2 -partition <backup\_label>**

Afterwards, you can verify the partition contents on the 7.x partition:

**partition contents**

## Cloning

The simplest method of migrating key material to a new 7.x partition is slot-to-slot cloning. This procedure copies all permitted cryptographic material from a 5.x/6.x Network HSM partition to a 7.x Network HSM partition.

The new configuration's operating system must be compatible with both the new 7.x and the old 5.x/6.x hardware. Consult the 5.x/6.x CRN for a list of compatible operating systems.

To clone cryptographic keys from one HSM to another, the HSMs must share the same cloning domain. For password-authenticated HSMs, this domain should have been specified when the partition was initialized. For PED-authenticated HSMs, the red key determines the cloning domain. You will need the same red key that was imprinted during 5.x/6.x partition creation to initialize the 7.x partition (see ["Initializing an Application Partition" on page 268](#)).

The 7.x client software should be installed, and the connection to both the source and destination partitions verified, before attempting this procedure (see ["Luna HSM Client Software Installation" on page 17](#) for details). The source and destination partitions must both be assigned to the client machine issuing the cloning commands (see ["Client-Partition Connections" on page 86](#) for details). Use **slot list** to ensure both partitions are visible to the client.

If the source partition contains asymmetric keys, its security policy must allow cloning of private and secret keys. Use `lunacm:> partition showpolicies` to ensure that your source partition's security template allows this. If the 5.x/6.x HSM's security template does not allow cloning of private/secret keys, the HSM Admin may be able to turn this feature on using `lunacm:> partition changepolicy`.

**CAUTION!** Check your source partition policies and adjust them to be sure you can clone private and symmetric keys. Depending on the configuration of your partition and HSM, these policies may be destructive.

### Preconditions

The following instructions assume that:

- > the 7.x client software has been installed
- > an uninitialized partition has been created on the 7.x Network HSM
- > the source and destination partitions must be registered with the client (visible)
- > the source 5.x/6.x partition's security policy allows cloning of private and secret keys

In the following examples:

- > Slot 0: the source 5.x/6.x partition
- > Slot 1: the destination 7.x partition

**NOTE** Partition login name requirements have changed with the hardware versions. With release 7.x, you can log in using the abbreviated **PO** (Partition Security Officer) or **CO** (Crypto Officer).

### To clone cryptographic keys from a 5.x/6.x partition to a 7.x partition

Follow these steps to clone all cryptographic material on a 5.x/6.x partition to a 7.x partition.

1. Run LunaCM, set the current slot to the 7.x partition, and initialize the Partition SO role.

**slot list**

**slot set -slot 1**

**partition init -label** <7.x\_partition\_label>

- a. If you are cloning a PED-authenticated 5.x/6.x partition, use the 5.x/6.x partition's red key when prompted.
  - b. If you are cloning a password-authenticated 5.x/6.x partition, enter the same cloning domain when prompted.
2. Log in as the **po** (Partition Security Officer) and initialize the **co** (Crypto Officer) role.

**role login -name po**

**role init -name co**

If you are cloning a PED-authenticated 5.x/6.x partition, you can create an optional challenge secret for the Crypto Officer.

**role createchallenge -name co -challengesecret** <password>

3. Set the current slot to the source 5.x/6.x slot, log in as the Crypto Officer.

**slot set -slot 0**

**NOTE** Be mindful of whether you're working with pre-PPSO or PPSO firmware and use the "partition login" or "role login" commands as specified below. Also, with PPSO firmware 6.22.0 and up, be careful with user names, i.e., type "Crypto Officer" in full (is case sensitive) and not "co".

- a. If you are cloning a release 5.x or 6.x pre-PPSO partition (up to and including Firmware 6.21.2), use:
- partition login**
- b. If you are cloning a release 6.x PPSO partition (Firmware 6.22.0 and up), use:
- role login -name Crypto Officer**
4. Optional: To verify the objects in the 5.x/6.x partition to be cloned, issue the "partition contents" command.
  5. Clone the objects to the 7.x partition slot (see ["partition clone" on page 1](#) for correct syntax).

**partition clone -objects 0 -slot 1**

Afterward, you can set the current slot to the 7.x partition and verify that all objects have cloned successfully.

**slot set -slot 1**

**role login -name co -password** <password>

**partition contents**

You should see the same number of objects that existed on the 5.x/6.x HSM. You can now decommission the old 5.x/6.x HSM.

## Cloning Using an HA Group

High Availability (HA) groups duplicate key material between the HSMs in the group. This function can be used to copy all cryptographic key material from a 5.x/6.x Network HSM partition to a new 7.x Network HSM partition.

The new configuration's operating system must be compatible with both the new 7.x and the old 5.x/6.x hardware. Consult the 5.x/6.x CRN for a list of compatible operating systems.

To clone cryptographic keys from one HSM to another, the HSMs must share the same cloning domain. For password-authenticated HSMs, this domain should have been specified when the partition was initialized. For PED-authenticated HSMs, the red key determines the cloning domain. You will need the same red key that was imprinted during 5.x/6.x partition creation to initialize the 7.x partition (see ["Initializing an Application Partition" on page 268](#)).

The 7.x client software should be installed, and the connection to both the source and destination HSM partitions verified, before attempting this procedure (see ["Luna HSM Client Software Installation" on page 17](#) for details). The source and destination partitions must both be assigned to the client machine issuing the cloning commands (see ["Client-Partition Connections" on page 86](#) for details). Use **slot list** to ensure both partitions are visible to the client.

**NOTE** It is not recommended to maintain an HA group with different versions of the Luna Network HSM hardware.

### Preconditions

The following instructions assume that:

- > the 7.x client software has been installed
- > an uninitialized partition has been created on the 7.x Network HSM
- > the source and destination partitions are both registered with the client (visible)

In the following examples:

- > Slot 0 = the source 5.x/6.x partition
- > Slot 1 = the destination 7.x partition

**NOTE** Partition login name requirements have changed between hardware versions. With release 7.x, you can log in using the abbreviated **po** (Partition Security Officer) or **co** (Crypto Officer).

### To clone cryptographic keys from a 5.x/6.x partition to a 7.x partition using an HA group

Follow these steps to copy cryptographic material from an 5.x/6.x partition to a new 7.x partition by creating an HA group that includes both partitions.

1. Run LunaCM, set the current slot to the SA7 partition, and initialize the Partition SO role.

**slot set -slot 1**

**partition init -label <7.x\_partition\_label>**

- a. If you are cloning a multi-factor-authenticated (PED-authenticated) 5.x/6.x partition, use the 5.x/6.x partition's red key when prompted.

- b. If you are cloning a password-authenticated 5.x/6.x partition, enter the same cloning domain when prompted.
2. Log in as the **po** (Partition Security Officer) and initialize the **co** (Crypto Officer) role.

**role login -name po**

**role init -name co**

If you are cloning a multi-factor-authenticated (PED-authenticated) 5.x/6.x partition, create a challenge secret for the Crypto Officer. This is required to set an HA activation policy.

**role createchallenge -name co -challengesecret <password>**

3. Set the current slot to the source 5.x/6.x slot, log in as the Crypto Officer.

**slot set -slot 0**

**NOTE** Be mindful of whether you're working with pre-PPSO or PPSO firmware and use the **partition login** or **role login** commands as specified below. Also, with PPSO firmware 6.22.0 and up, be careful with user names, i.e., type **Crypto Officer** in full (is case sensitive) and not **co**.

- a. If you are cloning a release 5.x or 6.x pre-PPSO partition (up to and including Firmware 6.21.2), use:
    - partition login**
  - b. If you are cloning a release 6.x PPSO partition (Firmware 6.22.0 and up), use:
    - role login -name Crypto Officer**
4. Optional: To verify the objects in the 5.x/6.x partition to be cloned, use:
    - partition contents**
  5. Using LunaCM, create an HA group of the 5.x/6.x slot and the 7.x slot.

**NOTE** HA requires that all members have an activation policy set. See ["Activation and Auto-activation on Multi-factor- \(PED-\) Authenticated Partitions"](#) on page 299 for details.

- a. Via LunaSH, log in as Security Officer and set policy 22 on the 5.x/6.x partition:
  - partition changepolicy -partition <5.x\_partition\_label> -policy 22 -value 1**
- b. In LunaCM, log in to the 7.x partition as Partition Security Officer, and set the activation policy from the client machine:
  - slot set -slot 1**
  - role login -name po**
  - partition changepolicy -policy 22 -value 1**
- c. Create the HA group with the 5.x/6.x partition as the primary partition. Select the "copy" option to preserve objects.
  - hagroup creategroup -label <group\_label> -slot 0 -password <password>**
- d. Add the 7.x partition slot to the HA group. Repeat this step to add multiple 7.x partitions to the group.
  - hagroup addmember -group <group\_label> -slot 1 -password <password>**

6. Synchronize the group to clone the objects to the 7.x member(s).

**hagroup synchronize -group** <group\_label> **-password** <password>

7. Check synchronization status of the group.

**hagroup listgroups**

Notice the entry "Needs sync: no". This means that the objects have been successfully cloned among all members of the HA group. You can also log in to the 7.x slot as the Crypto Officer and check the partition contents.

## Luna USB HSM (5.x or 6.x) to Luna Network HSM (7.x)

This chapter describes how to migrate your key material from a release 5.x or 6.x Luna USB HSM partition to a release 7.x Luna Network HSM partition. You can migrate your key material using one of the following methods:

- > ["Backup and Restore" below](#)
- > ["Cloning" on page 320](#)

### Backup and Restore

Cryptographic key material can be backed up from a release 5.x or 6.x Luna USB HSM partition and then restored to a release 7.x Luna Network HSM partition using a Luna Backup HSM. The following procedure performs a backup of a 5.x/6.x partition on an older operating system to a Luna Backup HSM. The Backup HSM is then moved to a newer operating system where the 5.x/6.x key material is restored to a 7.x partition.

Consult the 5.x/6.x/7.x CRN for a list of compatible operating systems.

To clone cryptographic keys from one HSM to another, the HSMs must share the same cloning domain. For password-authenticated HSMs, this domain should have been specified when the 5.x/6.x partition was initialized. For PED-authenticated HSMs, the red key determines the cloning domain. You will need the same red key that was imprinted during 5.x/6.x partition creation to initialize the 7.x partition (see ["Initializing an Application Partition" on page 268](#)).

HSM Client software must be installed before attempting this procedure (see ["Luna HSM Client Software Installation" on page 17](#) for details). The source and destination partitions must be assigned to the client machine issuing the backup or restore command (see ["Client-Partition Connections" on page 86](#) for details). Use **slot list** to ensure both partitions are visible to the client.

### Preconditions

On the older operating system, the following instructions assume that:

- > 5.x/6.x HSM Client Software is installed
- > the source 5.x/6.x partition is visible
- > the source partition's security policy allows cloning of private and secret keys
- > the destination Backup HSM partition is visible

On the new operating system, the following instructions assume that:

- > 7.x HSM Client Software is installed

- > you have created an uninitialized partition on the 7.x Network HSM
- > the destination 7.x partition is registered with the client software (visible)
- > the source Backup HSM partition's security policy allows cloning of private and secret keys

Slots used in the following instructions:

On the older operating system running 5.x/6.x client software:

- Slot 0: the source 5.x/6.x partition
- Slot 2: the destination Luna Backup HSM partition

On the new operating system running 7.x client software:

- Slot 1: the destination 7.x partition
- Slot 2: the source Luna Backup HSM partition (with the backup of the 5.x/6.x partition)

**NOTE** Partition login name requirements have changed with the hardware versions. With release 7.x, you can log in using the abbreviated **PO** (Partition Security Officer) or **CO** (Crypto Officer).

## To backup/restore cryptographic keys from a 5.x/6.x partition to a 7.x partition using a Backup HSM

Follow these steps to back up all cryptographic material on a 5.x/6.x partition to a Luna Backup HSM, and restore to a new 7.x partition.

1. On the old operating system running 5.x/6.x client software, run LunaCM and set the current slot to the 5.x/6.x partition.

**slot list**

**slot set -slot 0**

2. Log in as the Crypto Officer.

**NOTE** Be mindful of whether you're working with pre-PPSO or PPSO firmware and use the "partition login" or "role login" commands as specified below. Also, with PPSO firmware 6.22.0 and up, be careful with user names, i.e., type "Crypto Officer" in full (is case sensitive) and not "co".

- a. If you are backing up a release 5.x or 6.x pre-PPSO partition (up to and including Firmware 6.21.2), use:
  - partition login**
- b. If you are backing up a release 6.x PPSO partition (Firmware 6.22.0 and up), use:
  - role login -name Crypto Officer**
3. Optional: To verify the objects in the 5.x/6.x partition to be backed up, use:
  - partition contents**
4. Back up the 5.x/6.x partition contents to the Luna Backup HSM.
  - partition archive backup -slot 2 -partition <backup\_label>**

- a. If you are backing up a PED-authenticated 5.x/6.x partition, use the 5.x/6.x partition's red key when prompted.
- b. If you are backing up a password-authenticated 5.x/6.x partition, enter the same cloning domain when prompted.

Optionally, verify that all objects were backed up successfully on the Luna Backup HSM by issuing the **partition contents** command.

5. Move the Luna Backup HSM (with the backup of the 5.x/6.x partition) to the new operating system running the 7.x client software, and make sure it is visible to the client along with the 7.x HSM.
6. On the new operating system running the 7.x client software, run LunaCM, set the current slot to the 7.x partition, and initialize the partition and the PPSO role.

#### **slot set -slot 1**

**partition init -label** <7.x\_partition\_label>

- a. If you are backing up a PED-authenticated 5.x/6.x partition, use the 5.x/6.x partition's red key when prompted.
  - b. If you are backing up a password-authenticated 5.x/6.x partition, enter the same cloning domain when prompted.
7. Log in as the **po** (Partition Security Officer) and initialize the **co** (Crypto Officer) role.

**role login -name po**

**role init -name co**

If you are backing up a PED-authenticated 5.x/6.x partition, you can create an optional challenge secret for the Crypto Officer.

**role createchallenge -name co -challengesecret** <password>

8. Set the current slot to the 7.x partition, log in as the Crypto Officer, and restore from backup.

**slot set -slot 1**

**role login -name co**

**partition archive restore -slot 2 -partition** <backup\_label>

Afterwards, you can verify the partition contents on the 7.x partition:

**partition contents**

## Cloning

The simplest method of migrating key material to a new 7.x partition is slot-to-slot cloning. This procedure copies all permitted cryptographic material from a 5.x/6.x USB HSM partition to a 7.x Network HSM partition.

The new configuration's operating system must be compatible with both the new 7.x and the old 5.x/6.x hardware. Consult the 5.x/6.x CRN for a list of compatible operating systems.

To clone cryptographic keys from one HSM to another, the HSMs must share the same cloning domain. For password-authenticated HSMs, this domain should have been specified when the partition was initialized. For PED-authenticated HSMs, the red key determines the cloning domain. You will need the same red key that was imprinted during 5.x/6.x partition creation to initialize the 7.x partition (see ["Initializing an Application Partition" on page 268](#)).



The 7.x client software should be installed, and the connection to both the source and destination partitions verified, before attempting this procedure (see "[Luna HSM Client Software Installation](#)" on page 17 for details). The source and destination partitions must both be assigned to the client machine issuing the cloning commands (see "[Client-Partition Connections](#)" on page 86 for details). Use **slot list** to ensure both partitions are visible to the client.

If the source partition contains asymmetric keys, its security policy must allow cloning of private and secret keys. Use `lunacm:> partition showpolicies` to ensure that your source partition's security template allows this. If the 5.x/6.x HSM's security template does not allow cloning of private/secret keys, the HSM Admin may be able to turn this feature on using `lunacm:> partition changepolicy`.

**CAUTION!** Check your source partition policies and adjust them to be sure you can clone private and symmetric keys. Depending on the configuration of your partition and HSM, these policies may be destructive.

### Preconditions

The following instructions assume that:

- > the 7.x client software has been installed
- > an uninitialized partition has been created on the 7.x Network HSM
- > the destination 7.x partition must be registered with the client (visible)
- > the source 5.x/6.x partition's security policy allows cloning of private and secret keys

In the following examples:

- > Slot 0: the source 5.x/6.x partition
- > Slot 1: the destination 7.x partition

**NOTE** Partition login name requirements have changed with the hardware versions. With release 7.x, you can log in using the abbreviated **PO** (Partition Security Officer) or **CO** (Crypto Officer).

### To clone cryptographic keys from a 5.x/6.x partition to a 7.x partition

Follow these steps to clone all cryptographic material on a 5.x/6.x partition to a 7.x partition.

1. Run LunaCM, set the current slot to the 7.x partition, and initialize the Partition SO role.

**slot list**

**slot set -slot 1**

**partition init -label** <7.x\_partition\_label>

- a. If you are cloning a PED-authenticated 5.x/6.x partition, use the 5.x/6.x partition's red key when prompted.
- b. If you are cloning a password-authenticated 5.x/6.x partition, enter the same cloning domain when prompted.

2. Log in as the **po** (Partition Security Officer) and initialize the **co** (Crypto Officer) role.

**role login -name po**

**role init -name co**

If you are cloning a PED-authenticated 5.x/6.x partition, you can create an optional challenge secret for the Crypto Officer.

**role createchallenge -name co -challengesecret <password>**

3. Set the current slot to the source 5.x/6.x slot, log in as the Crypto Officer.

**slot set -slot 0**

**NOTE** Be mindful of whether you're working with pre-PPSO or PPSO firmware and use the "partition login" or "role login" commands as specified below. Also, with PPSO firmware 6.22.0 and up, be careful with user names, i.e., type "Crypto Officer" in full (is case sensitive) and not "co".

- a. If you are cloning a release 5.x or 6.x pre-PPSO partition (up to and including Firmware 6.21.2), use:

**partition login**

- b. If you are cloning a release 6.x PPSO partition (Firmware 6.22.0 and up), use:

**role login -name Crypto Officer**

4. Optional: To verify the objects in the 5.x/6.x partition to be cloned, issue the "partition contents" command.

**partition contents**

5. Clone the objects to the 7.x partition slot (see ["partition clone" on page 1](#) for correct syntax).

**partition clone -objects 0 -slot 1**

Afterward, you can set the current slot to the 7.x partition and verify that all objects have cloned successfully.

**slot set -slot 1**

**role login -name co -password <password>**

**partition contents**

You should see the same number of objects that existed on the 5.x/6.x HSM. You can now decommission the old 5.x/6.x HSM.

## Luna PCIe HSM (5.x or 6.x) to Luna Network HSM (7.x)

This chapter describes how to migrate your key material from a release 5.x or 6.x Luna PCIe HSM partition to a release 7.x Luna Network HSM partition. You can migrate your key material using one of the following methods:

- > ["Backup and Restore" on the next page](#)
- > ["Cloning" on page 325](#)

## Backup and Restore

Cryptographic key material can be backed up from a release 5.x or 6.Luna PCIe HSM partition and then restored to a release 7.x Luna Network HSM partition using a Luna Backup HSM. The following procedure performs a backup of a 5.x/6.x partition on an older operating system to a Luna Backup HSM. The Backup HSM is then moved to a newer operating system where the 5.x/6.x key material is restored to a 7.x partition.

Consult the 5.x/6.x/7.x CRN for a list of compatible operating systems.

To clone cryptographic keys from one HSM to another, the HSMs must share the same cloning domain. For password-authenticated HSMs, this domain should have been specified when the 5.x/6.x partition was initialized. For PED-authenticated HSMs, the red key determines the cloning domain. You will need the same red key that was imprinted during 5.x/6.x partition creation to initialize the 7.x partition (see ["Initializing an Application Partition" on page 268](#)).

HSM Client software must be installed on both operating systems (older and new) before attempting this procedure (see ["Luna HSM Client Software Installation" on page 17](#) for details). The destination partition must be assigned to the client machine (see ["Client-Partition Connections" on page 86](#) for details). Use **slot list** to ensure partitions are visible to the client.

### Preconditions

On the older operating system, the following instructions assume that:

- > 5.x/6.x HSM Client Software is installed with "Luna Backup HSM" option selected.
- > the source 5.x/6.x partition is visible
- > the source partition's security policy allows cloning of private and secret keys
- > the destination Backup HSM partition is visible

On the new operating system, the following instructions assume that:

- > 7.x HSM Client Software is installed with "Luna Backup HSM" option selected.
- > you have created an uninitialized partition on the 7.x Network HSM
- > the destination 7.x partition is registered with the client software (visible)
- > the source Backup HSM partition's security policy allows cloning of private and secret keys

Slots used in the following instructions:

On the older operating system running 5.x/6.x client software:

- Slot 0: the source 5.x/6.x partition
- Slot 2: the destination Luna Backup HSM partition

On the new operating system running 7.x client software:

- Slot 1: the destination 7.x partition
- Slot 2: the source Backup HSM partition (with the backup of the 5.x/6.x partition)

**NOTE** Partition login name requirements have changed with the hardware versions. With release 7.x, you can log in using the abbreviated **po** (Partition Security Officer) or **co** (Crypto Officer).

## To backup/restore cryptographic keys from a 5.x/6.x partition to a 7.x partition using a Backup HSM

Follow these steps to back up all cryptographic material on a 5.x/6.x partition to a Luna Backup HSM, and restore to a new 7.x partition.

1. On the old operating system running 5.x/6.x client software, run LunaCM and set the current slot to the 5.x/6.x partition.

**slot list**

**slot set -slot 0**

2. Log in as the Crypto Officer.

**NOTE** Be mindful of whether you're working with pre-PPSO or PPSO firmware and use the "partition login" or "role login" commands as specified below. Also, with PPSO firmware 6.22.0 and up, be careful with user names, i.e., type "Crypto Officer" in full (is case sensitive) and not "co".

- a. If you are backing up a release 5.x or 6.x pre-PPSO partition (up to and including Firmware 6.21.2), use:

**partition login**

- b. If you are backing up a release 6.x PPSO partition (Firmware 6.22.0 and up), use:

**role login -name Crypto Officer**

3. Optional: To verify the objects in the 5.x/6.x partition to be backed up, use:

**partition contents**

4. Back up the 5.x/6.x partition contents to the Luna Backup HSM.

**partition archive backup -slot 2 -partition <backup\_label>**

- a. If you are backing up a PED-authenticated 5.x/6.x partition, use the 5.x/6.x partition's red key when prompted.
- b. If you are backing up a password-authenticated 5.x/6.x partition, enter the same cloning domain when prompted.

Optionally, verify that all objects were backed up successfully on the Luna Backup HSM by issuing the **partition contents** command.

5. Move the Luna Backup HSM (with the backup of the 5.x/6.x partition) to the new operating system running the 7.x client software, and make sure it is visible to the client along with the 7.x HSM.
6. On the new operating system running the 7.x client software, run LunaCM, set the current slot to the 7.x partition, and initialize the partition and the PPSO role.

**slot set -slot 1**

**partition init -label <7.x\_partition\_label>**

- a. If you are backing up a PED-authenticated 5.x/6.x partition, use the 5.x/6.x partition's red key when prompted.
- b. If you are backing up a password-authenticated 5.x/6.x partition, enter the same cloning domain when prompted.

7. Log in as the **po** (Partition Security Officer) and initialize the **co** (Crypto Officer) role.

**role login -name po**

**role init -name co**

If you are backing up a PED-authenticated 5.x/6.x partition, you can create an optional challenge secret for the Crypto Officer.

**role createchallenge -name co -challengesecret <password>**

8. Set the current slot to the 7.x partition, log in as the Crypto Officer, and restore from backup.

**slot set -slot 1**

**role login -name co**

**partition archive restore -slot 2 -partition <backup\_label>**

Afterwards, you can verify the partition contents on the 7.x partition:

**partition contents**

## Cloning

The simplest method of migrating key material to a new 7.x partition is slot-to-slot cloning. This procedure copies all permitted cryptographic material from a 5.x/6.x PCIe HSM partition to a 7.x Network HSM partition.

The new configuration's operating system must be compatible with both the new 7.x and the old 5.x/6.x hardware. Consult the 5.x/6.x CRN for a list of compatible operating systems.

To clone cryptographic keys from one HSM to another, the HSMs must share the same cloning domain. For password-authenticated HSMs, this domain should have been specified when the partition was initialized. For PED-authenticated HSMs, the red key determines the cloning domain. You will need the same red key that was imprinted during 5.x/6.x partition creation to initialize the 7.x partition (see ["Initializing an Application Partition" on page 268](#)).

The 7.x client software should be installed, and the connection to both the source and destination partitions verified, before attempting this procedure (see ["Luna HSM Client Software Installation" on page 17](#) for details). The destination partition must be assigned to the client machine issuing the cloning commands (see ["Client-Partition Connections" on page 86](#) for details). Use the **slot list** command to ensure both partitions are visible to the client.

If the source partition contains asymmetric keys, its security policy must allow cloning of private and secret keys. Use the command **partition showpolicies** in LunaCM to ensure that your source partition's security template allows this (see ["partition showpolicies" on page 1](#)). If the 5.x/6.x HSM's security template does not allow cloning of private/secret keys, the HSM Admin may be able to turn this feature on using **partition changepolicy** (see ["partition changepolicy" on page 1](#)).

If the source partition contains asymmetric keys, its security policy must allow cloning of private and secret keys. Use `lunacm:> partition showpolicies` to ensure that your source partition's security template allows this. If the 5.x/6.x HSM's security template does not allow cloning of private/secret keys, the HSM Admin may be able to turn this feature on using `lunacm:> partition changepolicy`.

**CAUTION!** Check your source partition policies and adjust them to be sure you can clone private and symmetric keys. Depending on the configuration of your partition and HSM, these policies may be destructive.

### Preconditions

On the operating system running 5.x/6.x client software, verify:

- > that the 5.x/6.x PCIe HSM partition's security policy allows cloning of private and secret keys
- > all key material on the 5.x/6.x PCIe HSM partition to be cloned

Regarding the operating system running 7.x client software, the following instructions assume that:

- > the 7.x client software has been installed with "Luna PCIe HSM" option selected.
- > an uninitialized partition has been created on the 7.x HSM
- > the destination 7.x HSM partition must be registered with the client (visible)
- > the Luna PCIe HSM card (with 5.x/6.x key material) has been installed

Slots used in the following instructions:

- > Slot 0: the source 5.x/6.x Luna PCIe HSM partition
- > Slot 1: the destination 7.x partition

**NOTE** Partition login name requirements have changed with the hardware versions. With release 7.x, you can log in using the abbreviated **po** (Partition Security Officer) or **co** (Crypto Officer).

### To clone cryptographic keys from a 5.x/6.x partition to a 7.x partition

Follow these steps to clone all cryptographic material on a 5.x/6.x partition to a 7.x partition.

1. Run LunaCM, set the current slot to the 7.x partition, and initialize the Partition SO role.

**slot list**

**slot set -slot 1**

**partition init -label <7.x\_partition\_label>**

- a. If you are cloning a PED-authenticated 5.x/6.x partition, use the 5.x/6.x partition's red key when prompted.
- b. If you are cloning a password-authenticated 5.x/6.x partition, enter the same cloning domain when prompted.

2. Log in as the **po** (Partition Security Officer) and initialize the **co** (Crypto Officer) role.

**role login -name po**

**role init -name co**

If you are cloning a PED-authenticated 5.x/6.x partition, you can create an optional challenge secret for the Crypto Officer.

**role createchallenge -name co -challengesecret <password>**

3. Set the current slot to the source 5.x/6.x slot, log in as the Crypto Officer.

**slot set -slot 0**

**NOTE** Be mindful of whether you're working with pre-PPSO or PPSO firmware and use the "partition login" or "role login" commands as specified below. Also, with PPSO firmware 6.22.0 and up, be careful with user names, i.e., type "Crypto Officer" in full (is case sensitive) and not "co".

- a. If you are cloning a release 5.x or 6.x pre-PPSO partition (up to and including Firmware 6.21.2), use:  
**partition login**
- b. If you are cloning a release 6.x PPSO partition (Firmware 6.22.0 and up) , use:  
**role login -name Crypto Officer**
4. Optional: To verify the objects in the 5.x/6.x partition to be cloned, issue the "partition contents" command.  
**partition contents**
5. Clone the objects to the 7.x partition slot (see ["partition clone" on page 1](#) for correct syntax).  
**partition clone -objects 0 -slot 1**

Afterward, you can set the current slot to the 7.x partition and verify that all objects have cloned successfully.

**slot set -slot 1**

**role login -name co -password <password>**

**partition contents**

You should see the same number of objects that existed on the 5.x/6.x HSM. You can now decommission the old 5.x/6.x HSM.

## Luna PCIe HSM or Luna USB HSM (5.x or 6.x) to Luna PCIe HSM (7.x)

This chapter describes how to migrate your key material from release 5.x or 6.x of the Luna PCIe HSM or Luna USB HSM partition to release 7.x of the Luna PCIe HSM partition. You can migrate your key material using one of the following three methods:

- > ["Backup and Restore" below](#)
- > ["Cloning" on page 330](#)
- > ["Cloning Using an HA Group" on page 332](#)

### Backup and Restore

Cryptographic key material can be backed up and then restored to a release 7.x Luna PCIe HSM partition using a Luna Backup HSM.

The new configuration's operating system must be compatible with both the new 7.x and the old 5.x/6.x hardware. Consult the 5.x/6.x CRN for a list of compatible operating systems.

To backup and restore cryptographic keys from one HSM to another, the HSMs must share the same cloning domain. For password-authenticated HSMs, this domain should have been specified when the partition was initialized. For PED-authenticated HSMs, the red key determines the cloning domain. You will need the same red key that was imprinted during 5.x/6.x partition creation to initialize the 7.x partition (see ["Initializing an Application Partition" on page 268](#)).

The 7.x client software should be installed, and the connection to both the source and destination partitions verified, before attempting this procedure (see ["Luna HSM Client Software Installation" on page 17](#) for details). The source and destination partitions must both be assigned to the client machine issuing the cloning commands (see ["Client-Partition Connections" on page 86](#) for details). Use **slot list** to ensure both partitions are visible to the client.

### Preconditions

The following instructions assume that:

- > the 10.x client software has been installed
- > an uninitialized partition has been created on the 7.x HSM
- > the source and destination partitions are both registered with the client (visible)
- > the source partition's security policy allows cloning of private and secret keys

In the following example:

- > Slot 0: the source 5.x/6.x partition
- > Slot 1: the destination 7.x partition
- > Slot 2: the Backup HSM partition

**NOTE** Partition login name requirements have changed with the hardware versions. With release 7.x, you can log in using the abbreviated **po** (Partition Security Officer) or **co** (Crypto Officer).

### To migrate cryptographic keys from a 5.x/6.x partition to a 7.x partition using a Backup HSM

Follow these steps to back up all cryptographic material on a 5.x/6.x partition to a Backup HSM, and restore to a new 7.x partition.

1. Run LunaCM, set the current slot to the 7.x partition, and initialize the partition and the Partition SO role.

**slot set -slot 0**

**partition init -label <7.x\_partition\_label>**

- a. If you are backing up a PED-authenticated 5.x/6.x partition, use the 5.x/6.x partition's red key when prompted.
- b. If you are backing up a password-authenticated 5.x/6.x partition, enter the same cloning domain when prompted.

2. Log in as the **po** (Partition Security Officer) and initialize the **co** (Crypto Officer) role.

**role login -name po**

**role init -name co**



If you are backing up a PED-authenticated 5.x/6.x partition, you can create an optional challenge secret for the Crypto Officer.

**role createchallenge -name co -challengeSecret <password>**

3. Connect your backup HSM and make sure it is visible to the client, along with the 5.x/6.x and 7.x HSMs.
4. Set the current slot to the source 5.x/6.x slot.

**slot list**

**slot set -slot 0**

5. Log in as the Crypto Officer.

**NOTE** Be mindful of whether you're working with pre-PPSO or PPSO firmware and use the **partition login** or **role login** commands as specified below. Also, with PPSO firmware 6.22.0 and up, be careful with user names, i.e., type **Crypto Officer** in full (is case sensitive) and not **co**.

- a. If you are cloning a release 5.x or 6.x pre-PPSO partition (up to and including Firmware 6.21.2), use:
 

**partition login**
  - b. If you are cloning a release 6.x PPSO partition (Firmware 6.22.0 and up), use:
 

**role login -name Crypto Officer**
6. Optional: To verify the objects in the 5.x/6.x partition to be cloned, issue the "partition contents" command.
 

**partition contents**
  7. Back up the 5.x/6.x partition contents to the Backup HSM.
 

**partition archive backup -slot 2 -partition <backup\_label>**

    - a. If you are backing up a PED-authenticated 5.x/6.x partition, use the 5.x/6.x partition's red key when prompted.
    - b. If you are backing up a password-authenticated 5.x/6.x partition, enter the same cloning domain when prompted.

Optionally, verify that all objects were backed up successfully on the Backup HSM by checking the partition contents.

8. Set the current slot to the 7.x partition, log in as the Crypto Officer, and restore from backup.

**slot set -slot 1**

**role login -name co**

**partition archive restore -slot 2 -partition <backup\_label>**

Afterwards, you can verify the partition contents on the 7.x partition:

**partition contents**

## Cloning

The simplest method of migrating key material to a new 7.x partition is slot-to-slot cloning. This procedure copies all permitted cryptographic material from a 5.x/6.x PCIe or USB HSM partition to a 7.x PCIe HSM partition.

The new configuration's operating system must be compatible with both the new 7.x and the old 5.x/6.x hardware. Consult the 5.x/6.x CRN for a list of compatible operating systems.

To clone cryptographic keys from one HSM to another, the HSMs must share the same cloning domain. For password-authenticated HSMs, this domain should have been specified when the partition was initialized. For PED-authenticated HSMs, the red key determines the cloning domain. You will need the same red key that was imprinted during 5.x/6.x partition creation to initialize the 7.x partition (see ["Initializing an Application Partition" on page 268](#)).

The 7.x client software should be installed, and the connection to both the source and destination partitions verified, before attempting this procedure (see ["Luna HSM Client Software Installation" on page 17](#) for details). The source and destination partitions must both be assigned to the client machine issuing the cloning commands (see ["Client-Partition Connections" on page 86](#) for details). Use **slot list** to ensure both partitions are visible to the client.

If the source partition contains asymmetric keys, its security policy must allow cloning of private and secret keys. Use `lunacm:> partition showpolicies` to ensure that your source partition's security template allows this. If the 5.x/6.x HSM's security template does not allow cloning of private/secret keys, the HSM Admin may be able to turn this feature on using `lunacm:> partition changepolicy`.

**CAUTION!** Check your source partition policies and adjust them to be sure you can clone private and symmetric keys. Depending on the configuration of your partition and HSM, these policies may be destructive.

### Preconditions

The following instructions assume that:

- > the 7.x client software has been installed
- > an uninitialized partition has been created on the 7.x Network HSM
- > the destination 7.x partition must be registered with the client (visible)
- > the source 5.x/6.x partition's security policy allows cloning of private and secret keys

In the following examples:

- > Slot 0: the source 5.x/6.x partition
- > Slot 1: the destination 7.x partition

**NOTE** Partition login name requirements have changed with the hardware versions. With release 7.x, you can log in using the abbreviated **PO** (Partition Security Officer) or **CO** (Crypto Officer).

### To clone cryptographic keys from a 5.x/6.x partition to a 7.x partition

Follow these steps to clone all cryptographic material on a 5.x/6.x partition to a 7.x partition.

1. Run LunaCM, set the current slot to the 7.x partition, and initialize the Partition SO role.

**slot list**

**slot set -slot 1**

**partition init -label <7.x\_partition\_label>**

- a. If you are cloning a PED-authenticated 5.x/6.x partition, use the 5.x/6.x partition's red key when prompted.
  - b. If you are cloning a password-authenticated 5.x/6.x partition, enter the same cloning domain when prompted.
2. Log in as the **po** (Partition Security Officer) and initialize the **co** (Crypto Officer) role.

**role login -name po**

**role init -name co**

If you are cloning a PED-authenticated 5.x/6.x partition, you can create an optional challenge secret for the Crypto Officer.

**role createchallenge -name co -challengesecret <password>**

3. Set the current slot to the source 5.x/6.x slot, log in as the Crypto Officer.

**slot set -slot 0**

**NOTE** Be mindful of whether you're working with pre-PPSO or PPSO firmware and use the "partition login" or "role login" commands as specified below. Also, with PPSO firmware 6.22.0 and up, be careful with user names, i.e., type "Crypto Officer" in full (is case sensitive) and not "co".

- a. If you are cloning a release 5.x or 6.x pre-PPSO partition (up to and including Firmware 6.21.2), use:
 

**partition login**
  - b. If you are cloning a release 6.x PPSO partition (Firmware 6.22.0 and up), use:
 

**role login -name Crypto Officer**
4. Optional: To verify the objects in the 5.x/6.x partition to be cloned, issue the "partition contents" command.
 

**partition contents**
  5. Clone the objects to the 7.x partition slot (see ["partition clone" on page 1](#) for correct syntax).

**partition clone -objects 0 -slot 1**

Afterward, you can set the current slot to the 7.x partition and verify that all objects have cloned successfully.

**slot set -slot 1**

**role login -name co -password <password>**

**partition contents**

You should see the same number of objects that existed on the 5.x/6.x HSM. You can now decommission the old 5.x/6.x HSM.

## Cloning Using an HA Group

High Availability (HA) groups duplicate key material between the HSMs in the group. This function can be used to copy all cryptographic key material from a 5.x/6.x PCIe or USB HSM partition to a new 7.x PCIe HSM partition.

The new configuration's operating system must be compatible with both the new 7.x and the old 5.x/6.x hardware. Consult the 5.x/6.x CRN for a list of compatible operating systems.

To clone cryptographic keys from one HSM to another, the HSMs must share the same cloning domain. For password-authenticated HSMs, this domain should have been specified when the partition was initialized. For PED-authenticated HSMs, the red key determines the cloning domain. You will need the same red key that was imprinted during 5.x/6.x partition creation to initialize the 7.x partition (see ["Initializing an Application Partition" on page 268](#)).

The 7.x client software should be installed, and the connection to both the source and destination HSM partitions verified, before attempting this procedure (see ["Luna HSM Client Software Installation" on page 17](#) for details). The source and destination partitions must both be assigned to the client machine issuing the cloning commands (see ["Client-Partition Connections" on page 86](#) for details). Use **slot list** to ensure both partitions are visible to the client.

**NOTE** It is not recommended to maintain an HA group with different versions of the Luna Network HSM hardware.

### Preconditions

The following instructions assume that:

- > the 7.x client software has been installed
- > an uninitialized partition has been created on the 7.x Network HSM
- > the source and destination partitions are both registered with the client (visible)

In the following examples:

- > Slot 0 = the source 5.x/6.x partition
- > Slot 1 = the destination 7.x partition

**NOTE** Partition login name requirements have changed between hardware versions. With release 7.x, you can log in using the abbreviated **po** (Partition Security Officer) or **co** (Crypto Officer).

### To clone cryptographic keys from a 5.x/6.x partition to a 7.x partition using an HA group

Follow these steps to copy cryptographic material from an 5.x/6.x partition to a new 7.x partition by creating an HA group that includes both partitions.

1. Run LunaCM, set the current slot to the SA7 partition, and initialize the Partition SO role.

**slot set -slot 1**

**partition init -label <7.x\_partition\_label>**

- a. If you are cloning a multi-factor-authenticated (PED-authenticated) 5.x/6.x partition, use the 5.x/6.x partition's red key when prompted.
  - b. If you are cloning a password-authenticated 5.x/6.x partition, enter the same cloning domain when prompted.
2. Log in as the **po** (Partition Security Officer) and initialize the **co** (Crypto Officer) role.

**role login -name po**

**role init -name co**

If you are cloning a multi-factor-authenticated (PED-authenticated) 5.x/6.x partition, create a challenge secret for the Crypto Officer. This is required to set an HA activation policy.

**role createchallenge -name co -challengesecret <password>**

3. Set the current slot to the source 5.x/6.x slot, log in as the Crypto Officer.

**slot set -slot 0**

**NOTE** Be mindful of whether you're working with pre-PPSO or PPSO firmware and use the **partition login** or **role login** commands as specified below. Also, with PPSO firmware 6.22.0 and up, be careful with user names, i.e., type **Crypto Officer** in full (is case sensitive) and not **co**.

- a. If you are cloning a release 5.x or 6.x pre-PPSO partition (up to and including Firmware 6.21.2), use:
 

**partition login**
  - b. If you are cloning a release 6.x PPSO partition (Firmware 6.22.0 and up) , use:
 

**role login -name Crypto Officer**
4. Optional: To verify the objects in the 5.x/6.x partition to be cloned, use:
- partition contents**
5. Using LunaCM, create an HA group of the 5.x/6.x slot and the 7.x slot.

**NOTE** HA requires that all members have an activation policy set. See "[Activation and Auto-activation on Multi-factor- \(PED-\) Authenticated Partitions](#)" on page 299 for details.

- a. Via LunaSH, log in as Security Officer and set policy 22 on the 5.x/6.x partition:
 

**partition changepolicy -partition <5.x\_partition\_label> -policy 22 -value 1**
- b. In LunaCM, log in to the 7.x partition as Partition Security Officer, and set the activation policy from the client machine:
 

**slot set -slot 1**

**role login -name po**

**partition changepolicy -policy 22 -value 1**
- c. Create the HA group with the 5.x/6.x partition as the primary partition. Select the "copy" option to preserve objects.
 

**hagroup creatigroup -label <group\_label> -slot 0 -password <password>**

- d. Add the 7.x partition slot to the HA group. Repeat this step to add multiple 7.x partitions to the group.

```
hagroup addmember -group <group_label> -slot 1 -password <password>
```

6. Synchronize the group to clone the objects to the 7.x member(s).

```
hagroup synchronize -group <group_label> -password <password>
```

7. Check synchronization status of the group.

```
hagroup listgroups
```

Notice the entry "Needs sync: no". This means that the objects have been successfully cloned among all members of the HA group. You can also log in to the 7.x slot as the Crypto Officer and check the partition contents.

## Moving from Pre-7.7.0 to Firmware 7.7.0 or Newer

One of the major changes at version 7.7.0 (or newer) and V1 partitions is PP 419-221.5 compliance and the addition of key object attributes that support Per-Key Authentication.

Any relevant key objects created in a V1 partition are automatically assigned CKA\_AUTH\_DATA attribute. However:

- > the default partition format at partition creation time, in firmware 7.7.0 (or newer) HSMs is V0, which does not immediately provide per-key authentication data or attributes;
- > V0 is also the partition version to which any pre-firmware-7.7.0 partitions are automatically converted when HSM firmware is updated to version 7.7;
- > V0 partitions can receive key objects from partitions on other HSMs (7.x-pre-7.7.0 HSMs, as well as 5.x and 6.x HSMs), and these come into the partition without auth data.

In a historic Luna HSM context, no auth data is needed, and non-visible auth-data (after firmware update or migration of keys) is irrelevant to the existing application or end user. The only noticeable changes, when remaining in the Luna context, for firmware 7.7.0 (or newer) partitions are:

- the increased size of objects to allow for authentication data, and
- the increased memory allotted to allow any objects that fit an earlier HSM/partition to likewise fit an updated partition.

In the eIDAS use case (such as Remote Signing and Sealing), specific authentication data is required, therefore an explicit call to CA\_SetAuthorizationData() should be made, for such key objects, so that keys can be assigned.

Various paths are possible to get existing objects from a partition on another HSM to a firmware 7.7.0 (or newer) partition.

**If you have no need for PP 419-221.5 or eIDAS compliance** or for SKS or PKA functionality, yet still have use for another aspect of firmware 7.7.0 (or newer), then

- > existing 7.x HSMs can have their firmware updated, and existing partitions become V0 partitions with all that implies  
(see ["What are 'pre-firmware 7.7.0', and V0, and V1 partitions?" on page 126](#))

- > key objects on existing 6.x and 5.x HSM partitions can be transferred to partitions on 7.x HSMs at pre-7.7.0 firmware

**NOTE** If you are attempting to migrate an SKS Master Key (SMK) from a 5.x or 6.x partition to Luna 7.7.0+ via a backup/restore procedure, Thales recommends one of the following:

- > Back up your SMK(s) to a Luna Backup HSM (G5) with firmware 6.25.0 to 6.25.9, to ensure compatibility with your older (6.x) client version.
- > If you have already updated the Backup HSM to a firmware version newer than 6.25.9, update Luna HSM Client to minimum version 10.3.0 before attempting the backup.

Once you have migrated your keys to Luna 7.7.0+ partitions, you require minimum Luna Backup HSM firmware 6.28.0 (G5) or 7.7.1 (G7) to do future backup/restore operations.

**If you do require PP 419-221.5 or eIDAS compliance**, then you will need to use V1 partitions on firmware 7.7.0 (or newer) HSMs.

Your objects from older partitions or HSMs can be:

- > already existing in a firmware 7.x (less than version 7.7) HSM that you update, causing the containing partition to become V0, and then you convert that partition, with your objects, to V1, or
- > imported from a pre-7.x HSM (5.x or 6.x) into a version zero (V0) partition on the firmware 7.7.0 (or newer) HSM, just as you would any object, and the V0 partition with the imported objects is then converted to a V1 partition (a one-way operation), or
- > cloned, unwrapped, or legacy-SKS-inserted, directly to a V1 partition (i.e., SIMinsert) - note that cloning in such case is a one-way operation; V1 partitions perform outbound cloning only for SMKs

### **Guidelines and Tips when partitions are part of an HA group**

Refer to ["General guidelines for updating or converting of HA member partitions" on page 376](#)

# CHAPTER 13: High-Availability Groups

Luna HSMs can provide scalability and redundancy for cryptographic applications that are critical to your organization. For applications that require continuous, uninterrupted uptime, the Luna HSM Client allows you to combine application partitions on multiple HSMs into a single logical group, known as a High-Availability (HA) group.

## High Availability Options for Luna HSMs

Luna HSMs support two, non-overlapping approaches to High Availability:

- > client-mediated HA creation and management of HA groups, by means of the LunaCM hagroup commands, with preparation, management, and usage described at ["High-Availability Groups" above](#) (this is believed to be the majority of HA implementations among Luna HSM customers)

versus

- > extensions to the PKCS#11 API to allow interested customers to create and maintain High Availability programmatically.

That is, if you want the redundancy and performance of High Availability,

- > you can do what many Luna HSM customers do and use LunaCM commands to declare and manage HA groups and their membership, while relying on the Luna Client library to carry out the day-to-day infrastructure and activity

or

- > you can program your own complete HA environment, in full, or tie into (integrate with) suitable COTS High Availability solutions that provide a suitable Application Interface, using HA Indirect Login calls to handle common authentication among HSM partitions in groups.

## Client-driven High Availability

This section is about the Client-driven HA feature, traditionally used by most Luna HSM customers. (To develop your own HA solution or integrate with a commercial one, see ["HA Indirect Login \(firmware 7.7.0 and newer\)" on page 1](#) instead.)

This feature is best suited to provide redundancy to the Network HSM and PCI-E HSM products. Network HSM partitions can be grouped with other Network HSM partitions or with a Luna Cloud HSM service. PCI-E HSM partitions can be grouped with other PCI-E HSM partitions or with a Luna Cloud HSM Service.

An HA group allows your client application to access cryptographic services as long as one member HSM is functional and network-connected. This allows you to perform maintenance on any individual member without ever pausing your application, and provides redundancy in the case of individual failures. Cryptographic requests are distributed across all active group members, enabling a performance gain for each member added. Cryptographic objects are replicated across the entire group, so HA can also be used to keep a current, automatic, remote backup of the group contents.



HA functionality is handled by the Luna HSM Client software. The individual partitions have no way to know they are configured in an HA group, so you can configure HA on a per-application basis. The way you group your HSMs depends on your circumstances and desired performance.

This chapter contains the following sections:

- > ["Planning Your HA Group Deployment" on page 346](#)
- > ["Setting Up an HA Group" on page 350](#)
- > ["Verifying an HA Group" on page 354](#)
- > ["Setting an HA Group Member to Standby" on page 356](#)
- > ["Configuring HA Auto-Recovery" on page 358](#)
- > ["Enabling/Disabling HA Only Mode" on page 358](#)
- > ["HA Logging" on page 359](#)
- > ["Adding/Removing an HA Group Member" on page 363](#)
- > ["Manually Recovering a Failed HA Group Member" on page 366](#)
- > ["Replacing an HA Group Member" on page 367](#)
- > ["Deleting an HA Group" on page 370](#)
- > ["Managing Your HA Groups" on page 1](#)
- > ["HA Troubleshooting" on page 370](#)
- > ["Updating Luna Network HSM HA Group Members to Luna 7.7.0 or Newer" on page 373](#)
- > ["General guidelines for updating or converting of HA member partitions" on page 376](#)

If you plan to create an HA group consisting of different kinds of Luna HSMs, refer also to:

- > ["Cloning Keys Between Luna 6, Luna 7, and Luna Cloud HSM" on page 171](#)

## Performance

For repetitive operations (for example, many signings using the same key), an HA group provides linear performance gains as group members are added. The best approach is to maintain an HA group at a size that best balances application server capability and the expected loads, with an additional unit providing capacity for bursts of traffic.

For best overall performance, keep all group members running near their individual performance ideal, about 30 simultaneous threads per HSM. If you assemble an HA group that is significantly larger than your server(s) can manage, you might not achieve full performance from all members. Gigabit Ethernet connections are recommended to maximize performance.

Performance is also affected by the kind of cryptographic operations being requested. For some operations, an HA group can actually hinder performance by requiring extra operations to replicate new key objects. For example, if the operation involves importing and unwrapping keys:

Using an HA group	Using an individual partition
<ol style="list-style-type: none"> <li>1. Encryption (to wrap the key)</li> <li>2. Decryption on the primary member partition (to unwrap the key)</li> <li>3. Object creation on the primary member partition (the unwrapped key is created and stored as a key object)</li> <li>4. Key replication across the HA group:               <ol style="list-style-type: none"> <li>a. RSA 4096-bit operation is used to derive a shared secret between HSMs</li> <li>b. Encryption of the key on the primary HA member using the shared secret</li> <li>c. Decryption of the key on each HA member using the shared secret</li> <li>d. Object creation on each HA member</li> </ol> </li> <li>5. Encryption (using the unwrapped key object to encrypt the data)</li> </ol>	<ol style="list-style-type: none"> <li>1. Encryption (to wrap the key)</li> <li>2. Decryption (to unwrap the key)</li> <li>3. Object creation (the unwrapped key is created and stored as a key object)</li> <li>4. Encryption (using the unwrapped key object to encrypt the data)</li> </ol>

In this case, the HA group must perform many more operations than an individual partition, most significantly the RSA-4096-bit operation and creating the additional objects. Those two operations are by far the most time-consuming on the list, and so this task would have much better performance on an individual partition.

The crucial HA performance consideration is whether the objects on the partitions are constant, or always being created and replaced. If tasks make use of already-existing objects, those objects exist on all HA group members; operations can be performed by different group members, boosting performance. If new objects are created, they must be replicated across the entire group, causing a performance loss.

**NOTE** The way your application uses the **C\_FindObjects** function to search for objects in a virtual HA slot can have a significant impact on your application performance (see ["Application Object Handles" on page 344](#)).

## Load Balancing

Cryptographic requests sent to the HA group's virtual slot are load-balanced across all active members of the HA group. The load-balancing algorithm sends requests for cryptographic operations to the least busy partition in the HA group. This scheme accounts for operations of variable length, ensuring that queues are balanced even when some partitions are assigned very long operations. When an application requests a repeated set of operations, this method works. When the pattern is interrupted, however, the request type becomes relevant, as follows:

- > Single-part (stateless) cryptographic operations are load-balanced.
- > Multi-part (stateful) cryptographic operations are load-balanced.
- > Multi-part (stateful) information retrieval requests are not load-balanced. In this case, the cost of distributing the requests to different HA group members is generally greater than the benefit. For this reason, multi-part information retrieval requests are all targeted at one member.

- > Key management requests are not load-balanced. Operations affecting the state of stored keys (creation, deletion) are performed on a single HA member, and the result is then replicated to the rest of the HA group.

For example, when a member partition is signing and an asymmetric key generation request is issued, additional operations on that member are queued while the partition generates the key. In this case, the algorithm schedules more operations on other partitions in the HA group.

The load-balancing algorithm operates independently in each application process. Multiple processes on the same client or on different clients do not share information when scheduling operations. Some mixed-use cases might cause applications to use some partitions more than others (see ["Planning Your HA Group Deployment" on page 346](#)). If you increase key sizes, interleave other cryptographic operations, or if network latency increases, performance may drop for individual active members as they become busier.

**NOTE** Partitions designated as standby members are not used to perform cryptographic operations, and are therefore not part of the load-balancing scheme (see ["Standby Members" on page 343](#)).

### The Primary Partition

The primary partition is the first partition you specify as a member of the HA group. While cryptographic operations are load-balanced across all the partitions in the group, new keys are always created on the primary partition, and then replicated on the other partitions (see ["Key Replication" below](#)). Depending on how many new keys you are creating on your HA group, this can mean that the primary partition has a heavier workload than the other partitions in the group. If your HSMs are in different remote locations, you could select one with the least latency as the primary partition.

Despite its name, the primary partition is not more critical than any other partition in the HA group. If the primary partition fails, its operations fail over to other partitions in the group, and the next member added to the group becomes the new primary partition.

### Network Topography

The network topography of the HA group is generally not important to the functioning of the group. As long as the client has a network path to each member, the HA logic will function. Different latencies between the client and each HA member cause a command scheduling bias towards the low-latency members. Commands scheduled on the long-latency devices have a longer overall latency associated with each command.

In this case, the command latency is a characteristic of the network. To achieve uniform load distribution, ensure that partitions in the group have similar network latency.

### Key Replication

When an application creates a key on the virtual HA slot, the HA library automatically replicates the key across all group members before reporting back to the application. Keys are created on one member partition and replicated to the other members. If a member fails during this process, the HA group reattempts key replication to that member until it recovers, or failover attempts time out. Once the key exists on all active members of the HA group, a success code is returned to the application.

**Key replication, for pre-firmware-7.7.0 HSM partitions and for V0 partitions**, uses the Luna cloning protocol, which provides mutual authentication, confidentiality, and integrity for each object that is copied from one partition to another. Therefore, all HA group member partitions must be initialized with the same cloning domain.

**Key replication for V1 partitions** uses the Luna cloning protocol to ensure that all HA group members have

the same SMK, and uses SKS to export a key originating at one member and to import and decrypt that key (using the common SMK) on each other member in the group. Again, all HA group member partitions must be initialized with the same cloning domain in order that the common SMK can be available on every member.

The cloning protocol (for pre-firmware-7.7.0 or V0 or mixed-version HA), or the SKS protocol (for blob transfers in a V1 partition HA) is invoked separately for each object to be replicated and the sequence of required calls must be issued by an authorized client library residing on a client platform that has been authenticated to each of the partitions in the HA group). That is, the client must have an authenticated NTLS or STC channel to the HSM appliance; only an authorized client can perform object synchronization across all HA members.

**NOTE** Objects (session or token) are replicated immediately to all members in an HA group when they are generated in the virtual HA slot. Similarly, deletion of objects (session or token) from the virtual HA slot is immediately replicated across all group members.

If your application bypasses the virtual slot and creates or deletes directly in a physical member slot, the action occurs only in that single physical slot, and can be overturned by the next synchronization operation. For this reason we generally advise to enable HA-only, unless you have specific reason to access individual physical slots, and are prepared (in your application) to perform the necessary housekeeping.

## Failover

When any active HA group member fails, a failover event occurs – the affected partition is dropped from the list of available HA group members, and all operations that were pending on the failed partition are transparently rescheduled on the remaining member partitions. The Luna HSM Client continuously monitors the health of member partitions at two levels:

- > network connectivity – disruption of the network connection causes a failover event after a 20-second timeout.
- > command completion – any command that is not executed within 20 seconds causes a failover event.

**NOTE** Most commands are completed within milliseconds. Some can take longer, either because the command itself is time-consuming (for example, key generation), or because the HSM is under extreme load. The HSM automatically sends a "heartbeat" signal every two seconds for commands that are pending or in progress. The client extends the 20-second timeout whenever it receives a heartbeat, preventing false failover events.

When an HA group member fails, the HA group status (see ["hagroup listgroups" on page 1](#)) reports a device error for the failed member. The client tries to reconnect the failed member at a minimum retry rate of once every 60 seconds, for the specified number of times (see ["Recovery" on the next page](#)).

When a failover occurs, the application experiences a latency stall on the commands in process on the failing unit, but otherwise there is no impact on the transaction flow. The scheduling algorithm described in ["Load Balancing" on page 338](#) automatically minimizes the number of commands that stall on a failing unit during the 20-second timeout.

As long as one HA group member remains functional, cryptographic service is maintained no matter how many other group members fail. As described in ["Recovery" on the next page](#), members can be returned to service without restarting the application.

## Mid-operation failures

Any operation that fails mid-point needs to be re-sent from the calling application. The entire operation returns a failure (CKR\_DEVICE\_ERROR). This is more likely to happen in a multi-part operation, but a failure could conceivably happen during a single atomic operation as well.

For example, multi-part operations could be block encryption/decryption or any other command where the previous state of the HSM is critical to the processing of the next command. These operations must be re-sent, since the HA group does not synchronize partitions' internal memory state, only the stored key material.

**NOTE** You must ensure that your applications can deal with the rare possibility of a mid-operation failure, by re-issuing the affected commands.

## Possible Causes of Failure

In most cases, a failure is a brief service interruption, like a system reboot. These temporary interruptions are easily dealt with by the failover and auto-recovery functions. In some cases, additional actions may be required before auto-recovery can take place. For example, if a partition becomes deactivated, it must be reactivated by the Crypto Officer (see "[Activation and Auto-activation on Multi-factor- \(PED-\) Authenticated Partitions](#)" on [page 299](#)). Some permanent failures may require manual recovery (see "[Recovery](#)" below). Possible failure events include:

### > HSM-side failures

- HSM card failure
- HSM re-initialization
- HSM reboot
- HSM power failure
- Deactivated partition
- NTLS service failure
- STC service failure

### > Client-side failures

- Client workstation power failure
- Client workstation reboot
- Network keepalive failure

### > Network failures

- Network failure near the HSM (one member partition disappears from client's view)
- Network failure near the client (client loses contact with all member partitions)

## Recovery

Recovery of a failed HA group member is designed to be automatic in as many cases as possible. You can configure your auto-recovery settings to require as much manual intervention as is convenient for you and your organization. In either an automated or manual recovery process, there is no need to restart your application. As part of the recovery process:

- > Any cryptographic objects created while the member was offline are automatically replicated to the recovered partition.
- > The recovered partition becomes available for its share of load-balanced cryptographic operations.

### Auto-recovery

When auto-recovery is enabled, Luna HSM Client performs periodic recovery attempts when it detects a member failure. You can adjust the frequency (maximum once per minute) and the total number of retries (no limit). If the failed partition is not recovered within the scheduled number of retries, it remains a member of the HA group, but the client will no longer attempt to recover it. You must then address whatever equipment or network issue caused the failure, and execute a manual recovery of the member partition.

With each recovery attempt, a single application thread experiences a slight latency delay of a few hundred milliseconds while the client uses the thread to recover the failed member partition.

There are two HA auto-recovery modes:

- > **activeBasic** – uses a separate, non-session-based Active Recovery Thread to perform background checks of HA member availability, recover failed members, and synchronize the contents of recovered members with the rest of the group. It does not restore existing sessions if all members fail simultaneously and are recovered.
- > **activeEnhanced** – works the same as activeBasic, but restores existing sessions and login states if all members fail and are recovered.

HA auto-recovery is disabled by default. It is automatically enabled when you set the recovery retry count (see ["Configuring HA Auto-Recovery" on page 358](#)). Thales recommends enabling auto-recovery in all configurations.

**NOTE** If a member partition loses Activation when it fails (it remains offline for more than two hours) you must present the black Crypto Officer PED key to re-cache the PED secret before the member can be recovered.

### Manual Recovery

When auto-recovery is disabled, or fails to recover the partition within the scheduled number of retries, you must execute a manual recovery in LunaCM. Even if you use manual recovery, you do not need to restart your application. When you execute the recovery command, the client makes a recovery attempt the next time the application uses the group member (see ["Manually Recovering a Failed HA Group Member" on page 366](#)).

Even with auto-recovery enabled and configured for a large number of retries, there are some rare occasions where a manual recovery may be necessary (for example, when a member partition and the client application fail at the same time).

**CAUTION!** Never attempt a manual recovery while the application is running and auto-recovery is enabled. This can cause multiple concurrent recovery processes, resulting in errors and possible key corruption.

## Failure of All Group Members

If all members of an HA group fail (and no standby members are configured), all logged-in sessions are lost, and operations that were active when the last member failed are terminated. If you have set the HA auto-recovery mode to `activeEnhanced`, all sessions will be restarted when one or more members are recovered, and normal operations will resume. Otherwise, you must restart the client application once the group members have been recovered.

## Permanent Failures

Sometimes an HSM failure is permanent (from the perspective of the HA group). For example, if the HSM is re-initialized, the member partition is erased and must be recreated. In this case, you can decide to recreate the original member or deploy a new member to the group. The client automatically replicates cryptographic objects to the new member and begins assigning operations to it (see ["Replacing an HA Group Member" on page 367](#)).

## Standby Members

After you add member partitions to an HA group, you can designate some as standby members. Cryptographic objects are replicated on all members of the HA group, including standby members, but standby members do not perform any cryptographic operations unless all the active members go offline. In this event, all standby members are immediately promoted to active service, and operations are load-balanced across them. This provides an extra layer of assurance against a service blackout for your application.

Since standby members replicate keys but do not perform operations, they can also serve as an automatic backup partition for the cryptographic objects on the HA group. The contents of standby partitions are always kept up-to-date, so it is not possible to keep multiple backups (different generations of preserved material) using an HA group (see ["Planning Your HA Group Deployment" on page 346](#)). You can consider HA standby members to be your backup only in the case where the most recent sync always replicates all objects you are interested in preserving and recovering.

If you have audit-compliance rules or other mandate to preserve earlier partition contents (keys and objects), then you should perform intentional backups with dedicated backup devices (see ["Backup and Restore Using a Luna Backup HSM \(G5\)" on page 379](#) if you already have a Luna Backup HSM (G5), or ["Backup and Restore Using a Luna Backup HSM \(G7\)" on page 408](#) if you purchase a new Backup HSM).

## Mixed-Version HA Groups

Generally, Thales recommends using HSMs with the same software/firmware in HA groups; different versions have different capabilities, and a mixed HA group is limited to those functions that are common to the versions involved. A mixed-version HA group may have access to fewer cryptographic mechanisms, or have different restrictions in FIPS mode. However, HA groups containing both Luna 6 and 7 partitions and Luna Cloud HSM services from Thales Data Protection on Demand are supported. This mixed-version configuration is useful for migrating keys to a new Luna 7 HSM or the cloud, or to gradually upgrade your production environment from Luna 6 to Luna 7.

## Process Interaction

At the lowest communication level, the transport protocol (TCP) maintains communication between the client and the appliance (whether HA is involved or not). For HA groups involving member partitions on Luna Network HSM, the protocol timeout is 10 seconds. This means:

- > In a period of no activity by client or appliance, the appliance's TCP will wonder if the client is still there, and send a packet after 10 seconds of silence.
- > If that packet is acknowledged, the 10-second TCP timer restarts, and the cycle repeats indefinitely.
- > If the packet is not acknowledged, TCP sends another every 10 seconds. If there is no response after 2 minutes, the connection is considered dead, and higher levels are alerted to perform their cleanup.

Above that level, the NTLS/STC layer provides the connection security and some other services. Any time a client sends a request for a cryptographic operation, the HSM on the appliance begins working on that operation.

While the HSM processes the request, appliance-side NTLS/STC sends a "keep-alive" ping every 2 seconds, until the HSM completes the request. NTLS/STC does not perform any interpretation of the ping, but simply keeps the TCP layer active. If your client application requests a lengthy operation (for example, an 8192-bit keygen), the random-number-generation portion of that operation could take minutes, during which the HSM would legitimately be sending nothing back to the client. The NTLS ping ensures that the connection remains alive during long pauses.

## Application Object Handles

Application developers should be aware that the PKCS #11 object handle model is fully virtualized when using an HA slot. The application must not assume fixed handle numbers across instances of an application. A handle's value remains consistent for the life of a process; but it might be a different value the next time the application is executed.

When you use an HA slot with your applications, the client behaves as follows when interacting with the application:

1. Intercept the call from the application.
2. Translate virtual object handles to physical object handles using the mappings specified by the virtual object table. The virtual object table is created and updated for the current session only, and only contains a list of the objects accessed in the current session.
3. Launch any required actions on the appropriate HSM or partition.
4. Receive the result from the HSM or partition and forward the result to your application,
5. Propagate any changes in objects on the physical HSM that performed the action to all of the other members of the HA group.

## Virtual slots and virtual objects

When an application uses a non-HA physical slot, it addresses all objects in the slot by their physical object handles. When an application uses an HA slot, however, a virtual layer of abstraction overlays the underlying physical slots that make up the HA group, and the HA group is presented to the application as a virtual slot. This virtual slot contains virtual objects that have virtual object handles. The object handles in an HA slot are virtualized since the object handles on each of the underlying physical slots might be different from slot to slot. Furthermore, the physical object handles could change if a member of the HA group drops out (fails or loses communication) and is replaced.



## The virtual object table

HA slots use a virtual object table to map the virtual objects in the virtual HA slot to the real objects in the physical slots that make up the HA group. The HA client builds a virtual object table for each application that loads the library. The table is ephemeral, and only exists for the current session. It is created and updated, if necessary, each time an application makes a request to access an object. To maximize performance and efficiency, the table only contains a list of the objects accessed in the current session. For example, the first time an application accesses an object after application start up, the table is created, a look up is performed to map the virtual object to its underlying physical objects, and an entry for the object is added to the table. For each subsequent request for that object, the data in the table is used and no look up is required. If the application then accesses a different object that is not listed in the table, a new look up is performed and the table is updated to add an entry for the new object.

## C\_FindObjects behavior and application performance

Since the client must perform a lookup to create the virtual object table, the way you use the C\_FindObjects function can have a significant impact on the performance of your applications. For example, if you use the C\_FindObjects function to ask for specific attributes, the client only needs to update the table to include the requested objects. If, however, you use the C\_FindObjects function to find all objects, the client queries each HSM/partition in the group, for each object, to create the table. This can take a significant amount of time if the slot contains a large number of objects, or if the HA group includes many members.

To mitigate performance degradation when using the C\_FindObjects function to list the objects on an HA slot, we recommend that you structure your applications to search by description, handles, or other attributes, rather than searching for all objects. Doing so minimizes the number of objects returned and the time required to create or update the table. If your application must find all objects, we recommend that you add the C\_FindObjects all function call to the beginning of your application so that the table is built on application start up, so that the table is available to the application for all subsequent C\_FindObjects function calls.

## Example: Database Encryption

This section walks through a sample use case of some of the HA logic with a specific application – a transparent database encryption.

### Typical Database Encryption Key Architecture

Database engines typically use a two-layered key architecture. At the top layer is a master encryption key that is the root of data protection. Losing this key is equivalent to losing the database, so it obviously needs to be highly durable. At the second layer are table keys used to protect table-spaces and/or columns. These table keys are stored with the database as blobs encrypted by the master encryption key (MEK). This architecture maps to the following operations on the HSM:

1. Initial generation of master key for each database.
2. Generation and encryption of table keys with the master key.
3. Decryption of table keys when the database needs to access encrypted elements.
4. Generation of new master keys during a re-key and then re-encrypting all table keys with it.
5. Generation and encryption of new table keys for storage in the database (often done in a software module).

The HSM is not involved in the use of table keys. Instead it provides the strong protection of the MEK which is used to protect the table keys. Users must follow backup procedures to ensure their MEK is as durable as the database itself ("[Backup and Restore Using a Luna Backup HSM \(G5\)](#) " on page 379).

## HSM High Availability with Database Encryption

When the HSMs are configured as an HA group, the database's master key is automatically and transparently replicated to all the members when the key is created or re-keyed. If an HSM group member was offline or fails during the replication, it does not immediately receive a copy of the key. Instead the HA group proceeds after replicating to all of the active members. Once a member is re-joined to the group the HSM client automatically replicates the new master keys to the recovered member.

Before every re-key event, the user must ensure the HA group has sufficient redundancy. A re-key will succeed as long as one HA group member exists, but proceeding with too few HSMs will result in an availability risk. For example, proceeding with only one HSM means the new master key will be at risk since it exists only on a single HSM. Even with sufficient redundancy, Thales Group recommends maintaining an offline backup of a database's master key.

## HSM Load Balancing with Database Encryption

While a database is up and running, the master key exists on all members in the HA group. Requests to encrypt or decrypt table keys are distributed across the entire group. The load-balancing feature is able to deliver improved performance and scalability when the database requires a large number of accesses to the table keys. Most deployments will not need much load balancing as the typical database deployment results in a small number of table keys.

While the table keys are re-keyed, new keys are generated in the HSM and encrypted for storage in the database. Within an HA group, these keys are generated on the primary member and then replicated to the entire HA group, even though they exist on the HSM for only a moment. These events are infrequent enough that this extra replication has minimal impact.

## Planning Your HA Group Deployment

This section describes important considerations and constraints to keep in mind as you plan your High-Availability (HA) group deployment. The benefits of HA are described in detail in ["High-Availability Groups" on page 336](#). There are several sample configurations described in this section that take advantage of different HA features. Depending on your organization's security needs, you might choose one of these configurations, or your own variation.

- > ["HSM and Partition Prerequisites" below](#)
- > ["Sample Configurations" on the next page](#)
  - ["Performance and Load Balancing" on the next page](#)
  - ["Redundancy and Failover" on page 348](#)
  - ["Automatic Remote Backup" on page 349](#)
  - ["HA Group Sharing" on page 349](#)

If you plan to create an HA group consisting of different kinds of Luna HSMs, refer also to:

- > ["Cloning Keys Between Luna 6, Luna 7, and Luna Cloud HSM" on page 171](#)

## HSM and Partition Prerequisites

The HSM partitions you plan to use in an HA group must meet the following prerequisites before you can use them in an HA group.

### Compatible HSM Software/Firmware Versions

Generally, Thales recommends using HSMs with the same software/firmware in HA groups; different versions have different capabilities, and a mixed-version HA group is limited to those functions that are common to the versions involved. This means they have access to fewer cryptographic mechanisms, or have different restrictions in FIPS mode. However, mixed-version HA groups containing Luna 6 and 7 member partitions and Luna Cloud HSM services are supported. See ["Cloning Keys Between Luna 6, Luna 7, and Luna Cloud HSM" on page 171](#) for more information.

### Common Cloning Domain

All key replication in an HA group uses the Luna cloning protocol, which provides mutual authentication, confidentiality, and integrity for each object that is copied from one partition to another. Therefore, all HA group member partitions must be initialized with the same cloning domain. If you are planning to combine already-existing partitions into an HA group, you must first re-initialize them using the same domain string or red PED key.

### Common Crypto Officer Credentials

An HA group essentially allows you to log in to all its member partitions simultaneously, using a single credential. Password-authenticated partitions must all be initialized with the same Crypto Officer password. PED-authenticated partitions must all be initialized with the same black Crypto Officer PED key and activated with the same CO challenge password.

It is not possible to create an HA group made up of both password- and PED-authenticated partitions.

### Common HSM/Partition Policies (FIPS Mode)

Generally, all HSMs/partitions used in an HA group must have the same policy configuration, especially FIPS mode. Do not attempt to use an HA group combining HSMs with FIPS mode on and others with FIPS mode off.

### Functionality Modules

If you intend to use Functionality Modules (FMs) with your HA group, all HSMs containing HA group members must have FMs enabled and they must all have the same FM(s) loaded. See [FM Deployment Constraints](#) for details. FMs are not supported for Luna Cloud HSM services.

## Sample Configurations

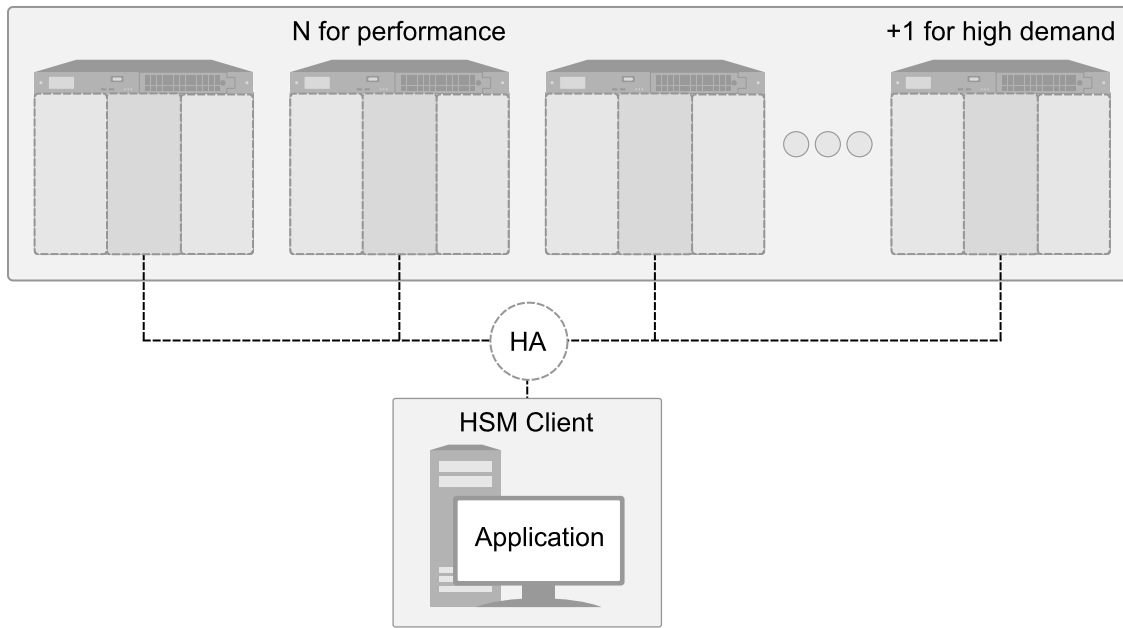
Your ideal HA group configuration depends on the number of HSMs you have available and the purpose of your application(s). Sample configurations for different types of deployment are described below.

### Performance and Load Balancing

If your application is designed to perform many cryptographic operations as quickly as possible, using keys or other objects that do not change often, you can create a large HA group using partitions on many HSMs. This deployment uses load balancing to provide linear performance gains for each HSM added to the group.

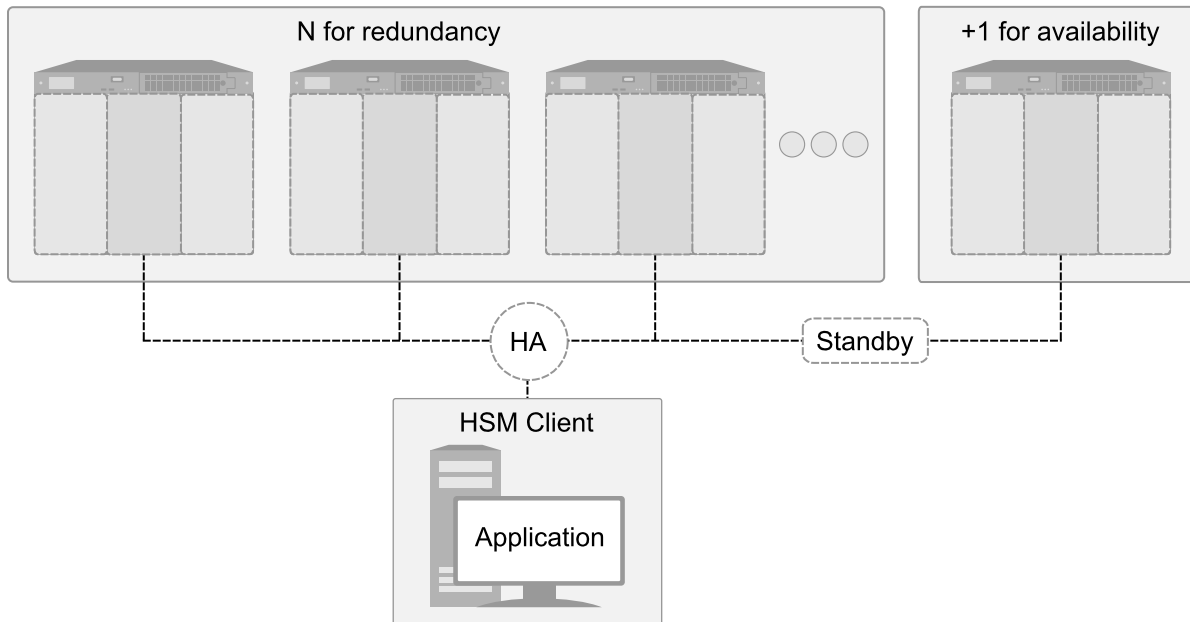
For example: your application uses keys stored on the HSM to perform many encrypt/decrypt or sign/verify operations. You want to minimize transaction latency by providing enough HSMs to handle capacity.

The Luna HSM Client allows HA groups with up to 32 member partitions. The best approach in this example is to add enough group members to handle the usual number of operations, plus enough extra members to handle periods of high demand.



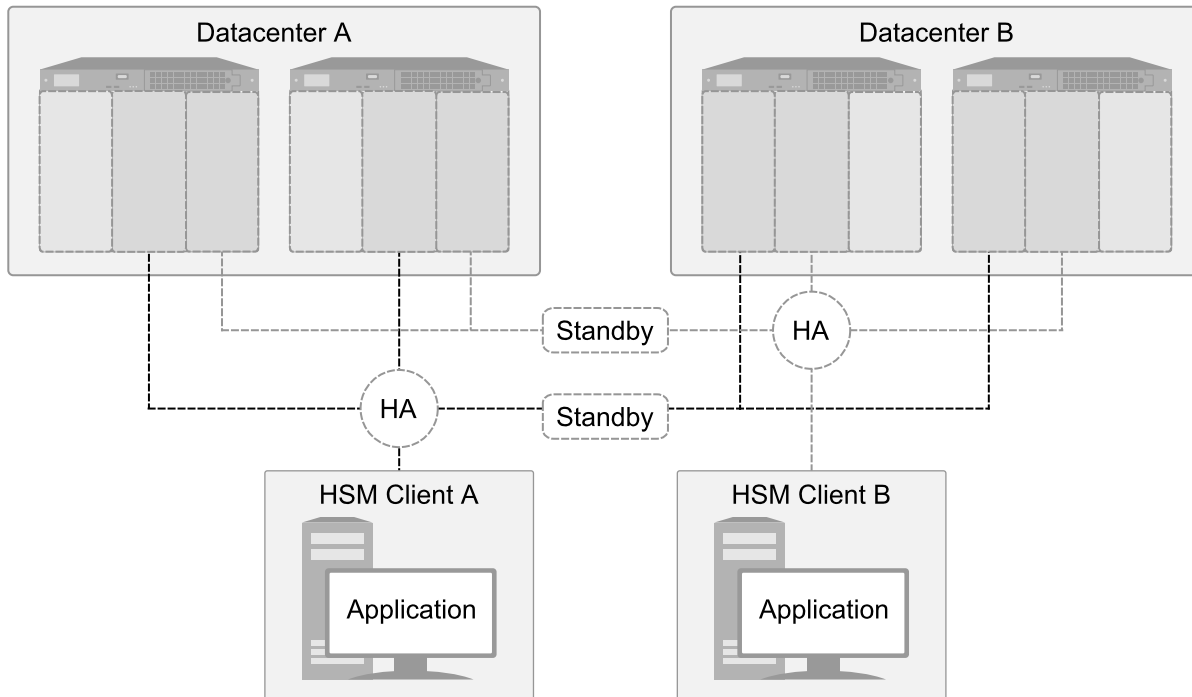
### Redundancy and Failover

If your application requires continuous, uninterrupted uptime, operations assigned to an HA group are reassigned to other group members in the event of a member failure (see ["Failover" on page 340](#) for details). Additional group members can be added and set to standby mode for an extra layer of redundancy (see ["Standby Members" on page 343](#) for details).



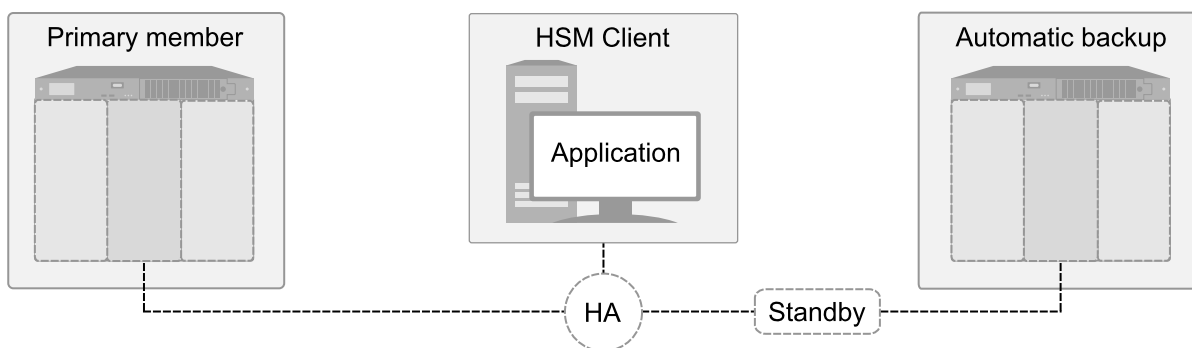
To maximize the use of your HSMs, plan which member partitions you will set to standby mode. Although the configuration above is a straightforward example of an HA group with a single standby member, it is not an ideal production configuration, because the standby member is idle unless all the other members fail. The configuration below is a more useful implementation of two HA groups, each with standby members on the other's HSMs.

As depicted below, applications can be deployed in geographically dispersed locations. In this scenario, Luna's standby capability allows you to use the HSMs in Datacenter B to cost-effectively improve availability for the local HA group at Datacenter A, and vice-versa. This approach allows the HA groups to avoid using remote HSMs with high latency, unless they are urgently required. If all local members fail, the standby partitions are automatically promoted to active status.



### Automatic Remote Backup

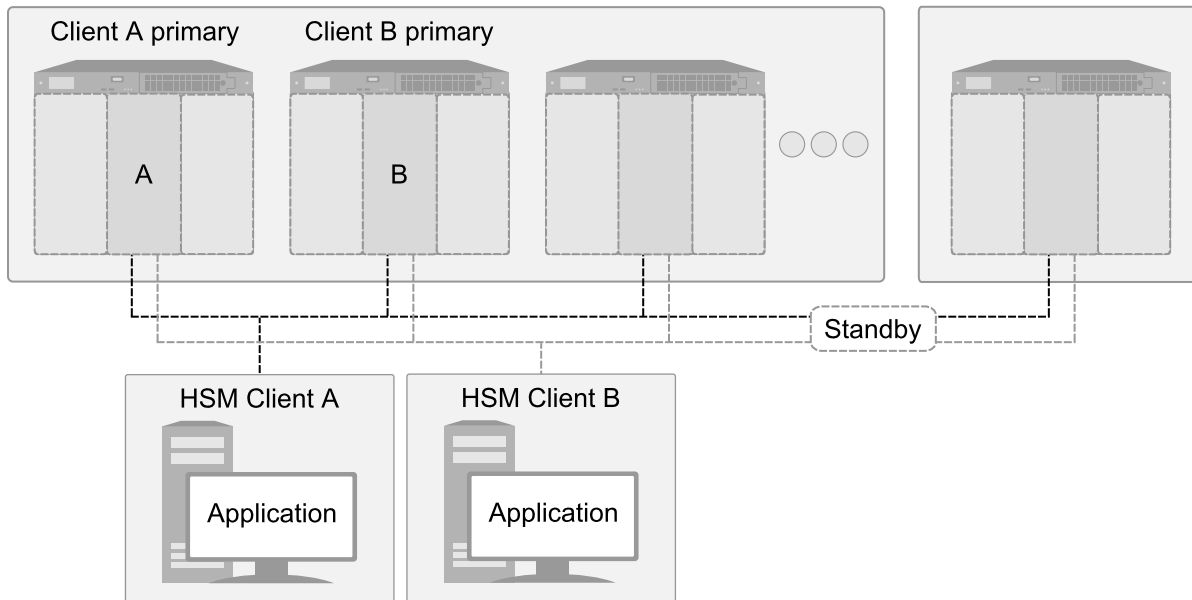
Since the contents of member partitions are always kept up-to-date, you can use an HA group to keep an automatic backup of your cryptographic objects. Set the backup member to standby mode so that it does not perform operations. If the regular member(s) fail, the standby member takes over operations.



### HA Group Sharing

Generally, an HA group is defined on a single client, which runs an application against the virtual HA group. You can share the HA group across multiple clients by assigning all member partitions to both clients and creating the HA group independently on each one.

**TIP** When an HA group is shared across multiple clients, the group can be defined with a different primary member (the first partition assigned to the group) on each client. This approach optimizes an HA group to distribute the key management and/or multi-part cryptographic operation load more equally.



## Setting Up an HA Group

Use LunaCM to create an HA group from partitions assigned to your client. This procedure is completed by the Crypto Officer. Ensure that you have met all necessary prerequisites before proceeding with group creation. For a detailed description of HA functionality, see ["High-Availability Groups" on page 336](#).

**NOTE** Your LunaCM instance needs to update the **Chrystoki.conf** (Linux/UNIX) or **crystoki.ini** file (Windows) when setting up or reconfiguring HA. Ensure that you have Administrator privileges on the client workstation.

Back up the SMK in any partition where that SMK is likely to be overwritten, if that SMK is ever likely to be needed to insert (decrypt) any SKS blobs. If an SMK is cloned from one partition to another (such as must be done when adding members to an HA group), a pre-existing SMK already in the target partition is overwritten by the incoming SMK. Any blobs still encrypted with it are lost, unless a backup exists.

## Prerequisites

HA groups are set up in LunaCM by the Crypto Officer. Before the CO can perform this setup, however, all HSMs and member partitions must meet the following prerequisites, completed by the HSM and Partition Security Officers.

## HSMs

The HSM SO must ensure that all HSMs containing HA group member partitions meet the following prerequisites:

- > All HSMs must use the same authentication method (Password/PED). Luna Cloud HSM Services support password authentication only.
- > HA groups cannot contain both PCIe HSMs and Network HSMs.
- > All must be running one of the supported software/firmware versions. Generally, Thales recommends using HSMs with the same software/firmware for HA. However, mixed-version HA groups containing Luna 6 and 7 member partitions and Luna Cloud HSM services are supported. See ["Cloning Keys Between Luna 6, Luna 7, and Luna Cloud HSM" on page 171](#) for more information.
- > For Network HSMs, network setup must be complete and the appliances must be accessible via SSH.
- > HSM policies **7: Allow Cloning** and **16: Allow Network Replication** must be set to **1** (see [Setting HSM Policies Manually](#)).
- > HSM policies must be consistent across all HSMs, particularly **12: Allow non-FIPS algorithms**. Do not attempt to use an HA group combining HSMs with FIPS mode on and others with FIPS mode off.
- > The client must be able to access all the application partitions using NTLS or STC links for Network HSMs, or XTC/REST for Luna Cloud HSM Services (see ["Client-Partition Connections" on page 86](#)).

A client can have a session with an STC slot, making use of only one appID. When running an HA command if you are already logged in or have a session open with an appID to a member of that HA slot, you will not be able to log into that slot at this time. When you run a command like "ha list", lunacm logs into each member using a randomly created appID. If any one of these slots already has a login session, such an attempt is rejected with CKR\_ACCESS\_ID\_ALREADY\_EXISTS. The workaround is to close the problem session first.

## Partitions

The Partition SO must ensure that all partitions in an HA group meet the following prerequisites:

- > The partitions must be created on different HSMs; partitions on a single HSM cannot provide failover for each other, as they have a single point of failure.
- > All partitions must be visible in LunaCM on the client workstation.
- > All partitions must be initialized with the same cloning domain:
  - Password-authenticated partitions must share the same domain string.
  - PED-authenticated partitions must share the same red domain PED key.
- > Partition policies **0: Allow private key cloning** and **4: Allow secret key cloning** must be set to **1** on all partitions.
- > Partition policies must be consistent across all member partitions.
- > The Crypto Officer role on each partition must be initialized with the same CO credential (password or black PED key).
- > PED-authenticated partitions must have partition policies **22: Allow activation** and **23: Allow auto-activation** set to **1**. All partitions must be activated and have auto-activation enabled, so that they can retain their login state after failure/recovery. Each partition must have the same activation challenge secret set (see ["Activation and Auto-activation on Multi-factor- \(PED-\) Authenticated Partitions" on page 299](#))

**NOTE** If HSM policy **21: Force user PIN change after set/reset** is set to **1** (the default setting), the Crypto Officer must change the initial CO credential before using the partition for cryptographic operations. This applies to the activation challenge secret as well (see [role changepw](#)).

## To set up an HA group

1. Decide which partition will serve as the primary member (see ["The Primary Partition" on page 339](#)). Create a new HA group, specifying the following information:

- the group label (do not call the group "HA")
- the Serial number OR the slot number of the primary member partition
- the Crypto Officer password or challenge secret for the partition

```
lunacm:>hagroup creategroup -label <label> {-slot <slotnum> | -serialnumber <serialnum>}
```

```
lunacm:> hagroup creategroup -label myHAGroup -slot 0
```

```
Enter the password: *****
```

```
New group with label "myHAGroup" created with group number 1154438865287.
Group configuration is:
```

```
HA Group Label: myHAGroup
HA Group Number: 1154438865287
HA Group Slot ID: Not Available
Synchronization: enabled
Group Members: 154438865287
Needs sync: no
Standby Members: <none>
```

Slot #	Member S/N	Member Label	Status
=====	=====	=====	=====
0	154438865287	par0	alive

```
Command Result : No Error
```

LunaCM generates a serial number for the HA group (by adding a "1" before the primary partition serial number), assigns it a virtual slot number, and automatically restarts.

```
lunacm (64-bit) v7.3.0. Copyright (c) 2018 SafeNet. All rights reserved.
```

```
Available HSMs:
```

```
Slot Id -> 0
Label -> par0
Serial Number -> 154438865287
Model -> LunaSA 7.3.0
Firmware Version -> 7.3.0
Configuration -> Luna User Partition With SO (PW) Key
Export With Cloning Mode
Slot Description -> Net Token Slot
```



```

Slot Id -> 1
Label -> par1
Serial Number -> 1238700701509
Model -> LunaSA 7.3.0
Firmware Version -> 7.3.0
Configuration -> Luna User Partition With SO (PW) Key
Export With Cloning Mode
Slot Description -> Net Token Slot

Slot Id -> 5
HSM Label -> myHAGroup
HSM Serial Number -> 1154438865287
HSM Model -> LunaVirtual
HSM Firmware Version -> 7.3.0
HSM Configuration -> Luna Virtual HSM (PW) Key Export With
Cloning Mode
HSM Status -> N/A - HA Group

```

Current Slot Id: 0

2. Add another partition to the HA group, specifying either the slot or the serial number. If the new member contains cryptographic objects, you are prompted to decide whether to replicate the objects within the HA group, or delete them.

```
lunacm:> hagroup addmember -group <grouplabel> {-slot <slotnum> | -serialnumber <serialnum>}
```

```
lunacm:> hagroup addmember -group myHAGroup -slot 1
```

Enter the password: \*\*\*\*\*

Warning: There are objects currently on the new member.  
Do you wish to propagate these objects within the HA group, or remove them?

Type 'copy' to keep and propagate the existing objects, 'remove' to remove them before continuing, or 'quit' to stop adding this new group member.  
> copy

Member 1238700701509 successfully added to group myHAGroup. New group configuration is:

```

HA Group Label: myHAGroup
HA Group Number: 1154438865287
HA Group Slot ID: 5
Synchronization: enabled
Group Members: 154438865287, 1238700701509
Needs sync: no
Standby Members: <none>

```

Slot #	Member S/N	Member Label	Status
=====	=====	=====	=====
0	154438865287	par0	alive
1	1238700701509	par1	alive

Please use the command "ha synchronize" when you are ready to replicate data between all members of the HA group. (If you have additional members to add, you may wish to wait until you have added them before synchronizing to save time by avoiding multiple synchronizations.)

Command Result : No Error

Repeat this step for each additional HA group member.

**NOTE** By default, `lunacm:>hagroup addmember` automatically adds a Luna Cloud HSM service as a standby HA member. If you prefer to use the Luna Cloud HSM service as an active HA member, you must first edit the following toggle in the `Chrystoki.conf/crystoki.ini` configuration file (see ["Configuration File Summary" on page 70](#)):

```
[Toggles]
lunacm_cv_ha_ui = 0
```

3. If you are adding member partitions that already have cryptographic objects stored on them, initiate a manual synchronization. You can tell whether this step is required by checking the line **Needs Sync : yes/no** in the HA group output. This will also confirm that the HA group is functioning correctly.
 

```
lunacm:> hagroup synchronize -group <grouplabel>
```
4. [Optional] If you created an HA group out of empty partitions, and you want to verify that the group is functioning correctly, see ["Verifying an HA Group" below](#).
5. Specify which member partitions, if any, will serve as standby members.
 

See ["Setting an HA Group Member to Standby" on page 356](#).
6. Set up and configure auto-recovery (recommended). If you choose to use manual recovery, you will have to execute a recovery command whenever a group member fails.
 

See ["Configuring HA Auto-Recovery" on page 358](#).
7. [Optional] Enable HA Only mode (recommended).
 

See ["Enabling/Disabling HA Only Mode" on page 358](#).
8. [Optional] Configure HA logging.
 

See ["HA Logging" on page 359](#) for procedures and information on reading HA logs.

The HA group is now ready for your application.

## Verifying an HA Group

After creating an HA group in LunaCM, you can see the group represented as a virtual slot alongside the physical slots:

```
lunacm (64-bit) v7.3.0. Copyright (c) 2018 SafeNet. All rights reserved.
```

```
Available HSMs:
```

```
Slot Id -> 0
Label -> par0
```

```

Serial Number -> 154438865287
Model -> LunaSA 7.3.0
Firmware Version -> 7.3.0
Configuration -> Luna User Partition With SO (PW) Key Export With Cloning Mode
Slot Description -> Net Token Slot

Slot Id -> 1
Label -> parl
Serial Number -> 1238700701509
Model -> LunaSA 7.3.0
Firmware Version -> 7.3.0
Configuration -> Luna User Partition With SO (PW) Key Export With Cloning Mode
Slot Description -> Net Token Slot

Slot Id -> 5
HSM Label -> myHAGroup
HSM Serial Number -> 1154438865287
HSM Model -> LunaVirtual
HSM Firmware Version -> 7.3.0
HSM Configuration -> Luna Virtual HSM (PW) Key Export With Cloning Mode
HSM Status -> N/A - HA Group

```

Current Slot Id: 0

The following procedure is one way to verify that your HA group is working as intended:

### To verify an HA group

1. Exit LunaCM and run **multitoken** against the HA group slot number (slot 5 in the example) to create some objects on the HA group partitions.

```
./multitoken -mode <keygen_mode> -key <key_size> -nodestroy -slots <HA_virtual_slot>
```

You can hit **Enter** at any time to stop the process before the partitions fill up completely. Any number of created objects will be sufficient to show that the HA group is functioning.

2. Run LunaCM and check the partition information on the two physical slots. Check the object count under "Partition Storage":

```
lunacm:> partition showinfo
```

```
Current Slot Id: 0
```

```
lunacm:> partition showinfo
```

```
... (clip) ...
```

```

Partition Storage:
 Total Storage Space: 325896
 Used Storage Space: 22120
 Free Storage Space: 303776
 Object Count: 14
 Overhead: 9648

```

```
Command Result : No Error
```

```
lunacm:> slot set slot 1
```

```

Current Slot Id: 1 (Luna User Slot 7.0.1 (PW) Signing With Cloning Mode)

Command Result : No Error

lunacm:> partition showinfo

... (clip) ...

Partition Storage:
 Total Storage Space: 325896
 Used Storage Space: 22120
 Free Storage Space: 303776
 Object Count: 14
 Overhead: 9648

Command Result : No Error

```

3. To remove the test objects, login to the HA virtual slot and clear the virtual partition.

```

lunacm:> slot set -slot <HA_virtual_slot>

lunacm:> partition login

lunacm:> partition clear

```

If you are satisfied that your HA group is working, you can begin using your application against the HA virtual slot. The virtual slot assignment will change depending on how many more application partitions are added to your client configuration. If your application invokes the HA group label, this will not matter. If you have applications that invoke the slot number, see ["Enabling/Disabling HA Only Mode" on page 358](#).

## Setting an HA Group Member to Standby

Some HA group members can be designated as standby members. Standby members do not perform any cryptographic operations unless all active members have failed (see ["Standby Members" on page 343](#) for details). They are useful as a last resort against loss of application service.

### Prerequisites

- > The partition you want to designate as a standby member must already be a member of the HA group (see ["Adding/Removing an HA Group Member" on page 363](#)).
- > The group member must be online.
- > The Crypto Officer must perform this procedure.

### To set an HA group member to standby

1. [Optional] Check the serial number of the member you wish to set to standby mode.

```
lunacm:> hagroup listgroups
```

2. Set the desired member to standby mode by specifying the serial number.

```
lunacm:> hagroup addstandby -group <label> -serialnumber <member_serialnum>
```

```
lunacm:> hagroup addstandby -group myHAGroup -serialnumber 2855496365544
```

The member 2855496365544 was successfully added to the standby list for the HA Group myHAGroup.

Command Result : No Error

## To make a standby HA member active

**NOTE** By default, a Luna Cloud HSM service from Thales DPoD is always added to an HA group as a standby member. If you prefer to use the Luna Cloud HSM service as an active HA member, you must first edit the following toggle in the **Chrystoki.conf/crystoki.ini** configuration file (see "[Configuration File Summary](#)" on page 70):

```
[Toggles]
lunacm_cv_ha_ui = 0
```

### 1. [Optional] Check the serial number of the standby member.

```
lunacm:> hagroup listgroups
```

If you would like to see synchronization data for group myHAGroup, please enter the password for the group members. Sync info not available in HA Only mode.

Enter the password: \*\*\*\*\*

```

 HA auto recovery: disabled
 HA recovery mode: activeBasic
Maximum auto recovery retry: 0
Auto recovery poll interval: 60 seconds
 HA logging: disabled
Only Show HA Slots: no

 HA Group Label: myHAGroup
 HA Group Number: 11238700701509
 HA Group Slot ID: 5
 Synchronization: enabled
 Group Members: 154438865287, 1238700701509
 Needs sync: no
 Standby Members: 2855496365544
```

Slot #	Member S/N	Member Label	Status
=====	=====	=====	=====
0	154438865287	par0	alive
1	1238700701509	par1	alive
2	2855496365544	par2	alive

### 2. Remove the member from standby and return it to active HA use.

```
lunacm:> hagroup removestandby -group <label> -serialnumber <member_serialnum>
```

```
lunacm:> hagroup removestandby -group myHAGroup -serialnumber 2855496365544
```

The member 2855496365544 was successfully removed from the standby list for the HA Group myHAGroup.

Command Result : No Error

## Configuring HA Auto-Recovery

When auto-recovery is enabled, Luna HSM Client performs periodic recovery attempts when it detects a member failure. HA auto-recovery is disabled by default for new HA groups. To enable it, you must set a maximum number of recovery attempts. You can also set the frequency of recovery attempts, and the auto-recovery mode (**activeBasic** or **activeEnhanced**). These settings will apply to all HA groups configured on the client.

### To configure HA auto-recovery

1. Set the desired number of recovery attempts by specifying the retry count as follows:

- Set a value of **0** to disable HA auto-recovery
- Set a value of **-1** for unlimited retries
- Set any specific number of retries from **1** to **500**

lunacm:> **hagroup retry -count** <retries>

2. [Optional] Set the desired frequency of recovery attempts by specifying the time in seconds. The acceptable range is **60-1200** seconds (default: **60**).

lunacm:> **hagroup interval -interval** <seconds>

3. [Optional] Set the auto-recovery mode. The default is **activeBasic**.

lunacm:> **hagroup recoverymode -mode** {**activeBasic** | **activeEnhanced**}

4. [Optional] Check that auto-recovery has been enabled. You are prompted for the Crypto Officer password/challenge secret.

lunacm:> **hagroup listgroups**

## Enabling/Disabling HA Only Mode

By default, client applications can see both physical slots and virtual HA slots. Directing applications at the physical slots bypasses the high availability and load balancing functionality. An application must be directed at the virtual HA slot to use HA load balancing and redundancy. HA Only mode hides the physical slots and leaves only the HA group slots visible to applications, simplifying the PKCS#11 slot numbering (see ["Slot Numbering and Behavior" on page 453](#)).

If an HA group member partition fails and is recovered, all visible slot numbers can change, including the HA group virtual slots. This can cause applications to direct operations to the wrong slot. If a physical slot in the HA group receives a direct request, the results will not be replicated on the other partitions in the group (see ["HA Troubleshooting" on page 370](#)) When HA Only mode is enabled, the HA virtual slots are not affected by partition slot changes. Thales recommends enabling HA Only mode on all clients running HA groups.

**NOTE** Individual partition slots are still visible in LunaCM when HA Only mode is enabled. They are hidden only from client applications. Use **CKdemo** (Option **11**) to see the slot numbers to use with client applications.

### To enable HA Only mode

1. Enable HA Only mode in LunaCM.

```
lunacm:> hagroup haonly -enable
```

2. [Optional] Since LunaCM still displays the partitions, you can check the status of HA Only mode at any time.

```
lunacm:> hagroup haonly -show
```

### To disable HA Only mode

1. Disable HA Only mode in LunaCM.

```
lunacm:> hagroup haonly -disable
```

## HA Logging

Logging of HA-related events takes place on the Luna HSM Client workstation. The log file **haErrorLog.txt** shows HA errors, as well as add-member and delete-member events. It does not record status changes of the group as a whole (like adding or removing the group).

The HA log rotates after the configured maximum length is reached. When it finishes writing the current record (even if that record slightly exceeds the configured maximum), the file is renamed to include the timestamp and the next log entry begins a new **haErrorLog.txt**.

> ["Configuring HA Logging" below](#)

> ["HA Log Messages" on page 361](#)

### Configuring HA Logging

Using Luna HSM Client 7.2.0 or newer, logging is automatically enabled when you configure an HA group (see ["Setting Up an HA Group" on page 350](#)), but you must configure a valid destination path before logging can begin. HA groups are configured on the client using LunaCM. The HA configuration settings are saved to the **Chrystoki.conf** (Linux/Unix) or **crystoki.ini** (Windows) file, as illustrated in the following example:

```
VirtualToken = {
VirtualToken00Label = haGroup1; // The label of the HA group.
VirtualToken00SN = 11234840370164; // The pseudo serial number of the HA group.
VirtualToken00Members = 1234840370164, 1234924189183; // The serial number of the members.
VirtualTokenActiveRecovery = activeEnhanced; // The recovery mode.
}
HASynchronize = {
haGroup1 = 1; // Enable automatic synchronization of objects.
}
HAConfiguration = {
HAOnly = 1; // Enable listing HA groups only via PKCS#11 library.
haLogPath = /tmp/halog; // Base path of the HA log file; i.e., "/tmp/halog/haErrorLog.txt".
haLogStatus = enabled; // Enable HA log.
logLen = 100000000; // Maximum size of HA log file in bytes.
```

```

failover_on_deactivation = 1; // if a partition becomes deactivated then the client will
immediately failover and resume its operation on the other HA partitions. This is currently an
alpha feature
reconnAtt = 120; // Number of recovery attempts.
}
HARecovery = {
haGroup1 = 1; // Deprecated in this release as auto recovery will cover the use case. When
cryptoki loads into memory it reads the number and if the number changes (gets incremented) then
cryptoki interprets this as a manual recovery attempt.
}

```

## To configure HA logging

Use the LunaCM command **hagroup halog**.

1. Set a valid path for the log directory. You must specify an existing directory.

```
lunacm:> hagroup halog -path <filepath>
```

```
lunacm:> hagroup halog -path "C:\Program Files\Safenet\Lunaclient\halog"
```

```
HA Log path successfully set to C:\Program Files\Safenet\Lunaclient\halog.
```

```
Command Result : No Error
```

2. [Optional] Set the maximum length for individual log files.

```
lunacm:> hagroup halog -maxlength <max_file_length>
```

```
lunacm:> hagroup halog -maxlength 500000
```

```
HA Log maximum file size was successfully set to 500000.
```

```
Command Result : No Error
```

3. [Optional] Enable or disable HA logging at any time.

```
lunacm:> hagroup halog -disable
```

```
lunacm:> hagroup halog -enable
```

```
lunacm:> hagroup halog -disable
```

```
HA Log was successfully disabled.
```

```
Command Result : No Error
```

4. [Optional] View the current status of the HA logging configuration.

```
lunacm:> hagroup halog -show
```

```
lunacm:> hagroup halog -show
```

```
HA Log: enabled
```

```
Log File: C:\Program Files\Safenet\Lunaclient\halog\haErrorLog.txt
```

```
Max File Length: 500000 bytes
```

```
Command Result : No Error
```



## HA Log Messages

The following table provides descriptions of the messages generated by the HA sub-system and saved to the HA log. The HA log is saved to the location specified by **haLogPath** in the **Chrystoki.conf** (Linux/Unix) or **crystoki.ini** (Windows) file.

### Message Format

Every HA log message has a consistent prefix consisting of the date, time, process id, and serial number (of the affected HA group). For example:

```
Wed Oct 4 16:29:21 2017 : [17469] HA group: 11234840370164 ...
```

### Message Descriptions

In the message descriptions, the term **connection** refers to the connection between the Luna HSM Client and the Luna Network appliance. A connection is considered **valid** if the appliance responds correctly on the IP address and port. The connection can transition to **invalid** for a number of reasons. Some examples include if the appliance Ethernet cable is detached, if the appliance is shutdown/rebooted, or if the NTLS service is stopped/restarted.

Message ID	Message/Description
HALOG_CONFIGURED_AS_PASSWORD	<MessagePrefix> configured as a "PASSWORD Based" virtual device <b>Description:</b> Message advising that the virtual partition is password-authenticated. This means that you cannot add a PED-authenticated member to the group.
HALOG_CONFIGURED_AS_PED	<MessagePrefix> configured as a "PED Based" virtual device <b>Description:</b> Message advising that the virtual partition is PED-authenticated. This means that you cannot add a password-authenticated member to the group.
HALOG_DROPMEMBER	<MessagePrefix> has dropped member: <SerialNumber> <b>Description:</b> The connection changed from valid to invalid, determined after an HSM command (such as C_Sign) fails.
HALOG_DROPUNRECOVERABLE	<MessagePrefix> unable to reach member: <SerialNumber>. Manual Recover or Auto Recovery will be able to recover this member <b>Description:</b> The connection is invalid, as determined during a call to C_Initialize.
HALOG_LOGINFAILED	<MessagePrefix> can not login to member: <SerialNumber>, autorecovery will be disabled. Code: <ErrorCodeHex> : <ErrorCodeString> <b>Description:</b> The connection changed from valid to invalid, as determined during a call to C_Login.
HALOG_MEMBER_DEACTIVATED	<MessagePrefix> member: <SerialNumber> deactivated <b>Description:</b> The user manually deactivated the partition, as determined after an HSM command (such as C_Sign) fails.

Message ID	Message/Description
HALOG_MEMBER_NOW_ACTIVATED	<p>&lt;MessagePrefix&gt; recovery attempt &lt;AttemptNumber&gt; member &lt;SerialNumber&gt; is now activated and will be reintroduce back into the HA group.</p> <p><b>Description:</b> Additional info about the recovered partition, which was deactivated and is now becoming activated.</p>
HALOG_MEMBER_REVOKED	<p>&lt;MessagePrefix&gt; member: &lt;SerialNumber&gt; revoked</p> <p><b>Description:</b> The user manually revoked the partition, as determined during a periodic recovery attempt.</p>
HALOG_MEMBERS_OFFLINE	<p>&lt;MessagePrefix&gt; all members gone offline.</p> <p><b>Description:</b> A situation where all members go offline. Recovery is not possible at this point.</p>
HALOG_MGMT_THREAD_START	<p>&lt;MessagePrefix&gt; management thread started</p> <p><b>Description:</b> This thread is responsible for managing all members and HA in general while the HA group is active. The thread starts up when the application first launches.</p>
HALOG_MGMT_THREAD_TERMINATE	<p>&lt;MessagePrefix&gt; management thread terminated</p> <p><b>Description:</b> This thread is responsible for managing all members and HA in general while the HA group is active. If the client application shuts down, this thread will simply terminate. The thread will start up again once the application re-launches.</p>
HALOG_NEWMEMBER	<p>&lt;MessagePrefix&gt; detected new member member: &lt;SerialNumber&gt;</p> <p><b>Description:</b> The user manually added a member to the HA group without restarting the application, as determined during a periodic recovery attempt.</p>
HALOG_RECOVERED	<p>&lt;MessagePrefix&gt; recovery attempt &lt;Integer&gt; succeeded for member: &lt;SerialNumber&gt;</p> <p><b>Description:</b> The connection changed from invalid to valid, as determined during a periodic recovery attempt.</p>
HALOG_RECOVERY_ATTEMPT_#_REINTRODUCING	<p>&lt;MessagePrefix&gt; recovery attempt &lt;AttemptNumber&gt; reintroducing &lt;Number&gt; token objects to recovered token &lt;TokenNumber&gt;</p> <p><b>Description:</b> Additional info about the recovered partition at which some objects were cloned.</p>
HALOG_RECOVERYFAILED	<p>&lt;MessagePrefix&gt; recovery attempt &lt;Integer&gt; failed for member: &lt;SerialNumber&gt;. Code: &lt;ErrorCodeHex&gt; : &lt;ErrorCodeString&gt;.</p> <p>If autorecovery fails, then a second message is logged, as follows:</p> <p>&lt;MessagePrefix&gt; exceeded maximum number of autorecovery attempts for member: &lt;SerialNumber&gt;. Autorecovery will be disabled</p> <p><b>Description:</b> The connection remains invalid, as determined during a periodic recovery attempt.</p>

Message ID	Message/Description
HALOG_REENABLEMEMBER (deprecated)	<pre>&lt;MessagePrefix&gt; Re-enable auto recovery process for member: &lt;SerialNumber&gt;</pre> <p><b>Description:</b> The user manually requested partition recovery, as determined during a periodic recovery attempt before an HSM command.</p>
HALOG_UNRECOVERABLE (deprecated)	<pre>&lt;MessagePrefix&gt; recovery attempt &lt;Integer&gt; failed for member: &lt;SerialNumber&gt;. Manual Recover or Auto Recovery will not be able to recover this member. Code: &lt;ErrorcodeHex&gt; : &lt;ErrorcodeString&gt;</pre> <p><b>Description:</b> The connection is invalid and is not eligible for recovery.</p>
No ID*	<pre>&lt;MessagePrefix&gt; member &lt;SerialNumber&gt; is not activated and is excluded from the HA group</pre> <p><b>Description:</b> The HA member was not activated at the time when a C_Initialize call was made, and is therefore excluded from the HA group. Once the partition is activated, the HA group will attempt an automatic recovery, resulting in one of the two messages below</p>
No ID*	<pre>&lt;MessagePrefix&gt; recovery attempt &lt;SerialNumber&gt; is not activated and cannot be reintroduced back into the HA group\n</pre> <p><b>Description:</b> Recovery failed</p>
No ID*	<pre>&lt;MessagePrefix&gt; recovery attempt &lt;SerialNumber&gt; is now activated and will be reintroduce back into the HA group.\n</pre> <p><b>Description:</b> Recovery succeeded</p>

\* You might encounter these extra messages in the HA logs. They were added for HA development testing and therefore have no Message IDs assigned to them. They could duplicate information covered by other log messages as defined above.

## Adding/Removing an HA Group Member

You can add a new member to an HA group at any time using LunaCM, even if your application is running. Cryptographic objects will be replicated on the new partition and operations will be scheduled according to the load-balancing algorithm (see "[Load Balancing](#)" on page 338).

Likewise, you can remove a member at any time, and currently-scheduled operations will fail over to the rest of the group members (see "[Failover](#)" on page 340).

**NOTE** If you remove the partition that was used to create the group, the HA group serial number changes to reflect this. This is to prevent another HA group from being assigned the same serial number as the original. If your application queries the HA group serial number, it must redirect operations to the new serial.

### Prerequisites

The new member partition must:

- > be assigned to the client and visible in LunaCM

- > be initialized with the same domain string/red domain PED key as the other partitions in the group
- > have the Crypto Officer role initialized with the same credentials as the other partitions in the group
- > be activated and have auto-activation enabled (PED-authenticated)

**NOTE** Back up the SMK in any partition where that SMK is likely to be overwritten, if that SMK is ever likely to be needed to insert (decrypt) any SKS blobs.

If an SMK is cloned from one partition to another (such as must be done when adding members to an HA group), a pre-existing SMK already in the target partition is overwritten by the incoming SMK. Any blobs still encrypted with it are lost, unless a backup exists.

## To add an HA group member

1. Open LunaCM on the client workstation and ensure that the new partition is visible.

```
lunacm (64-bit) v7.3.0. Copyright (c) 2018 SafeNet. All rights reserved.
```

```
Available HSMs:
```

```
Slot Id -> 0
Label -> par0
Serial Number -> 154438865287
Model -> LunaSA 7.3.0
Firmware Version -> 7.3.0
Configuration -> Luna User Partition With SO (PW) Key Export With Cloning Mode
Slot Description -> Net Token Slot
```

```
Slot Id -> 1
Label -> par1
Serial Number -> 1238700701509
Model -> LunaSA 7.3.0
Firmware Version -> 7.3.0
Configuration -> Luna User Partition With SO (PW) Key Export With Cloning Mode
Slot Description -> Net Token Slot
```

```
Slot Id -> 2
Label -> par2
Serial Number -> 2855496365544
Model -> LunaSA 7.3.0
Firmware Version -> 7.3.0
Configuration -> Luna User Partition With SO (PW) Key Export With Cloning Mode
Slot Description -> Net Token Slot
```

```
Slot Id -> 5
HSM Label -> myHAGroup
HSM Serial Number -> 1154438865287
HSM Model -> LunaVirtual
HSM Firmware Version -> 7.3.0
HSM Configuration -> Luna Virtual HSM (PW) Key Export With Cloning Mode
HSM Status -> N/A - HA Group
```

```
Current Slot Id: 0
```

2. Add the new partition to the HA group by specifying either the slot or the serial number. You are prompted for the Crypto Officer password/challenge secret.

```
lunacm:> hagroup addmember -group <label> {-slot <slotnum> | -serial <serialnum>}
```

```
lunacm:> hagroup addmember -group myHAGroup -slot 2
```

```
Enter the password: *****
```

```
Member 2855496365544 successfully added to group myHAGroup. New group configuration is:
```

```
HA Group Label: myHAGroup
HA Group Number: 1154438865287
HA Group Slot ID: 5
Synchronization: enabled
Group Members: 154438865287, 1238700701509, 2855496365544
Needs sync: no
Standby Members: <none>
```

Slot #	Member S/N	Member Label	Status
=====	=====	=====	=====
0	154438865287	par0	alive
1	1238700701509	par1	alive
2	2855496365544	par2	alive

Please use the command "ha synchronize" when you are ready to replicate data between all members of the HA group. (If you have additional members to add, you may wish to wait until you have added them before synchronizing to save time by avoiding multiple synchronizations.)

```
Command Result : No Error
```

## To remove an HA group member

1. Remove the partition from the group by specifying either the slot or the serial number.

```
lunacm:> hagroup removemember -group <label> {-slot <slotnum> | -serial <serialnum>}
```

```
lunacm:> hagroup removemember -group myHAGroup -slot 0
```

```
Member 154438865287 successfully removed from group myHAGroup.
```

```
Note: Serial number for the group changed to 11238700701509.
```

```
Command Result : No Error
```

**NOTE** If you remove the partition that was used to create the group, the HA group serial number changes to reflect this. This is to prevent another HA group from being assigned the same serial number as the original. If your application queries the HA group serial number, it must redirect operations to the new serial.

LunaCM restarts.

lunacm (64-bit) v7.3.0. Copyright (c) 2018 SafeNet. All rights reserved.

Available HSMs:

```
Slot Id -> 0
Label -> par0
Serial Number -> 154438865287
Model -> LunaSA 7.3.0
Firmware Version -> 7.3.0
Configuration -> Luna User Partition With SO (PW) Key Export With Cloning Mode
Slot Description -> Net Token Slot
```

```
Slot Id -> 1
Label -> par1
Serial Number -> 1238700701509
Model -> LunaSA 7.3.0
Firmware Version -> 7.3.0
Configuration -> Luna User Partition With SO (PW) Key Export With Cloning Mode
Slot Description -> Net Token Slot
```

```
Slot Id -> 2
Label -> par2
Serial Number -> 2855496365544
Model -> LunaSA 7.3.0
Firmware Version -> 7.3.0
Configuration -> Luna User Partition With SO (PW) Key Export With Cloning Mode
Slot Description -> Net Token Slot
```

```
Slot Id -> 5
HSM Label -> myHAgrouP
HSM Serial Number -> 11238700701509
HSM Model -> LunaVirtual
HSM Firmware Version -> 7.3.0
HSM Configuration -> Luna Virtual HSM (PW) Key Export With Cloning Mode
HSM Status -> N/A - HA Group
```

Current Slot Id: 0

2. [Optional] Check that the partition was removed from the group.

lunacm:> [hagroup listgroups](#)

## Manually Recovering a Failed HA Group Member

### Manually Recovering a Failed HA Group Member

Thales recommends using auto-recovery for all HA group configurations (see "[Configuring HA Auto-Recovery](#)" on page 358). If you do not enable auto-recovery and a member partition fails, or if the recovery retry count expires before the partition comes back online, you must recover the partition manually using LunaCM. You do not need to pause your application(s) to perform a manual recovery; the HA group handles load-balancing and automatically replicates any new or changed keys to the recovered member.

## To perform a manual recovery of a failed HA group member

1. [Optional] Ensure that the failed member is available and visible in LunaCM by addressing the problem that caused the failure. Display the HA group to see the failed members. You are prompted for the Crypto Officer password/challenge secret.

```
lunacm:> hagroup listgroups
```

```

 HA Group Label: myHAGroup
 HA Group Number: 1154438865287
 HA Group Slot ID: 5
 Synchronization: enabled
 Group Members: 154438865287, 1238700701509
 Needs sync: no
 Standby Members: <none>

```

Slot #	Member S/N	Member Label	Status
-----	-----	-----	-----
-----	154438865287	par0	alive
-----	1238700701509	-----	down

2. If you are using a PED-authenticated partition with auto-activation disabled, or if the partition was down for longer than two hours, log in to the partition as Crypto Officer and present the black CO PED key.

```
lunacm:> slot set -slot <slotnum>
```

```
lunacm:> role login -name co
```

3. Execute the manual recovery command, specifying the HA group label.

```
lunacm:> hagroup recover
```

If you have an application running on the HA group, the failed members will be recovered the next time an operation is scheduled. Load-balancing and key replication is automatic.

4. If you do not currently have an application running, you can manually synchronize the contents of the HA group.

**CAUTION!** Never use manual synchronization if you have an application running. The HA group performs this automatically. Using this command on an HA group that is running an application could create conflicting key versions.

```
lunacm:> hagroup synchronize -group <label>
```

## Replacing an HA Group Member

Sometimes an HSM failure is permanent (from the perspective of the HA group). For example, if the HSM is re-initialized, the member partition is erased and must be recreated. In this case, you can recreate a partition on the same HSM or another HSM, and deploy the new member to the group. You do not need to pause your application to replace an HA group member.

## Prerequisites

The Crypto Officer must complete this procedure, but any new member partition must first be created and assigned to the client by the HSM SO, and initialized by the Partition SO. All the prerequisites listed in ["Setting Up an HA Group" on page 350](#) must be met.

**NOTE** Back up the SMK in any partition where that SMK is likely to be overwritten, if that SMK is ever likely to be needed to insert (decrypt) any SKS blobs.

If an SMK is cloned from one partition to another (such as must be done when adding members to an HA group), a pre-existing SMK already in the target partition is overwritten by the incoming SMK. Any blobs still encrypted with it are lost, unless a backup exists.

## To replace an HA group member

1. [Optional] Display the HA group to see the failed member. You are prompted for the Crypto Officer password/challenge secret.

```
lunacm:> hagroup listgroups
```

```

 HA Group Label: myHAGroup
 HA Group Number: 1154438865287
 HA Group Slot ID: 5
 Synchronization: enabled
 Group Members: 154438865287, 1238700701509
 Needs sync: no
 Standby Members: <none>
```

Slot #	Member S/N	Member Label	Status
-----	-----	-----	-----
-----	154438865287	par0	alive
-----	1238700701509	-----	down

2. Prepare the new HA group member, whether that means creating a new partition on the original HSM or configuring a new Luna Network HSM, and assign the new partition to the HA client. Ensure that the new member partition and the HSM on which it resides meet the prerequisites outlined in ["Setting Up an HA Group" on page 350](#) and is visible in LunaCM.

```
lunacm (64-bit) v7.3.0. Copyright (c) 2018 SafeNet. All rights reserved.
```

```
Available HSMs:
```

```

Slot Id -> 0
Label -> par0
Serial Number -> 154438865287
Model -> LunaSA 7.3.0
Firmware Version -> 7.3.0
Configuration -> Luna User Partition With SO (PW) Key Export With Cloning Mode
Slot Description -> Net Token Slot

Slot Id -> 1
Label -> par1
Serial Number -> 1238700701510
Model -> LunaSA 7.3.0
Firmware Version -> 7.3.0
Configuration -> Luna User Partition With SO (PW) Key Export With Cloning Mode
```



```

Slot Description -> Net Token Slot

Slot Id -> 5
HSM Label -> myHAGroup
HSM Serial Number -> 1154438865287
HSM Model -> LunaVirtual
HSM Firmware Version -> 7.3.0
HSM Configuration -> Luna Virtual HSM (PW) Key Export With Cloning Mode
HSM Status -> N/A - HA Group

```

Current Slot Id: 0

3. Add the new partition to the HA group by specifying either the slot or the serial number. You are prompted for the Crypto Officer password/challenge secret.

```
lunacm:> hagroup addmember -group <label> {-slot <slotnum> | -serial <serialnum>}
```

```
lunacm:> hagroup addmember -group myHAGroup -slot 1
```

```

Enter the password: *****
Member 1238700701510 successfully added to group myHAGroup. New group
configuration is:

```

```

HA Group Label: myHAGroup
HA Group Number: 1154438865287
HA Group Slot ID: 5
Synchronization: enabled
 Group Members: 154438865287, 1238700701509, 1238700701510
 Needs sync: no
 Standby Members: <none>

```

Slot #	Member S/N	Member Label	Status
0	154438865287	par0	alive
1	1238700701510	par1	alive

Please use the command "ha synchronize" when you are ready to replicate data between all members of the HA group. (If you have additional members to add, you may wish to wait until you have added them before synchronizing to save time by avoiding multiple synchronizations.)

Command Result : No Error

The new partition is now an active member of the HA group. If you have an application currently running, cryptographic objects are automatically replicated to the new member and it is assigned operations according to the load-balancing algorithm.

4. Remove the old partition from the group by specifying the serial number.

```
lunacm:> hagroup removemember -group <label> -serial <serialnum>
```

LunaCM restarts.

5. [Optional] If you do not currently have an application running, you can manually synchronize the contents of the HA group.

**CAUTION!** Never use manual synchronization if you have an application running. The HA group performs this automatically. Using this command on an HA group that is running an application could create conflicting key versions.

```
lunacm:> hagroup synchronize -group <label>
```

- [Optional] If you intend to have the new partition serve as a standby member, see "[Setting an HA Group Member to Standby](#)" on page 356.

## Deleting an HA Group

Use LunaCM to delete an HA group from your configuration.

**NOTE** This procedure only removes the HA group virtual slot; the member partitions and all their contents remain intact. Only the HSM SO can delete individual partitions.

### To delete an HA group

- Stop any applications currently using the HA group.
- Delete the group by specifying its label (see [hagroup listgroups](#)).

```
lunacm:> hagroup deletegroup -label <label>
```

```
lunacm:> hagroup deletegroup -label myHAGroup
```

```
 The HA group myHAGroup was successfully deleted.
```

```
Command Result : No Error
```

## HA Troubleshooting

If you encounter problems with an HA group, refer to this section.

### Administration Tasks on HA Groups

Do not attempt to run administrative tasks on an HA group virtual slot (such as changing the CO password or altering partition policies). These virtual slots are intended for cryptographic operations only. It is not possible to use an HA group to make administrative changes to all partitions in the group simultaneously.

### Unique Object IDs (OUID)

If two applications using the same HA group modify the same object using different members, the object fingerprint might conflict.

<b>Network HSM</b>	<b>Potential HA member partition "A" (serial# 1312151770919)</b>	<b>Potential HA member partition "B" (serial# 1462751259592)</b>
Appliance software	7.7.1	pre-7.7.0
HSM firmware version	7.7.1	pre-7.7.0
FIPS status	non-FIPS	non-FIPS
<b>Network HSM</b>	<b>Potential HA member partition "A" (serial# 1462751259592)</b>	<b>Potential HA member partition "B" (serial# 1312151770919)</b>
Appliance software	pre-7.7.0	7.7.1
HSM firmware version	pre-7.7.0	7.7.1
FIPS status	non-FIPS	non-FIPS
<b>Network HSM</b>	<b>Potential HA member partition "A" (serial# 1312151770919)</b>	<b>Potential HA member partition "B" (serial# 1462751259592)</b>
Appliance software	7.7.1	pre-7.7.0
HSM firmware version	7.7.1	pre-7.7.0
FIPS status	non-FIPS	non-FIPS
<b>Network HSM</b>	<b>Potential HA member partition "A" (serial# 1462751259592)</b>	<b>Potential HA member partition "B" (serial# 1312151770919)</b>
Appliance software	pre-7.7.0	7.7.1
HSM firmware version	pre-7.7.0	7.7.1
FIPS status	non-FIPS	non-FIPS

If two applications using the same HA group modify the same object using different members, the object fingerprint may conflict.

## Client-Side Limitations

New features or abilities, or new cryptographic mechanisms added by firmware update, or previously usable mechanisms that become restricted for security reasons, can have an impact on the working of an HA group, when the Client version is older. Luna Clients are "universal" in the sense that they are able to work fully with current Luna HSMs/partitions, and with earlier versions, as well as with cloud crypto solutions (DPoD Luna Cloud HSM service), but a client version cannot be aware of HSM versions that were not yet developed when the Client was released.

## Client-Side Failures

Any failure of the client (such as operating system problems) that does not involve corruption or removal of files, should resolve itself when the client is rebooted.

If the client workstation seems to be working fine otherwise, but you have lost visibility of the HSMs in LunaCM or your client, try the following remedies:

- > verify that the Thales drivers are running, and retry
- > reboot the client workstation
- > restore your client configuration from backup
- > re-install Luna HSM Client and re-configure the HA group

## Failures Between the HSM Appliance and Client

The only failure that could likely occur between a Luna Network HSM (or multiple HSMs) and a client computer coordinating an HA group is a network failure. In that case, the salient factor is whether the failure occurred near the client or near one (or more) of the Luna Network HSM appliances.

If the failure occurs near the client, and you have not set up port bonding on the client, then the client would lose sight of all HA group members, and the application fails. The application resumes according to its timeouts and error-handling capabilities, and HA resumes automatically if the members reappear within the recovery window that you had set.

If the failure occurs near a Luna Network HSM member of the HA group, then that member disappears from the group until the network failure is cleared, but the client can still see other members, and normal failover occurs.

## Avoid direct access to individual HA group members when securing with STC

This is best ensured by having `HAonly` setting turned ON, in the configuration file, so that only the HA virtual slot is visible and all requests and responses are handled transparently by the HA system ( see "[Configuration File Summary](#)" on page 70 ). If you cannot avoid directly accessing an individual HA member slot, then be sure to *log out of it before your application attempts to use the HA virtual slot*. This is especially important when STC is invoked ( see "[Client-Partition Connections](#)" on page 86 ).

Each HSM keeps track of any appid registered against a remote connection, and rejects any attempt to create a new session with different appID from the same client. That is, only one access ID is permitted per STC channel. If a client opens a session directly to an individual HA member partition, then an ID is assigned. If the client next attempts operation via the HA virtual slot, then as part of that process, random appids are assigned to each member partition for the open channel, but one of those member partitions already has the earlier ID, so the HSM responds with `CKR_ACCESS_ID_ALREADY_EXISTS` and the operation fails.

Log out of any individual member slot, before invoking the HA slot, to avoid this problem.

## Effect of PED Operations

PED operations can block some cryptographic operations, so that while a member of an HA group is performing a PED operation, it could appear to the HA group as a failed member. When the PED operation is complete, failover and recovery HA logic are invoked to return the member to normal operation.

## Updating Luna Network HSM HA Group Members to Luna 7.7.0 or Newer

Luna HSM firmware 7.7.0 and newer includes changes to the Luna cloning protocol that HA groups use to duplicate cryptographic objects among their individual members. These changes make it impossible to support HA groups combining 7.7.0+ and older firmware versions (see ["Cloning Keys Between Luna 6, Luna 7, and Luna Cloud HSM" on page 171](#)). Therefore, all HSMs containing HA group members must be updated to firmware 7.7.0+ at the same time to allow the HA group to continue functioning normally. You can use the following procedures to update your Luna 7 HA group members with minimal service disruption.

**CAUTION!** If your HA group uses STC connections, refer to ["Updating Luna Network HSM with STC Partitions to 7.7.0 or Newer" on page 123](#) before continuing. The upgrade process for STC partitions is destructive of existing key material; you must back up your partitions and then restore them to the updated HA group as described in that procedure.

This procedure differs depending on whether you plan to upgrade your HA group to full eIDAS compliance using V1 partitions, or use V0 partitions to simply gain new features and bug fixes (see ["What are "pre-firmware 7.7.0", and V0, and V1 partitions?" on page 126](#)).

- > ["Updating Luna Network HSM HA Group Members to Luna 7.7.0 + V1 Partitions" below](#)
- > ["Updating Luna Network HSM HA Group Members to Luna 7.7+ V0 partitions" on page 375](#)

### Guidelines and Tips when partitions are part of an HA group

Refer to ["General guidelines for updating or converting of HA member partitions" on page 376](#)

## Updating Luna Network HSM HA Group Members to Luna 7.7.0 + V1 Partitions

To convert your HA group members to V1 partitions, use the following procedure to ensure a minimal amount of application downtime. This procedure is performed by the HSM SO for each Luna Network HSM, the Partition SO and Crypto Officer for the HA group members, and requires **admin**-level access to the Luna Network HSM appliance.

### To update Luna Network HSM HA group members to V1 partitions

1. [Optional] Back up the contents of the HA group members to a Luna Backup HSM capable of restoring objects to V1 partitions. Backup/restore should not be necessary as part of this procedure, but it is good practice in case of equipment failure.
  - ["Backing Up to a Client-Connected Luna Backup HSM \(G7\)" on page 419](#)
  - ["Backing Up to an Appliance-Connected Luna Backup HSM \(G7\)" on page 435](#)

- ["Backup/Restore Using a Client-Connected Luna Backup HSM \(G5\)" on page 401](#)
- ["Backup/Restore Using an Appliance-Connected Luna Backup HSM \(G5\)" on page 397](#)

**NOTE** Once you update the Luna HSM firmware to 7.7.0 or newer, you will require a Luna Backup HSM with minimum firmware version 7.7.1 (G7) or 6.28.0 (G5) to back up and restore partitions. You can use earlier firmware versions to migrate keys to 7.7.0+ partitions.

- > ["Updating the Luna Backup HSM \(G7\) Firmware" on page 449](#)
- > ["Updating the Luna Backup HSM \(G5\) Firmware" on page 395](#)

- Using an SSH or serial connection, log in to one of the Luna Network HSM appliances containing an HA group member partition as **admin** (see [Logging In to LunaSH](#)) and turn off the NTLS service on the appliance.

```
lunash:> service stop ntlis
```

- Update the Luna Network HSM appliance software to 7.7.0 or newer (see [Updating the Luna Network HSM Appliance Software](#)).
- Update the Luna Network HSM firmware (see [Updating the Luna HSM Firmware](#)).
- Confirm that the NTLS service has resumed running on the appliance.

```
lunash:> service status ntlis
```

- Repeat steps 2-5 for each Luna Network HSM containing an HA group member.
- On the client workstation that administers the HA group, stop all client applications.
- Update the Luna HSM Client software to version 10.3.0 or newer (see ["Updating the Luna HSM Client Software" on page 85](#)).
- [Optional] You may now restart your client applications, or wait until the end of the procedure.
- Launch LunaCM and use the following procedure to convert each HA member partition to V1. To prevent the HA group serial number from changing and disrupting your client applications, the member originally used to create the group must be the last member still remaining in the group:

**NOTE** The member partition that has the same serial number as the HA group, minus the leading **1**, is the original member.

- Remove a member partition from the HA group (see ["Adding/Removing an HA Group Member" on page 363](#)).

```
lunacm:> hagroup removemember -group <label> {-slot <slotnum> | -serial <serialnum>}
```

- Log in as Partition SO.

```
lunacm:> role login -name po
```

- Convert the partition to V1 by changing partition policy **41: Partition Version**.

```
lunacm:> partition changepolicy -policy 41 -value 1
```

- Repeat steps **a-c** until only the original member remains in the HA group.

- e. When only the original member remains in the group, log in as Partition SO and convert it to V1. This member's SMK will be the one used for the entire HA group (see ["Scalable Key Storage \(SKS\)" on page 139](#) for more information).

```
lunacm:> role login -name po
```

```
lunacm:> partition changepolicy -policy 41 -value 1
```

- f. Add each V1 partition back to the HA group (see ["Adding/Removing an HA Group Member" on page 363](#)). The primary member's SMK is automatically cloned to each new member added to the HA group.

```
lunacm:> hagroup addmember -group <label> {-slot <slotnum> | -serial <serialnum>}
```

## Updating Luna Network HSM HA Group Members to Luna 7.7+ V0 partitions

To update your HA group members to V0 partitions in Luna 7.7.0 or newer, use the following procedure to ensure a minimal amount of application downtime. This procedure is performed by the HSM SO for each Luna Network HSM, the Crypto Officer for the HA group members, and requires **admin**-level access to the Luna Network HSM appliance.

### To update Luna Network HSM HA group members to V0 partitions

- [Optional] Back up the contents of the HA group members to a Luna Backup HSM capable of restoring objects to Luna 7.7+ partitions.
  - ["Backing Up to a Client-Connected Luna Backup HSM \(G7\)" on page 419](#)
  - ["Backing Up to an Appliance-Connected Luna Backup HSM \(G7\)" on page 435](#)
  - ["Backup/Restore Using a Client-Connected Luna Backup HSM \(G5\)" on page 401](#)
  - ["Backup/Restore Using an Appliance-Connected Luna Backup HSM \(G5\)" on page 397](#)

**NOTE** Once you update the Luna HSM firmware to 7.7.0 or newer, you will require a Luna Backup HSM with minimum firmware version 7.7.1 (G7) or 6.28.0 (G5) to back up and restore partitions. You can use earlier firmware versions to migrate keys to 7.7.0+ partitions.

> ["Updating the Luna Backup HSM \(G7\) Firmware" on page 449](#)

> ["Updating the Luna Backup HSM \(G5\) Firmware" on page 395](#)

- Using an SSH or serial connection, log in to one of the Luna Network HSM appliances containing an HA group member partition as **admin** (see [Logging In to LunaSH](#)) and turn off the NTLS service on the appliance.

```
lunash:> service stop ntlis
```

- Update the Luna Network HSM appliance software to 7.7.0 or newer (see [Updating the Luna Network HSM Appliance Software](#)).
- Update the Luna Network HSM firmware (see [Updating the Luna HSM Firmware](#)).
- Confirm that the NTLS service has resumed running on the appliance.

```
lunash:> service status ntlis
```

- Repeat steps 2-5 for each Luna Network HSM containing an HA group member.

7. [Optional] On the client workstation that administers the HA group, stop all client applications.
8. [Optional] Update the Luna HSM Client software to version 10.3.0 or newer (see "[Updating the Luna HSM Client Software](#)" on page 85).
9. [Optional] You may now restart your client applications.

## General guidelines for updating or converting of HA member partitions

---

For full HA functionality, all members of a working HA group should be identical in firmware version and partition type. For best results, the Client library, that enables HA among several HSM, should be the most current available.

- > Expect HA functionality (with some caveats) when members have been updated, but not *during* firmware update to version 7.7.0 (or newer) or *during* conversion of member partitions from V0 to V1.
- > The kind of HA discussed here, is mediated by the Client library. If you are updating firmware from pre-7.7.0 to version 7.7.0 (or newer), while continuing to use a Client version earlier than 10.3.0, then as your HA group members are converted (by the firmware update) into V0 partitions, note these HA considerations:
  - A V0 partition on an appliance with HSM firmware 7.7.0 (or newer) can be added to an existing HA group that already has HA members made up of partitions from HSM with pre-version-7.7.0 firmware .
    - **ha addMember** command functions as expected.
    - When cloning objects from HSM firmware earlier than 7.7.0 into V0 partition, the size of the object increases.
  - **ha createGroup** functions as expected using V0 partition.
  - **ha deleteGroup** functions as expected on a HA group containing V0 partition.
  - A V0 partition on an appliance with HSM firmware 7.7.0 (or newer) can be removed from an existing HA group.
    - **ha removeMember** command functions as expected.
  - A V0 partition on an appliance with HSM firmware 7.7.0 (or newer) can be added as a standby member of an existing HA group.
    - **ha addStandby** command functions as expected.
  - After a V0 partition on an appliance with HSM firmware 7.7.0 (or newer) is added as a member of an existing HA group, it can be synchronized with other members of the HA group.
    - **ha synchronize** command functions as expected.
    - As described in **ha addMember** section above, synchronization from partition in pre-7.7.0-firmware HSM to V0 partition may fail due to storage limitation.
  - When V0 partition in a HA group becomes a primary partition, synchronization with other members on a pre-7.7.0-firmware HSM is not supported.
  - V1 partition can be added to an existing HA group that already has HA members made up of partitions from a pre-7.7.0-firmware HSM. However, when V1 partition becomes the primary member of the HA group, synchronization with remaining member of the HA group will no longer function.



- > Cloning of keys and objects can proceed only from a lower-security environment (in this context, pre-7.7.0) to a higher-security environment (firmware 7.7.0 or newer), but not in the other direction.
- > Members of HA groups must all be at the same level. Perform an update from pre-7.7.0 firmware to 7.7.0 (or newer) - which invokes conversion of partitions to V0 as an effect of the update - while the partition is *not* a member of an HA group.
- > An HA group with V1 partitions must have all members at V1 and all members sharing the same SMK.
- > A V1 partition cannot be a member of more than one HA group unless both groups have the same SMK.
- > An HA group with V0 partitions should have all members at V0; the new, more secure cloning protocol, and changes to key attributes mean that attempting to mix pre-firmware-7.7.0 partitions with V0 partitions is not recommended and would not work as expected.
- > If a member of an existing HA group is added to a different HA group with a different SMK, the new member takes on the SMK of the new HA group and ceases to function properly in its original group (and should be removed).
- > Converting a partition from V0 to V1 preserves contents, and should be done while the partition is *not* in an HA group.
- > Converting a partition from V1 to V0 is destructive, so the partition cannot remain an HA member.
- > Similarly, cloning of keys and objects can proceed from partitions of an HSM that has had Functionality Modules enabled into partitions that have never had Functionality Modules enabled, but not in the other direction. Again, firmware updates should take place outside of HA groups.

**NOTE** Remove/ stop all ongoing operations with HA and update-or-convert members one at a time, leaving the primary member for last. Then resume using the HA group with all members now updated or converted.

**TIP**

An HA group functions properly when all member partitions are V0 (and the same firmware version), or an HA group functions properly when all member partitions are V1 (and the same firmware version), but it is generally best to not mix partition types in an HA group.

An HA group functions properly when all members are FM-enabled, or all members are FM-never-enabled, but not some of each.

## Avoid direct access to individual HA group members when securing with STC

This is best ensured by having `HAonly` setting turned ON, in the configuration file, so that only the HA virtual slot is visible and all requests and responses are handled transparently by the HA system ( see "[Configuration File Summary](#)" on page 70 ). If you cannot avoid directly accessing an individual HA member slot, then be sure to *log out of it before your application attempts to use the HA virtual slot*. This is especially important when STC is invoked ( see "[Client-Partition Connections](#)" on page 86 ).

Each HSM keeps track of any appid registered against a remote connection, and rejects any attempt to create a new session with different appID from the same client. That is, only one access ID is permitted per STC channel. If a client opens a session directly to an individual HA member partition, then an ID is assigned. If the

client next attempts operation via the HA virtual slot, then as part of that process, random appids are assigned to each member partition for the open channel, but one of those member partitions already has the earlier ID, so the HSM responds with `CKR_ACCESS_ID_ALREADY_EXISTS` and the operation fails.

Log out of any individual member slot, before invoking the HA slot, to avoid this problem.

# CHAPTER 14: Backup and Restore Using a Luna Backup HSM (G5)

Luna Network HSM allows secure creation, storage, and use of cryptographic data (keys and other objects). It is critically important, however, to safeguard your important cryptographic objects against unforeseen damage or data loss. No device can offer total assurance against equipment failure, physical damage, or human error. Therefore, a comprehensive strategy for making regular backups is essential. There are multiple ways to perform these operations, depending on your implementation.

This section contains the following information:

- > ["Backup and Restore Best Practices" below](#)
- > ["Planning Your Backup HSM Deployment" on the next page](#)
- > ["About the Luna Backup HSM \(G5\)" on page 383](#)
- > ["Installing the Backup HSM" on page 387](#)
- > ["Installing or Replacing the Luna Backup HSM \(G5\) Battery" on page 388](#)
- > ["Backup HSM Secure Transport and Tamper Recovery" on page 390](#)
- > ["Resetting the Backup HSM to Factory Conditions" on page 397](#)
- > ["Backup/Restore Using an Appliance-Connected Luna Backup HSM \(G5\)" on page 397](#)
- > ["Backup/Restore Using a Client-Connected Luna Backup HSM \(G5\)" on page 401](#)
- > ["Configuring a Remote Luna Backup HSM \(G5\) Server" on page 406](#)

## Backup and Restore Best Practices

To ensure that your data is protected in the event of a failure or other catastrophic event, Thales recommends that you use the following best practices as part of a comprehensive backup strategy:

**CAUTION!** Failure to develop and exercise a comprehensive backup and recovery plan may prevent you from being able to recover from a catastrophic event. Although Thales provides a robust set of backup hardware and utilities, we cannot guarantee the integrity of your backed-up key material, especially if stored for long periods. Thales strongly recommends that you exercise your recovery plan at least semi-annually (every six months) to ensure that you can fully recover your key material.

### Develop and document a backup and recovery plan

This plan should include the following:

- > What is being backed up
- > The backup frequency

- > Where the backups are stored
- > Who is able to perform backup and restore operations
- > Frequency of exercising the recovery test plan

### Make multiple backups

To ensure that your backups are always available, build redundancy into your backup procedures.

### Use off-site storage

In the event of a local catastrophe, such as a flood or fire, you might lose both your working HSMs and locally-stored backup HSMs. To fully protect against such events, always store a copy of your backups at a remote location.

### Regularly exercise your disaster recovery plan

Execute your recovery plan at least semi-annually (every six months) to ensure that you can fully recover your key material. This involves retrieving your stored Backup HSMs and restoring their contents to a test partition, to ensure that the data is intact and that your recovery plan works as documented.

## Planning Your Backup HSM Deployment

When setting up your backup deployment, you have multiple configuration options. This section will help you choose the right configuration for your organization, depending on where you prefer to keep your backups. You can use a Luna Backup HSM or an application partition on any other Luna HSM for backup/restore operations.

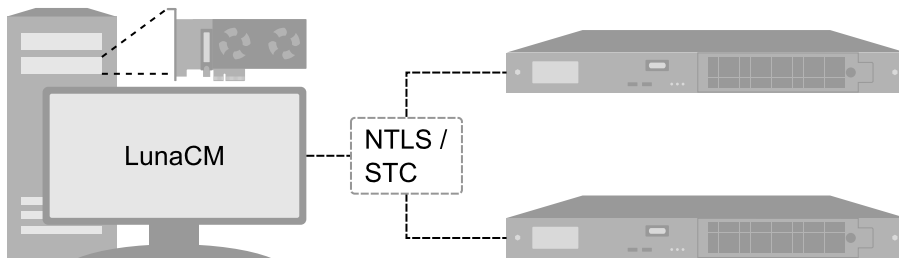
Backup and restore operations require that cloning be enabled on the HSM/partition.

- > ["Partition to Partition" below](#)
- > ["Backup HSM Connected to the Appliance" on the next page](#)
- > ["Backup HSM Connected to the Client Workstation" on the next page](#)
- > ["Backup HSM Installed Using Remote Backup Service \(RBS\)" on page 382](#)

**NOTE** The diagrams below depict the client workstation as the remote PED server, but you can also use a separate remote PED station. Since remote PED is supported on Windows clients only, this will be necessary if you use Linux/UNIX clients.

### Partition to Partition

You can clone objects from any Luna 7 application partition to any other Luna 7 partition that shares its cloning domain. You must have the Crypto Officer credential for both partitions. Both partitions must use the same authentication method (either password or PED).

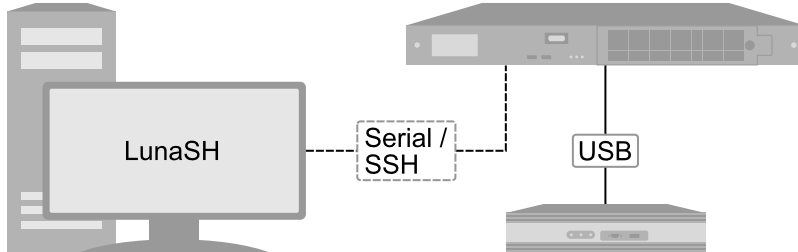


See ["Cloning Objects to Another Application Partition"](#) on page 170.

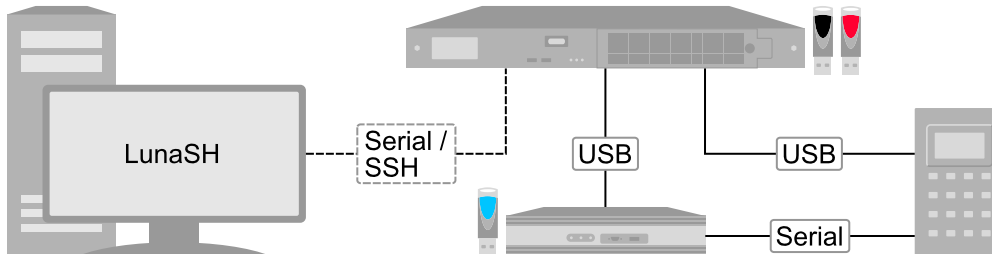
## Backup HSM Connected to the Appliance

In this configuration, the Luna Backup HSM is connected directly to one of the USB ports on the Luna Network HSM appliance. It is useful in deployments where backups are kept in the same location as the HSM. Backup and restore operations are performed using LunaSH commands via a serial or SSH connection. The Crypto Officer must have **admin**-level access to LunaSH on the appliance to use this configuration.

**Figure 1: Locally-connected Backup HSM using password authentication**



**Figure 2: Locally-connected Backup HSM using local PED authentication**

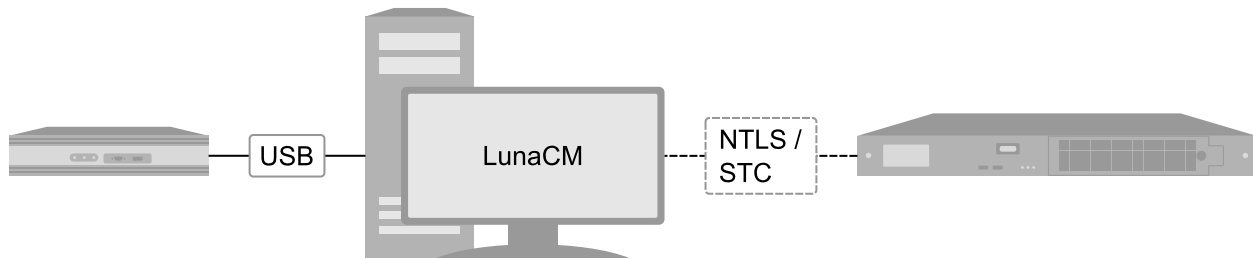
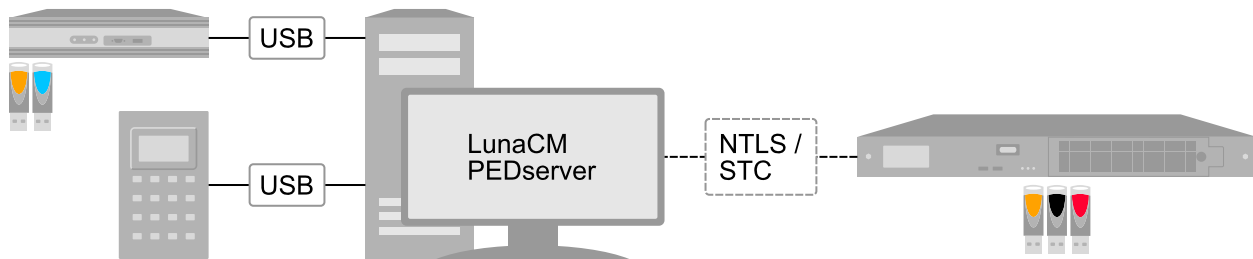


**NOTE** This configuration cannot be used to back up or restore a partition that uses an STC connection. STC partitions must be backed up at the client using LunaCM. This configuration cannot be used with Remote PED.

See ["Backup/Restore Using an Appliance-Connected Luna Backup HSM \(G5\)"](#) on page 397.

## Backup HSM Connected to the Client Workstation

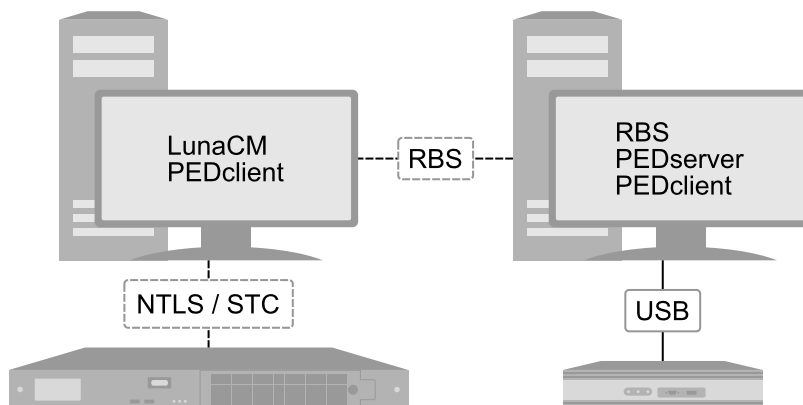
In this configuration, the Luna Backup HSM is connected to a USB port on the client workstation. It is useful in deployments where the partition Crypto Officer keeps backups at the client. This allows you to perform backup/restore operations for all application partitions that appear as visible slots in LunaCM. You can restore a partition backup to the original source partition or to another existing Luna application partition that shares the same cloning domain.

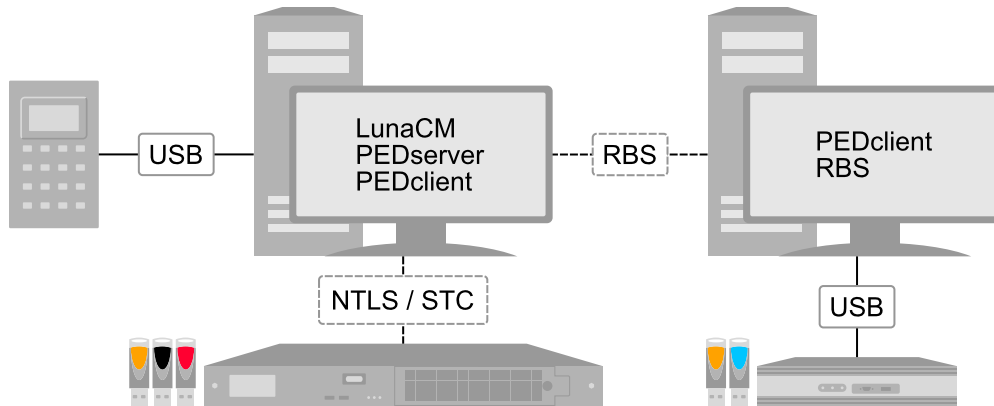
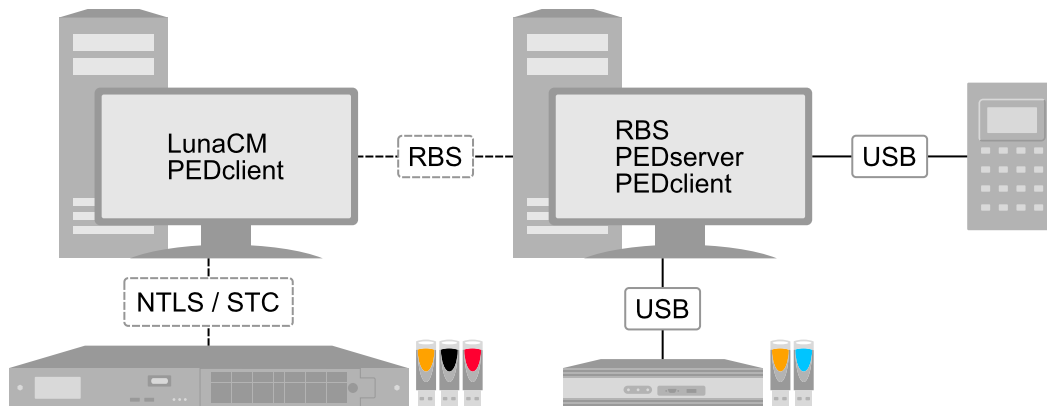
**Figure 3: Client-connected backup HSM using password authentication****Figure 4: Client-connected backup HSM using remote PED authentication**

See ["Backup/Restore Using a Client-Connected Luna Backup HSM \(G5\)"](#) on page 401.

## Backup HSM Installed Using Remote Backup Service (RBS)

In this configuration, the Luna Backup HSM is connected to a remote client workstation that communicates with the client via the Remote Backup Service (RBS). It is useful in deployments where backups are stored in a separate location from the Luna Network HSM, to mitigate the consequences of catastrophic loss (fire, flood, etc).

**Figure 5: Remote backup (RBS) using password authentication**

**Figure 6: Remote backup (RBS) using remote PED authentication at the client****Figure 7: Remote backup (RBS) using remote PED authentication at the RBS server**

See ["Configuring a Remote Luna Backup HSM \(G5\) Server"](#) on page 406.

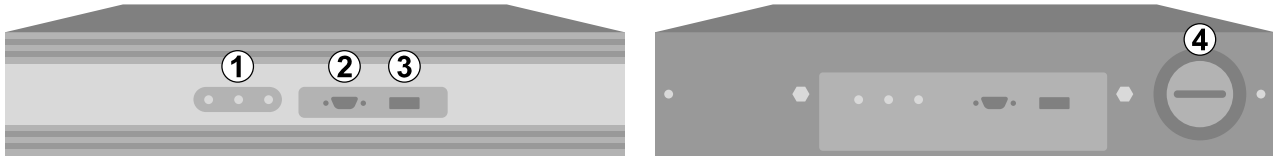
## About the Luna Backup HSM (G5)

The Luna Backup HSM (G5) allows you to safeguard your important cryptographic objects by making secure backups, and restoring those backups to an application partition. It uses the Luna G5 architecture. This section contains the following information about the Luna Backup HSM (G5):

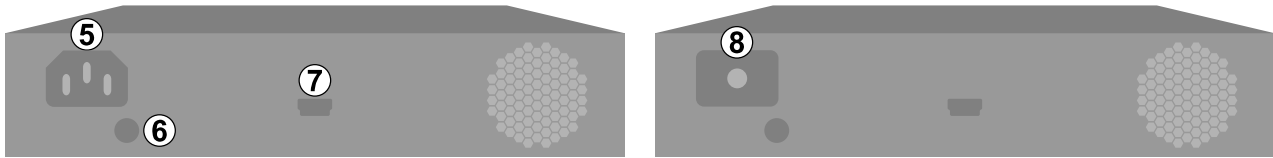
- > ["Physical Features" on the next page](#)
- > ["Luna Backup HSM \(G5\) Functionality" on the next page](#)
- > ["Storage and Maintenance" on page 385](#)
- > ["Installing the Backup HSM" on page 387](#)
- > ["Installing or Replacing the Luna Backup HSM \(G5\) Battery" on page 388](#)
- > ["Backup HSM Secure Transport and Tamper Recovery" on page 390](#)
- > ["Initializing the Backup HSM Remote PED Vector" on page 393](#)
- > ["Resetting the Backup HSM to Factory Conditions" on page 397](#)

## Physical Features

The front panel of the Luna Backup HSM (G5) is illustrated below, with important features labeled. In the second image, the front bezel has been removed, exposing the battery enclosure.



The rear panel of the Luna Backup HSM (G5) is illustrated below, with important features labeled. The first image depicts a Backup HSM with an internal power supply. The second image depicts one that ships with an external power supply.



1	<p>Status LEDs. When illuminated, they indicate:</p> <ul style="list-style-type: none"> <li>&gt; <b>Active:</b> The Backup HSM is performing a procedure. Do not disconnect or unplug the device when this light is illuminated.</li> <li>&gt; <b>Tamper:</b> The Backup HSM is in a tamper state. You must clear the tamper state before backing up or restoring partitions.</li> <li>&gt; <b>Error:</b> HSM device driver error. Contact Thales Customer Support (see <a href="#">"Support Contacts" on page 16</a>).</li> </ul>
2	Serial port for attaching a local Luna PED using a 9-pin Micro-D to Micro-D cable.
3	USB port. Not applicable to backup/restore functions.
4	Battery enclosure. See <a href="#">"Installing or Replacing the Luna Backup HSM (G5) Battery" on page 388</a> .
5	Power connector for a Luna Backup HSM with an internal power supply. See <a href="#">"Storage and Maintenance" on the next page</a> for more information.
6	Index hole. Engages with the index post on a Luna Backup HSM rack shelf.
7	Mini-USB port for connecting the Luna Backup HSM to a Luna HSM or client workstation. See <a href="#">"Installing the Backup HSM" on page 387</a> .
8	Power source connector for a Luna Backup HSM (G5) with an external power supply (included).

## Luna Backup HSM (G5) Functionality

The Luna Backup HSM allows you to back up application partitions from one or more Luna General Purpose HSMs. Backup operations are performed on a per-partition basis.



## Password or PED Authentication

The Luna Backup HSM (G5) can be configured to back up either password- or PED-authenticated partitions. You must specify the authentication method when you initialize the Luna Backup HSM (see ). Once initialized, the Backup HSM can only be used with partitions sharing the same authentication type. The only way to change the authentication method is to restore the Backup HSM to factory condition and re-initialize it.

## Storage Capacity and Maximum Allowable Backup Partitions

The storage capacity and maximum number of backup partitions allowed on the Backup HSM is determined by the firmware. You can check the capacity using `lunash:>token backup show -serial <serialnum>` or `lunacm:> hsm showinfo`. To update the Backup HSM firmware to a version that allows more backups, see ["Updating the Luna Backup HSM \(G5\) Firmware" on page 395](#).

**NOTE** Objects stored on a Backup HSM may be smaller than their originals. For example, symmetric keys are 8 bytes smaller when stored on a Backup HSM. This size difference has no effect on backup and restore operations.

## Storage and Maintenance

The Luna Backup HSM can be safely stored, containing backups, when not in use. When stored properly, the hardware has a lifetime of 10+ years. Newer Backup HSMs ship with an external power supply.

**CAUTION!** The internal power supply on older Luna Backup HSMs uses capacitors that may be affected if they are left unpowered for extended periods of time. If your Backup HSM has an internal power supply, power it on occasionally to recharge the capacitors. If the capacitors lose function, the Backup HSM will no longer receive power. With the introduction of external power supplies, this is no longer a requirement. If the external power supply fails from being left unpowered, it can be easily replaced.

## The Backup HSM Battery

The battery powers the NVRAM and Real-Time-Clock (RTC), and must be installed for use. The battery can be removed for storage, and this is generally good practice. Thales uses high-quality, industrial-grade batteries that are unlikely to leak and damage the HSM hardware, but an externally-stored battery will last longer. The battery must be stored in a clean, dry area (less than 30% Relative Humidity). Temperature should not exceed +30 °C. When properly stored, the battery has a shelf life of 10 years.



If the battery dies or is removed, and the main power is not connected, NVRAM and the RTC lose power. Battery removal triggers a tamper event. After replacing the battery, the HSM SO must clear the tamper event before operation can resume. The working copy of the Master Tamper Key (MTK) is lost (see ["Backup HSM Secure Transport and Tamper Recovery" on page 390](#)). Backup objects are stored in non-volatile memory, so they are preserved and remain uncorrupted.


There is no low battery indicator, or other provision for checking the battery status. The voltage remains constant until the very end of battery life.

## Luna Backup HSM (G5) Required Items

This section provides a list of the components you should have received with your Luna Backup HSM (G5) order.

### Luna Backup HSM (G5) Order Items

Qty	Item
1	<p><b>Luna Backup HSM (G5)</b></p>  <p>The image shows a black, rectangular Luna Backup HSM (G5) device. The front panel features the Gemalto logo on the left, followed by a small display area with 'Active Target Error' and 'PED' indicators, and a USB port on the right. The text 'SafeNet Remote Backup HSM' is printed on the bottom right of the front panel.</p>
1	<p><b>External Power Supply</b></p> <p>The Luna Backup HSM (G5) now ships with an external power supply. Previously, these HSMs relied on an internal power supply, requiring the HSM to be periodically powered on to recharge internal capacitors. Failure to charge the capacitors could result in an inability to power on the HSM.</p> <p>With the introduction of external power supplies, periodically powering on the HSM is no longer required. A failed external power supply can be replaced and there is no need to return the HSM for repair (RMA).</p> <div style="border: 1px solid black; padding: 5px; margin-top: 10px;"> <p><b>NOTE</b> External power supplies do contain capacitors which may be affected by extended periods of being unpowered, but they are more easily replaced in the event of failure.</p> </div>
1	<p><b>Power Supply Cord</b></p> <p>Your order should include one power supply cord for the Luna Backup HSM (G5). The actual cord received depends on the country for which you ordered the Luna Backup HSM (G5).</p>  <p>The image shows two power supply cords. The cord on the left is a standard three-prong AC power cord with a black plastic housing. The cord on the right is a power supply cord with a blue plastic housing and a three-prong AC power plug.</p>

Qty	Item
1	<p data-bbox="245 268 683 298"><b>USB cable (USB A to USB mini B)</b></p>  <p data-bbox="245 772 932 802">Your order should include one USB A to 5-pin (Mini-B) cable.</p>

## Optional Items

Your order may also include the following optional item.

### Luna Backup HSM (G5) Rack-Mount Shelf

The Luna Backup HSM (G5) rack-mount shelf (available by separate order) fits a standard 19-inch equipment rack, allowing you to install up to two Luna Backup HSM (G5) units side-by-side in server-room racks. For office use, without rack mounting, Luna Backup HSM (G5) units can be placed on a desktop and are stackable.

## Installing the Backup HSM

You can connect the Luna Backup HSM to a Luna Network HSM, a Luna HSM Client workstation, or a host machine containing a Luna PCIe HSM. Refer to ["Planning Your Backup HSM Deployment" on page 380](#) for detailed descriptions of the configuration options.

### To install the Luna Backup HSM

1. Connect the Luna Backup HSM to power using the external power source or a standard power cable.
2. If you are connecting the Backup HSM to a client workstation or PCIe HSM host, ensure that you have installed the **Backup** option in the Luna HSM Client installer (see ["Luna HSM Client Software Installation" on page 17](#) for details).
3. [Local PED] If you plan to authenticate the Luna Backup HSM with a local Luna PED, connect the PED using a 9-pin Micro-D to Micro-D cable (see ["Physical Features" on page 384](#)).  
To use the same local PED to authenticate both the Backup HSM and Luna Network HSM, connect the PED to the Luna Network HSM using a USB Mini-B to USB cable (see ["Physical Features" on page 186](#)). You can switch between the two using PED modes (see ["Modes of Operation" on page 188](#)).
4. Connect the Luna Backup HSM using the included Mini-USB to USB cable. If you are connecting the Backup HSM to:

- a. **Luna Network HSM:** Connect to one of the USB ports on the front or rear panel of the appliance.
  - b. **Luna HSM Client:** Connect to a USB port on the client workstation.
  - c. **Luna PCIe HSM host:** Connect to a USB port on the host workstation.
5. If your Backup HSM was shipped in Secure Transport Mode, see ["Backup HSM Secure Transport and Tamper Recovery"](#) on page 390.

## Installing or Replacing the Luna Backup HSM (G5) Battery

The Luna Backup HSM (G5) must have a functioning battery installed to preserve the NVRAM and RTC in case of primary power loss. You can purchase a replacement battery from any supplier who can match the following specifications:

- > 3.6 V Primary lithium-thionyl chloride (Li-SOCl<sub>2</sub>)
- > Fast voltage recovery after long term storage and/or usage
- > Low self discharge rate
- > 10 years shelf life
- > Operating temperature range -55 °C to +85 °C
- > U.L. Component Recognition, MH 12193

### Prerequisites

- > Removing the battery causes a tamper event. If you have created a Secure Recovery Vector (purple PED key) and enabled Secure Recovery, you will need this key to clear the tamper after replacing the battery.

### To install or replace the Luna Backup HSM (G5) battery

1. Remove the front bezel. It is held in place by two spring clips.



2. The battery compartment is spring-loaded and can be removed without much pressure. Use a coin or your fingers to press in the compartment cover and turn counter-clockwise to remove it.



3. If you are replacing the old battery, remove it from the battery compartment.



4. Insert the new battery, negative end first. The positive end should be visible.



- Use the battery compartment cover to push the battery into the compartment, aligning the tabs on the cover with the compartment slots. Twist the cover clockwise to lock the compartment.



- Replace the front bezel by aligning the clips with their posts and pushing it into place. Removing the battery causes a tamper event on the Luna Backup HSM (G5).
- To clear the tamper, see "[Backup HSM Secure Transport and Tamper Recovery](#)" below.

## Backup HSM Secure Transport and Tamper Recovery

The Luna Backup HSM recognizes a similar list of tamper conditions to the Luna Network HSM (see [Tamper Events](#)). When a tamper event occurs, a tamper state is reported in the **HSM Status** field in LunaCM's list of slots.

By default, tamper events are cleared automatically when you reboot the Backup HSM and log in as HSM SO. However, you can choose to prevent any further operations on the Backup HSM. The following procedures will allow you to create a purple Secure Recovery Key (SRK) that the Backup HSM SO must present to unlock the HSM after a tamper event. This key contains part of the Master Tamper Key (MTK), which encrypts all sensitive data stored on the Backup HSM. By splitting the MTK and storing part of it on an SRK (purple PED key), you ensure that none of the stored material can be accessible until the SRK is presented.

You can create the purple SRK even for a Backup HSM that is initialized for password authentication. There is no password-based SRK equivalent; you must have a Luna PED and a purple PED key to use Secure Tamper Recovery and Secure Transport Mode.

Initializing the SRK also allows you to place the Backup HSM in Secure Transport Mode (STM). STM on the Backup HSM functions differently from STM on the Luna Network HSM (see "[Secure Transport Mode](#)" on [page 1](#) for comparison). When the SRK is initialized and secure recovery enabled, STM on the Backup HSM is effectively a voluntary tamper state, where no operations are possible until you present the purple PED key.

**CAUTION!** Always keep a securely-stored backup copy of the purple PED key. If you lose this key, the Backup HSM is permanently locked and you will have to obtain an RMA for the Backup HSM.

This section provides directions for the following procedures:

- > ["Creating a Secure Recovery Key" below](#)
- > ["Setting Secure Transport Mode" on the next page](#)
- > ["Recovering From a Tamper Event or Secure Transport Mode" on the next page](#)
- > ["Disabling Secure Recovery" on page 393](#)

## Creating a Secure Recovery Key

To enable secure recovery, you must create the Secure Recovery Key (purple PED key). This procedure will zeroize the SRK split on the Backup HSM, so that you must present the purple PED key to recover from a tamper event or Secure Transport Mode.

### Prerequisites

- > Install the Backup HSM at the client and connect it to power (see ["Installing the Backup HSM" on page 387](#)). This procedure is only available using LunaCM. If the Backup HSM is connected directly to a Luna Network HSM, disconnect it and connect it to a workstation with Luna HSM Client software installed.
- > You require the Backup HSM SO credential (blue PED key).
- > Ensure that the Backup HSM can access PED service (Local or Remote PED), and that you have enough blank or rewritable purple PED keys available for your desired authentication scheme (see ["Creating PED Keys" on page 224](#)).
  - [Local PED] Connect the PED using a 9-pin Micro-D to Micro-D cable. Set the PED to **Local PED-SCP** mode (see ["Modes of Operation" on page 188](#)).
  - [Remote PED] Set up a Remote PED server to authenticate the Backup HSM (see [Remote PED Setup](#)).
  - [Remote PED] Initialize the Backup HSM RPV (see ["Initializing the Backup HSM Remote PED Vector" on page 393](#)). You require the orange PED key.

### To create a Secure Recovery Key

1. Launch LunaCM on the client workstation.

2. Set the active slot to the Luna Backup HSM.

```
lunacm:> slot set -slot <slotnum>
```

3. [Remote PED] Connect the Backup HSM to the Remote PED server.

```
lunacm:> ped connect -ip <PEDserver_IP> -port <portnum>
```

4. Create a new split of the MTK on the Backup HSM.

```
lunacm:> srk generate
```

5. Log in as Backup HSM SO.

```
lunacm:> role login -name so
```

6. Enable secure recovery.

```
lunacm:> srk enable
```

Attend to the Luna PED prompts to create the purple PED key. Secure Recovery is now enabled on the Backup HSM.



## Setting Secure Transport Mode

The following procedure will allow you to set Secure Transport Mode on the Backup HSM.

### Prerequisites

- > Ensure the Backup HSM can access PED services.
- > Secure Recovery must be enabled on the Backup HSM (see ["Creating a Secure Recovery Key" on the previous page](#)). You require the Secure Recovery Key (purple PED key) for the Backup HSM.

### To set Secure Transport Mode on the Backup HSM

1. Launch LunaCM on the client workstation.
2. Set the active slot to the Luna Backup HSM.  
lunacm:> **slot set -slot** <slotnum>
3. [Remote PED] Connect the Backup HSM to the Remote PED server.  
lunacm:> **ped connect -ip** <PEDserver\_IP> **-port** <portnum>
4. Set Secure Transport Mode.  
lunacm:> **srk transport**
  - a. You are prompted for the SRK (purple PED key). This is to ensure that you have the key that matches the SRK split on the HSM.
  - b. The Luna PED displays a 16-digit verification code. Write this code down as an additional optional check.  
The SRK is zeroized on the Backup HSM and STM is now active.

## Recovering From a Tamper Event or Secure Transport Mode

With Secure Recovery Mode enabled, the procedure to recover from a tamper event or to exit STM is the same.

### Prerequisites

- > Ensure the Backup HSM can access PED services.
- > You require the Secure Recovery Key (purple PED key) for the Backup HSM.
- > If you are recovering from a tamper event, reboot the Backup HSM and LunaCM before recovering.

lunacm:> **hsm restart**

lunacm:> **clientconfig restart**

### To recover from a tamper event or exit STM

1. Launch LunaCM on the client workstation.
2. Set the active slot to the Luna Backup HSM.  
lunacm:> **slot set -slot** <slotnum>
3. [Remote PED] Connect the Backup HSM to the Remote PED server.  
lunacm:> **ped connect -ip** <PEDserver\_IP> **-port** <portnum>



#### 4. Recover the Backup HSM from the tamper event or STM.

```
lunacm:> srk recover
```

Attend to the Luna PED prompts:

- a. You are prompted for the SRK (purple PED key).
- b. [STM] The Luna PED displays a 16-digit verification code. If this code matches the one that was presented when you set STM, you can be assured that the Backup HSM has remained in STM since then.

The Backup HSM is recovered from the tamper/STM state and you can resume backup/restore operations.

## Disabling Secure Recovery

To disable secure recovery, you must present the Secure Recovery Key (purple PED key) so that it can be stored on the Backup HSM. You will no longer need to present the purple key to recover from a tamper event.

### Prerequisites

- > Ensure the Backup HSM can access PED services.
- > You require the Secure Recovery Key (purple PED key) for the Backup HSM.

### To disable secure recovery

1. Launch LunaCM on the client workstation.
2. Set the active slot to the Luna Backup HSM.
3. [Remote PED] Connect the Backup HSM to the Remote PED server.

```
lunacm:> slot set -slot <slotnum>
```

```
lunacm:> ped connect -ip <PEDserver_IP> -port <portnum>
```

4. Log in as Backup HSM SO.

```
lunacm:> role login -name so
```

5. Disable secure recovery.

```
lunacm:> srk disable
```

You are prompted for the SRK (purple PED key).

## Initializing the Backup HSM Remote PED Vector

The Remote PED (via PEDserver) authenticates itself to the Luna Backup HSM with a randomly-generated encrypted value stored on an orange PED key. The orange key proves to the HSM that the Remote PED is authorized to perform authentication. The Backup HSM SO can create this key using LunaCM (connected to a client workstation) or LunaSH (connected to a Luna Network HSM appliance).

If the Backup HSM is already initialized, the HSM SO must log in to complete this procedure.

### Prerequisites

- > Luna PED with firmware 2.7.1 or newer

- > USB mini-B to USB-A connector cable
- > Luna PED DC power supply (if included with your Luna PED)
- > Blank or reusable orange PED key (or multiple keys, if you plan to make extra copies or use an M of N security scheme). See ["Creating PED Keys" on page 224](#) for more information.
- > Install the Backup HSM at the client/appliance and connect it to power (see ["Installing the Backup HSM" on page 387](#)).
- > If you are using LunaSH, the Backup HSM must be initialized first (see ["Initializing the Backup HSM" on page 398](#)).
- > Connect the PED to the Backup HSM using a 9-pin Micro-D to Micro-D cable. Set the PED to **Local PED-SCP** mode (see ["Modes of Operation" on page 188](#)).

### To initialize the RPV and create the orange PED key using LunaCM

1. Launch LunaCM on the client workstation.
2. Set the active slot to the Backup HSM.  
lunacm:> **slot set -slot** <slotnum>
3. If the Backup HSM is initialized, log in as HSM SO. If not, continue to the next step.  
lunacm:> **role login -name so**
4. Ensure that you have the orange PED key(s) ready. Initialize the RPV.  
lunacm:> **ped vector init**
5. Attend to the Luna PED and respond to the on-screen prompts. See ["Creating PED Keys" on page 224](#) for a full description of the key-creation process.

```
SLOT
SETTING RPV...
Would you like to
reuse an existing
keyset?(Y/N)
```

- If you have an orange PED key with an existing RPV that you wish to use for this HSM, press **Yes**.
- If you are creating a new RPV, press **No**.

```
SLOT
SETTING RPV...
Insert a
RPK / Remote
PED Key (ORANGE)
Press ENTER.
```

Continue following the prompts for PED PIN, M of N, and duplication options.

To set up a Remote PED server, see ["Installing PEDserver and Setting Up the Remote Luna PED" on page 200](#).

## To initialize the RPV and create the orange PED key using LunaSH

**NOTE** This procedure requires appliance software version 7.7.0 or newer.

1. Log in to LunaSH as **admin**, or an **admin**-level custom user.
2. [Optional] View the Luna Backup HSMs currently connected to the appliance and find the correct serial number.  

```
lunash:> token backup list
```
3. Log in as HSM SO.  

```
lunash:> token backup login -serial <serialnum>
```
4. Ensure that you have the orange PED key(s) ready. Initialize the RPV by specifying the Backup HSM serial number.  

```
lunash:> hsm ped vector init -serial <serialnum>
```
5. Attend to the Luna PED and respond to the on-screen prompts. See ["Creating PED Keys" on page 224](#) for a full description of the key-creation process.

```
SLOT
SETTING RPV...
Would you like to
reuse an existing
keyset? (Y/N)
```

- If you have an orange PED key with an existing RPV that you wish to use for this HSM, press **Yes**.
- If you are creating a new RPV, press **No**.

```
SLOT
SETTING RPV...
Insert a
RPK / Remote
PED Key (ORANGE)
Press ENTER.
```

To set up a Remote PED server, see ["Installing PEDserver and Setting Up the Remote Luna PED" on page 200](#).

## Updating the Luna Backup HSM (G5) Firmware

To update the firmware on a Luna Backup HSM (G5), use LunaCM on a client computer that is connected to the Luna Backup HSM. You require:

- > Luna Backup HSM (G5) firmware update file (<filename>.**fuf**)
- > the firmware update authentication code file(s) (<filename>.**txt**)

**CAUTION!** Use an uninterruptible power supply (UPS) to power your HSM. There is a small chance that a power failure during an update could leave your HSM in an unrecoverable condition.

**NOTE** To perform backup operations on HSM firmware 7.7.0 or newer (V0 or V1 partitions):

- > Luna Backup HSM (G7) requires minimum firmware version 7.7.1
- > Luna Backup HSM (G5) requires minimum firmware version 6.28.0

You can use a Luna Backup HSM with older firmware to restore objects to a V0 or V1 partition, but this is supported for purposes of getting your objects from the older partitions onto the newer V0 or V1 partitions only.

V0 and V1 partitions are considered more secure than partitions at earlier firmware versions - any attempt to restore from a higher-security status to lower-security status fails gracefully.

SMK backup for appliance is supported only with local connection.

### To update the Luna Backup HSM (G5) firmware

1. Copy the firmware file (<filename>.fuf) and the authentication code file (<filename>.txt) to the Luna HSM Client root directory.
  - Windows: C:\Program Files\SafeNet\LunaClient
  - Linux: /usr/safenet/lunaclient/bin
  - Solaris: /opt/safenet/lunaclient/bin

**NOTE** On some Windows configurations, you might not have authority to copy or unzip files directly into **C:\Program Files\...** If this is the case, put the files in a known location that you can reference in a LunaCM command.

2. Launch LunaCM.
3. If more than one HSM is installed, set the active slot to the Admin partition of the HSM you wish to update.
 

```
lunacm:> slot set -slot <slot_number>
```
4. Log in as HSM SO. Depending on the currently-installed firmware version, use one of the following two commands:
  - lunacm:> **role login -name so**
  - lunacm:> **hsm login**
5. Apply the new firmware update by specifying the update file and the authentication code file. If the files are not located in the Luna HSM Client root directory, specify the filepaths.

```
lunacm:> hsm updatefw -fuf <filename>.fuf -authcode <filename>.txt
```

## Resetting the Backup HSM to Factory Conditions

These instructions will allow you to restore your Luna Backup HSM to its original factory conditions, erasing its contents. This could be necessary if you have old backups that you do not wish to keep, or if you want to re-initialize the Backup HSM to store backups using a different authentication method (password or PED). If you have performed firmware updates, they are unaffected. Factory reset can be performed via LunaSH or LunaCM, depending on your Backup HSM deployment.

### To reset the Backup HSM to factory conditions using LunaSH

1. Log in to LunaSH as **admin** or an **admin**-level custom user using a local serial connection.
2. [Optional] View the Luna Backup HSMs currently connected to the appliance and find the correct serial number.

```
lunash:> token backup list
```

3. Reset the Backup HSM by specifying its serial number.

```
lunash:> token backup factoryreset -serial <Backup_HSM_serialnum>
```

### To reset the Backup HSM to factory conditions using LunaCM

1. Launch LunaCM on the Luna Backup HSM host workstation.
2. Set the active slot to the Backup HSM.

```
lunacm:> slot set -slot <slotnum>
```

3. Reset the Backup HSM.

```
lunacm:> hsm factoryreset
```

## Backup/Restore Using an Appliance-Connected Luna Backup HSM (G5)

You can connect the Luna Backup HSM directly to one of the USB ports on the Luna Network HSM appliance. This configuration allows you to perform backup/restore operations using LunaSH, via a serial or SSH connection to the appliance. It is useful in deployments where backups are kept in the same location as the HSM. The Crypto Officer must have **admin**-level access to LunaSH on the appliance. You can restore a partition backup to the original source partition or to another existing Luna application partition that shares the same cloning domain.

**NOTE** Please note the following conditions for using an appliance-connected Luna Backup HSM (G5):

- > If you are backing up or restoring encrypted blobs stored on a V1 partition, the Backup HSM must be connected to the client (see ["Backup/Restore Using a Client-Connected Luna Backup HSM \(G5\)" on page 401](#)). Only the SMK can be backed up/restored using an appliance-connected Backup HSM.
- > If partition policy **37: Force Secure Trusted Channel** is enabled on the partition, the Backup HSM must be connected to the client (see ["Backup/Restore Using a Client-Connected Luna Backup HSM \(G5\)" on page 401](#)).
- > You can use an appliance-connected Backup HSM with Remote PED only if the source partition is activated (["Activation and Auto-activation on Multi-factor- \(PED-\) Authenticated Partitions" on page 299](#)) and appliance software version 7.7.0 or newer is installed.

This section provides instructions for the following procedures using this kind of deployment:

- > ["Initializing the Backup HSM" below](#)
- > ["Backing Up an Application Partition" on the next page](#)
- > ["Restoring an Application Partition from Backup" on page 400](#)

**NOTE** To perform backup operations on HSM firmware 7.7.0 or newer (V0 or V1 partitions):

- > Luna Backup HSM (G7) requires minimum firmware version 7.7.1
- > Luna Backup HSM (G5) requires minimum firmware version 6.28.0

You can use a Luna Backup HSM with older firmware to restore objects to a V0 or V1 partition, but this is supported for purposes of getting your objects from the older partitions onto the newer V0 or V1 partitions only.

V0 and V1 partitions are considered more secure than partitions at earlier firmware versions - any attempt to restore from a higher-security status to lower-security status fails gracefully.

SMK backup for appliance is supported only with local connection.

## Initializing the Backup HSM

Before you can use the Luna Backup HSM to back up your partition objects, it must be initialized. This procedure is analogous to the standard HSM initialization procedure.

### Prerequisites

- > Install the Backup HSM and connect it to power (see ["Installing the Backup HSM" on page 387](#)).
- > Ensure that the Backup HSM is not in Secure Transport Mode and that any tamper events are cleared (see ["Backup HSM Secure Transport and Tamper Recovery" on page 390](#)).
- > [PED Authentication] Ensure that you have enough blank or rewritable blue and red PED keys available for your desired authentication scheme (see ["Creating PED Keys" on page 224](#)).
- > [Local PED] Connect the PED using a 9-pin Micro-D to Micro-D cable. Set the PED to **Local PED-SCP** mode (see ["Modes of Operation" on page 188](#)).

## To initialize a locally-connected Backup HSM using LunaSH on the Luna Network HSM

1. Log in to LunaSH as **admin**, or an **admin**-level custom user.
2. [Optional] View the Luna Backup HSMs currently connected to the appliance and find the correct serial number.

```
lunash:> token backup list
```

3. Initialize the Backup HSM by specifying its serial number and a label.

```
lunash:> token backup init -serial <serialnum> -label <label>
```

You are prompted to set the HSM SO credential and cloning domain for the Backup HSM.

## Backing Up an Application Partition

You can use LunaSH to back up the contents of an application partition to the locally-connected Luna Backup HSM. You can use this operation to create a backup on the Backup HSM, or add objects from the source partition to an existing backup.

### Prerequisites

- > The Backup HSM must be initialized (see ["Initializing the Backup HSM" on the previous page](#)).
- > You must have **admin** or **admin**-level access to LunaSH on the Luna Network HSM.
- > The following policies are set (see [HSM Capabilities and Policies](#) and ["Partition Capabilities and Policies" on page 272](#) for more information):
  - HSM policy **16: Enable network replication** must be set to **1** (ON) on the HSM that hosts the source partition.
  - Partition policy **0: Allow private key cloning** must be set to **1** (ON) on the source partition.
  - Partition policy **4: Allow secret key cloning** must be set to **1** (ON) on the source partition.
- > You must have the Crypto Officer credential (black PED key) and domain (red PED key) for the source partition.
- > [Local PED] Connect the PED to the Luna Network HSM using a Mini-B to USB-A cable (see ["Local PED Setup" on page 190](#)), and to the Backup HSM using a 9-pin Micro-D to Micro-D cable. Set the PED to **Local PED-USB** mode (see ["Modes of Operation" on page 188](#)).
- > [Remote PED] The source partition must be activated (see ["Activation and Auto-activation on Multi-factor-\(PED-\) Authenticated Partitions" on page 299](#)).
- > [Remote PED] Set up a Remote PED server to authenticate the Backup HSM (see ["Remote PED Setup" on page 1](#)).
- > [Remote PED] You require the orange PED key for the Backup HSM, which must be initialized using a local PED connection (see ["Initializing the Backup HSM Remote PED Vector" on page 393](#)).

## To back up an application partition to a locally-connected Backup HSM using LunaSH

1. Log in to LunaSH as **admin**, or an **admin**-level custom user.
2. [Remote PED] Connect the Backup HSM to the remote PED server.

```
lunash:> hsm ped connect -ip <PEDserver_IP> -serial <Backup_HSM_serialnum>
```

3. [Optional] View the Luna Backup HSMs currently connected to the appliance and find the correct serial number.

lunash:> **token backup list**

4. Back up the partition, specifying the source partition label, a label for the backup (either a new or existing label), and the Backup HSM serial number. If you specify an existing backup, use one of the following options:

- **-add** to keep the existing partition contents and add new objects only
- **-replace** to erase the partition contents and replace them with the backup

You do not need to specify these options when backing up a V1 partition, as only the SMK is backed up.

If you omit the **-tokenpar** option when creating a new backup, the partition is assigned a default name (<source\_partition\_name>\_<YYYYMMDD>) based on the source HSM's internally-set time and date.

lunash:> **partition backup -partition** <source\_label> **-serial** <Backup\_HSM\_serialnum> [**-tokenpar** <target\_label>] [**-add**] [**-replace**]

You are prompted for the source partition's Crypto Officer credential (black PED key or challenge secret).

[Remote PED] You are prompted for a Crypto Officer credential for the backup (black PED key) and for the cloning domain that matches the source partition (red PED key). If you are adding to an existing backup, you are not asked for the cloning domain.

5. [Local PED] LunaSH prompts you to connect the Luna PED to the Backup HSM. Set the mode on the Luna PED to **Local PED-SCP** (see "[Modes of Operation](#)" on page 188). Enter **proceed** in LunaSH.

You are prompted to set the following credentials:

- Crypto Officer (password or black PED key) for the backup (can be the same as the source partition)
- Cloning domain (string or red PED key) for the backup (must be the same as the source partition)

The partition contents are cloned to the backup.

## Restoring an Application Partition from Backup

You can use LunaSH to restore the contents of a backup to the original application partition, or any other Luna application partition that shares the same cloning domain.

### Prerequisites

- > The target partition must be initialized with the same cloning domain as the backup.
- > You must have **admin** or **admin**-level access to LunaSH on the Luna Network HSM.
- > The following policies are set (see [HSM Capabilities and Policies](#) and "[Partition Capabilities and Policies](#)" on page 272 for more information):
  - HSM policy **16: Enable network replication** must be set to **1** (ON) on the HSM that hosts the target partition.
  - Partition policy **0: Allow private key cloning** must be set to **1** (ON) on the target partition.
  - Partition policy **4: Allow secret key cloning** must be set to **1** (ON) on the target partition.
- > You must have the Crypto Officer credentials (black PED key) for the backup and the target partition.



- > [Local PED] Connect the PED to the Luna Network HSM using a Mini-B to USB-A cable (see "[Local PED Setup](#)" on page 190), and to the Backup HSM using a 9-pin Micro-D to Micro-D cable. Set the PED to **Local PED-USB** mode (see "[Modes of Operation](#)" on page 188).
- > [Remote PED] The source partition must be activated (see "[Activation and Auto-activation on Multi-factor-\(PED-\) Authenticated Partitions](#)" on page 299).
- > [Remote PED] Set up a Remote PED server to authenticate the Backup HSM (see "[Remote PED Setup](#)" on page 1). You require the orange PED key for the Backup HSM.

### To restore the contents of a backup to an application partition

1. Log in to LunaSH as **admin**, or an **admin**-level custom user.
2. [Remote PED] Connect the Backup HSM to the remote PED server.  

```
lunash:> hsm ped connect -ip <PEDserver_IP> -serial <Backup_HSM_serialnum>
```
3. [Optional] View the Luna Backup HSMs currently connected to the appliance and find the correct serial number.  

```
lunash:> token backup list
```
4. [Optional] View the backups currently available on the Backup HSM.  

```
lunash:> token backup partition list -serial <Backup_HSM_serialnum>
```
5. Restore the partition contents, specifying the target partition label, the backup label, the Backup HSM serial number, and either:
  - **-add** to keep the existing partition contents and add new objects only
  - **-replace** to erase the partition contents and replace them with the backup

**CAUTION!** If you are restoring a V1 backup to a V1 partition, use **-add** to restore the SMK. Use **-replace** only if you wish to erase any existing cryptographic material on the target partition. By default, V1 backups only include the SMK.

```
lunash:> partition restore -partition <target_label> -tokenpar <backup_label> -serial <Backup_HSM_serialnum> {-add | -replace}
```

You are prompted for the target partition's Crypto Officer credential (black PED key or challenge secret).

6. [Local PED] LunaSH prompts you to connect the Luna PED to the Backup HSM. Change the mode on the Luna PED to **Local PED-SCP** (see "[Modes of Operation](#)" on page 188). Enter **proceed** in LunaSH. You are prompted for the backup's Crypto Officer credential (black PED key or challenge secret). The backup contents are cloned to the application partition.

## Backup/Restore Using a Client-Connected Luna Backup HSM (G5)

You can connect the Luna Backup HSM to a USB port on the client workstation. This configuration allows you to perform backup/restore operations for all application partitions that appear as visible slots in LunaCM. It is useful in deployments where the partition Crypto Officer wants to keep backups at the client. You can restore a

partition backup to the original source partition or to another existing Luna application partition that shares the same cloning domain.

This section provides instructions for the following procedures using this kind of deployment:

- > ["Initializing the Backup HSM" below](#)
- > ["Backing Up an Application Partition" on the next page](#)
- > ["Restoring an Application Partition from Backup" on page 404](#)

**NOTE** To perform backup operations on HSM firmware 7.7.0 or newer (V0 or V1 partitions):

- > Luna Backup HSM (G7) requires minimum firmware version 7.7.1
- > Luna Backup HSM (G5) requires minimum firmware version 6.28.0

You can use a Luna Backup HSM with older firmware to restore objects to a V0 or V1 partition, but this is supported for purposes of getting your objects from the older partitions onto the newer V0 or V1 partitions only.

V0 and V1 partitions are considered more secure than partitions at earlier firmware versions - any attempt to restore from a higher-security status to lower-security status fails gracefully.

SMK backup for appliance is supported only with local connection.

## Initializing the Backup HSM

Before you can use the Luna Backup HSM to back up your partition objects, it must be initialized. This procedure is analogous to the standard HSM initialization procedure.

### Prerequisites

- > Install the Backup HSM at the client and connect it to power (see ["Installing the Backup HSM" on page 387](#)).
- > Ensure that the Backup HSM is not in Secure Transport Mode and that any tamper events are cleared (see ["Backup HSM Secure Transport and Tamper Recovery" on page 390](#)).
- > [PED Authentication] Ensure that you have enough blank or rewritable blue and red PED keys available for your desired authentication scheme (see ["Creating PED Keys" on page 224](#)).
  - [Local PED] Connect the PED using a 9-pin Micro-D to Micro-D cable. Set the PED to **Local PED-SCP** mode (see ["Modes of Operation" on page 188](#)).
  - [Remote PED] Initialize the Backup HSM RPV (see ["Initializing the Backup HSM Remote PED Vector" on page 393](#)). You require the orange PED key.
  - [Remote PED] Set up a Remote PED server to authenticate the Backup HSM (see ["Remote PED Setup" on page 1](#)).

### To initialize a client-connected Backup HSM

1. Launch LunaCM on the client workstation.
2. Set the active slot to the Luna Backup HSM.
 

```
lunacm:> slot set -slot <slotnum>
```
3. [Remote PED] Connect the Backup HSM to the Remote PED server.
 

```
lunacm:> ped connect -ip <PEDserver_IP> -port <portnum>
```

- Initialize the Backup HSM, specifying a label and the method of authentication (**-initwithped** or **-initwithpwd**). You must initialize the HSM with the same authentication method as the partition(s) you plan to back up.

```
lunacm:> hsm init -label <label> {-initwithped | -initwithpwd}
```

You are prompted to set an HSM SO credential and cloning domain for the Backup HSM.

## Backing Up an Application Partition

You can use LunaCM to back up the contents of an application partition to the client-connected Luna Backup HSM. You can use this operation to create a backup on the Backup HSM, or add objects from the source partition to an existing backup.

### Prerequisites

- > The Backup HSM must be initialized (see ["Initializing the Backup HSM" on the previous page](#)).
- > The following policies are set (see [HSM Capabilities and Policies](#) and ["Partition Capabilities and Policies" on page 272](#) for more information):
  - HSM policy **16: Enable network replication** must be set to **1 (ON)** on the HSM that hosts the source partition.
  - [Pre-7.7.0 and V0 partitions only] Partition policy **0: Allow private key cloning** is set to **1 (ON)** on the source partition.
  - [Pre-7.7.0 and V0 partitions only] Partition policy **4: Allow secret key cloning** is set to **1 (ON)** on the source partition.
- > You must have the Crypto Officer credential (black PED key) and domain (red PED key) for the source partition.
- > You must have the Backup HSM SO credential (blue PED key).
- > [PED Authentication] This procedure is simpler if the source partition is activated (see ["Activation and Auto-activation on Multi-factor- \(PED-\) Authenticated Partitions" on page 299](#)), since you require a Luna PED only for the Backup HSM.
  - [Local PED] Connect the PED to the Backup HSM using a 9-pin Micro-D to Micro-D cable. The source partition must be activated. If not, you must use Remote PED.
  - [Remote PED] You must have the orange PED key for the Backup HSM (see ["Initializing the Backup HSM Remote PED Vector" on page 393](#)). If the source partition is not activated, you may need the orange PED key for the Luna Network HSM as well.
  - [Remote PED] Set up Remote PED on the workstation you plan to use for PED authentication (see ["Remote PED Setup" on page 1](#)). If the partition is not activated, you must connect to PEDserver with **ped connect** before logging in, and disconnect with **ped disconnect** before initiating the backup.

### To back up an application partition to a client-connected Backup HSM

- Launch LunaCM on the client workstation.
- Set the active slot to the source partition and log in as Crypto Officer.

```
lunacm:> slot set -slot <slotnum>
```

```
lunacm:> role login -name co
```

### 3. [PED Authentication] Connect the Backup HSM to the Luna PED.

- [Local PED] Set the mode on the Luna PED to **Local PED-SCP** (see "Modes of Operation" on page 188).
- [Remote PED] Connect the Backup HSM slot to PEDserver.

```
lunacm:> ped connect -slot <Backup_HSM_slotnum> -ip <PEDserver_IP> -port <portnum>
```

### 4. Back up the partition, specifying the Backup HSM slot and a label for the backup (either a new or existing label). If you specify an existing backup label, include the **-append** option to add only new objects to the backup (duplicate objects will not be cloned). By default, the existing backup will be overwritten with the current contents of the source partition.

```
lunacm:> partition archive backup -slot <Backup_HSM_slotnum> [-partition <backup_label>] [-append] [-replace] [-smkonly]
```

If you omit the **-partition** option when creating a new backup, the partition is assigned a default name (<source\_partition\_name>\_<YYYYMMDD>) based on the source HSM's internally-set time and date.

If you are backing up a V1 partition, include **-smkonly** to back up the SMK only. By default, the SMK and any encrypted cryptographic material on the partition are backed up.

The backup begins once you have completed the authentication process. Objects are backed up one at a time. For existing backups, you can use the following options to define how individual objects are backed up:

<b>-append</b>	Add only new objects to an existing backup.
<b>-replace</b>	Delete the existing objects in a target backup partition and replace them with the contents of the source user partition. This is the default.
<b>-append</b> and <b>-replace</b>	Add new objects and replace existing objects that have the same OUID but a different fingerprint (such as would occur if any of the object attributes were changed since the previous backup).

You are prompted to present or set the following credentials:

- [Remote PED] Backup HSM Remote PED vector (orange PED key)
- Backup HSM SO (password or blue PED key)
- Crypto Officer (password or black PED key) for the backup (can be the same as the source partition)
- Cloning domain (string or red PED key) for the backup (must be the same as the source partition)

The partition contents are cloned to the backup.

### 5. [Remote PED] Disconnect the Backup HSM from PEDserver.

```
lunacm:> ped disconnect
```

## Restoring an Application Partition from Backup

You can use LunaCM to restore the contents of a backup to the original application partition, or any other Luna application partition that shares the same cloning domain.

### Prerequisites

- > The target partition must be initialized with the same cloning domain as the backup partition.

- > The following policies are set (see [HSM Capabilities and Policies](#) and ["Partition Capabilities and Policies" on page 272](#) for more information):
  - HSM policy **16: Enable network replication** must be set to **1 (ON)** on the HSM that hosts the target partition.
  - [Pre-7.7.0 and V0 partitions only] Partition policy **0: Allow private key cloning** is set to **1 (ON)** on the target partition.
  - [Pre-7.7.0 and V0 partitions only] Partition policy **4: Allow secret key cloning** is set to **1 (ON)** on the target partition.
- > You must have the Crypto Officer credentials for the backup partition and the target partition.
- > [PED Authentication] This procedure is simpler if the application partition is activated (see ["Activation and Auto-activation on Multi-factor- \(PED-\) Authenticated Partitions" on page 299](#)), since you require a Luna PED only for the Backup HSM.
  - [Local PED] Connect the PED to the Backup HSM using a 9-pin Micro-D to Micro-D cable. The source partition must be activated. If not, you must use Remote PED.
  - [Remote PED] Set up Remote PED on the workstation you plan to use for PED authentication (see ["Remote PED Setup" on page 1](#)). If the partition is not activated, you must connect to PEDserver with **ped connect** before logging in, and disconnect with **ped disconnect** before initiating the backup.

### To restore the contents of a backup to an application partition

1. Launch LunaCM on the client workstation.
2. Set the active slot to the target partition and log in as Crypto Officer.
 

```
lunacm:> slot set -slot <slotnum>
```

```
lunacm:> role login -name co
```
3. [PED Authentication] Connect the Backup HSM to the Luna PED.
  - [Local PED] Set the mode on the Luna PED to **Local PED-SCP** (see ["Modes of Operation" on page 188](#)).
  - [Remote PED] Connect the Backup HSM slot to PEDserver.
 

```
lunacm:> ped connect -slot <Backup_HSM_slotnum> -ip <PEDserver_IP> -port <portnum>
```
4. [Optional] Display the available backups by specifying the Backup HSM slot. Each available backup also appears as a slot in LunaCM.
 

```
lunacm:> partition archive list -slot <Backup_HSM_slotnum>
```
5. [Optional] Display the contents of a backup by specifying the Backup HSM slot and the backup partition label in LunaCM.
 

```
lunacm:> partition archive contents -slot <backup_slotnum> -partition <backup_label>
```
6. Restore the partition contents, specifying the Backup HSM slot and the backup you wish to use. By default, duplicate backup objects with the same OUID as objects currently existing on the partition are not restored.
 

If you have changed attributes of specific objects since your last backup and you wish to revert these changes, include the **-replace** option.

If you are restoring a V1 partition and you only want to restore the SMK, include the **-smkonly** option.

```
lunacm:> partition archive restore -slot <Backup_HSM_slotnum> -partition <backup_label> [-replace]
[-smkonly]
```

You are prompted for the backup's Crypto Officer credential.

The backup contents are cloned to the application partition.

## Configuring a Remote Luna Backup HSM (G5) Server

In this configuration, the Luna Backup HSM is connected to a remote client workstation that communicates with the client via the Remote Backup Service (RBS). It is useful in deployments where backups are stored in a separate location from the Luna Network HSM, to protect against catastrophic loss (fire, flood, etc).

RBS is a utility, included with the Luna HSM Client software, that runs on a workstation hosting one or more Backup HSMs. When RBS is configured and running, other clients or HSMs registered to it can see its Backup HSM(s) as slots in LunaCM. RBS is compatible with both Luna G5 and G7 Backup HSMs.

### Installing/Configuring the Remote Backup Service

RBS is installed using the Luna HSM Client installer. You must create a certificate for the RBS workstation and register it on all clients/appliances that will use the remote Backup HSMs. These instructions will allow you to install and configure RBS.

#### Prerequisites

- > On any Luna Network HSM client workstation, install the following Luna HSM Client components (see "[Luna HSM Client Software Installation](#)" on page 17):
  - **Network:** The Network component includes utilities that are required for remote backups
  - **Remote PED:** if you are backing up PED-authenticated partitions

**NOTE** The Luna HSM Client version installed on the RBS workstation must be the same version installed on the client workstation(s). Ensure that you use a client version that is compatible with your Backup HSM firmware.

- > Install the Luna Backup HSM(s) at the workstation that will host RBS (see "[Installing the Backup HSM](#)" on page 387).
- > [PED Authentication] Initialize the remote PED vector for each Backup HSM. You will need the orange PED key for backup/restore operations (see "[Initializing the Backup HSM Remote PED Vector](#)" on page 393).

#### To install and configure RBS

1. On the workstation hosting the Backup HSM(s), install the **Backup** component of the Luna HSM Client (see "[Luna HSM Client Software Installation](#)" on page 17). If this workstation will also host a Remote PED, install the **Remote PED** component as well (Windows only).
2. Navigate to the Luna HSM Client home directory (`/usr/safenet/lunaclient/rbs/bin` on Linux/Unix) and generate a certificate for the RBS host.

```
> rbs --genkey
```

You are prompted to enter and confirm an RBS password. The certificate is generated in:

- Linux/UNIX: <LunaClient\_install\_directory>/rbs/server/**server.pem**
  - Windows: <LunaClient\_install\_directory>\cert\server\**server.pem**
3. Specify the Backup HSM(s) that RBS will make available to clients.  
> **rbs --config**  
RBS displays a list of Backup HSMs currently connected to the workstation. Select the ones you want to provide remote backup services. When you have specified your selection, enter **X** to exit the configuration tool.
  4. Launch the RBS daemon (Linux/UNIX) or console application (Windows).
    - Linux/UNIX: # **rbs --daemon**
    - Windows: Double-click the **rbs** application. A console window will remain open.  
You are prompted to enter the RBS password.
  5. Securely transfer the RBS host certificate (**server.pem**) to your Luna HSM Client workstation using **pscp** or **scp**.
  6. On the client workstation, register the RBS host certificate to the server list.  
> **vtl addServer -n <Backup\_host\_IP> -c server.pem**
  7. [Optional] Launch LunaCM on the client to confirm that the Backup HSM appears as an available slot.

**NOTE** If you encounter issues, try changing the RBS and PEDclient ports from their default values. Check that your firewall is not blocking ports used by the service.

You can now use the Backup HSM(s) as though they were connected to the client workstation locally, using Remote PED. See "[Backup/Restore Using a Client-Connected Luna Backup HSM \(G5\)](#)" on page 401 for procedures.

# CHAPTER 15: Backup and Restore Using a Luna Backup HSM (G7)



The following topics describe how to configure and use the Luna Backup HSM (G7) to backup and restore the cryptographic objects in your user partitions. You can perform backup and restore operations by connecting the Luna Backup HSM (G7) to a Luna HSM Client workstation or Luna Network HSM appliance:

## About Backup/Restore Using the Luna Backup HSM (G7)

- > ["Overview and Key Concepts" below](#)

## Installing the Luna Backup HSM (G7) Hardware

- > ["Luna Backup HSM \(G7\) Hardware Installation" on page 412](#)

## Backup/Restore from a Luna HSM Client Workstation Using LunaCM

- > ["Initializing a Client-Connected Luna Backup HSM \(G7\)" on page 414](#)
- > ["Backing Up to a Client-Connected Luna Backup HSM \(G7\)" on page 419](#)
- > ["Restoring From a Client-Connected Luna Backup HSM \(G7\)" on page 426](#)

## Backup/Restore from a Luna HSM Client Workstation Using the Remote Backup Service (RBS)

- > ["Backup and Restore to a Remote Backup Service \(RBS\)-Connected Luna Backup HSM \(G7\)" on page 447](#)

## Backup/Restore from a Luna Network HSM Appliance Using LunaSH

- > ["Initializing an Appliance-Connected Luna Backup HSM \(G7\)" on page 431](#)
- > ["Backing Up to an Appliance-Connected Luna Backup HSM \(G7\)" on page 435](#)
- > ["Restoring From an Appliance-Connected Luna Backup HSM \(G7\)" on page 442](#)

## Backup HSM Firmware Update/Rollback

- > ["Updating the Luna Backup HSM \(G7\) Firmware" on page 449](#)
- > ["Rolling Back the Luna Backup HSM \(G7\) Firmware" on page 452](#)

## Overview and Key Concepts

This topic provides the following background information you need to perform backup and restore operations using a Luna Backup HSM (G7):

- > ["Overview" on the next page](#)



- > ["Credentials Required to Perform Backup and Restore Operations" below](#)
- > ["Client Software Required to Perform Backup and Restore Operations From a Client Workstation" on the next page](#)
- > ["PED Authentication with the Luna Backup HSM \(G7\) " on the next page](#)
- > ["Backup and Restore Best Practices" on page 411](#)

## Overview

A Crypto Officer (CO) can use the backup HSM to backup the objects in any partition they can log in to, provided that:

- > The user partition and the backup HSM share the same domain.
- > The user partition and the backup HSM use the same authentication method (PED or password).
- > The CO has the required credentials on the backup HSM.

You can perform backup/restore operations on your user partitions by connecting the backup HSM to a Luna HSM Client workstation, or to a Luna Network HSM appliance:

- > When you connect the backup HSM to a Luna HSM Client workstation, the backup HSM Admin partition is added to the slots listed in LunaCM, allowing you to clone objects between the <source> user partition and the <target> backup partition.
- > When you connect the backup HSM to a Luna Network HSM appliance, the backup HSM is available as an attached backup token identified by its serial number, allowing you to use LunaSH to clone objects between the <source> user partition and the <target> backup partition. Local backup via LunaSH requires minimum Luna Network HSM appliance software 7.7.0 (see [Version Dependencies by Feature](#) for more information).

**NOTE** To perform backup operations on HSM firmware 7.7.0 or newer (V0 or V1 partitions):

- > Luna Backup HSM (G7) requires minimum firmware version 7.7.1
- > Luna Backup HSM (G5) requires minimum firmware version 6.28.0

You can use a Luna Backup HSM with older firmware to restore objects to a V0 or V1 partition, but this is supported for purposes of getting your objects from the older partitions onto the newer V0 or V1 partitions only.

V0 and V1 partitions are considered more secure than partitions at earlier firmware versions - any attempt to restore from a higher-security status to lower-security status fails gracefully.

SMK backup for appliance is supported only with local connection.

Backups are created and stored as partitions within the Admin partition on the backup HSM.

## Credentials Required to Perform Backup and Restore Operations

You require the following credentials to perform backup/restore operations:

<b>&lt;source&gt; User HSM</b>	Remote PED (orange) key. Required for PED-authenticated backups only, to establish a remote PED connection to the HSM that hosts the <source> user partition.
--------------------------------	---------------------------------------------------------------------------------------------------------------------------------------------------------------

<b>&lt;source&gt; User Partition</b>	<p>Crypto Officer (CO). Required to access the objects in the &lt;source&gt; user partition that will be backed up.</p> <p>Domain. Required to allow objects to be cloned between the &lt;source&gt; user partition and &lt;target&gt; backup partition. The domains for the &lt;source&gt; user partition and &lt;target&gt; backup partition must match, otherwise the backup will fail.</p>
<b>&lt;target&gt; Backup HSM</b>	<p>HSM Security Officer (SO). Required to create or access the &lt;target&gt; backup partition in the Admin slot, where all backups are archived.</p> <p>Remote PED (orange) key. Required for PED-authenticated backups only, to establish a remote PED connection to the HSM that hosts the &lt;target&gt; backup partition.</p> <p><b>Note:</b> You create new credentials for both roles on HSM initialization, and use them for subsequent backups to the &lt;target&gt; backup HSM.</p>
<b>&lt;target&gt; Backup Partition</b>	<p>Partition owner (PSO). Required to access the &lt;target&gt; backup partition.</p> <p>Crypto Officer (CO). Required to access the objects in the &lt;target&gt; backup partition.</p> <p><b>Note:</b> You create new credentials for both roles on the initial backup, and use them for subsequent backups to the &lt;target&gt; backup partition.</p>

## Client Software Required to Perform Backup and Restore Operations From a Client Workstation

You must install the Luna HSM Client software and USB driver for the backup HSM on the workstation you intend to use to perform backup and restore operations. The Luna Backup HSM (G7) requires minimum client version 10.1. Refer to "[Luna HSM Client Software Installation](#)" on page 17 for detailed installation instructions.

**NOTE** Ensure that the backup HSM is not connected to the Luna HSM Client workstation when you install or uninstall the client software. Failure to do so may result in the backup HSM becoming unresponsive.

When you install the client software, you must select the following options:

- > The **USB** option. This installs the driver for the backup HSM.
- > The **Network** and/or **PCIe** options, depending on which type of HSM you intend to backup.
- > The **Remote PED** option, if you want to backup PED-authenticated partitions. Note that you can install and use a remote PED on the same workstation used to host the backup HSM, or on a different workstation.
- > The **Backup** option, if you want to backup to a remote backup HSM using RBS.

## PED Authentication with the Luna Backup HSM (G7)

The Luna Backup HSM (G7) is equipped with a single USB port that is used to connect the backup HSM to a Luna HSM Client workstation or Luna Network HSM appliance. As such, any PED connections to the backup HSM must use a remote PED and the **pedserver** service:

- > When the Luna Backup HSM (G7) is connected to a client workstation, you authenticate to it with a remote PED connected to the same client workstation, or to a separate workstation set up as a Remote PED server.

To backup or restore a partition, you must use `lunacm:> ped connect` to establish remote PED connections to both the <source> user partition and <target> backup HSM.

- > When the Luna Backup HSM (G7) is connected to a Luna Network HSM appliance you authenticate to it with a remote PED that is also connected to the appliance. To backup or restore a partition, you must use `lunash:> hsm ped connect` to establish a remote PED connection to the appliance loopback IP address (127.0.0.1) using the `pedserver` service running on the appliance. Neither the PED nor the Backup HSM can be connected to the HSM USB port (see [Physical Features](#)); each must be connected to one of the appliance USB ports.

## Backup and Restore Best Practices

To ensure that your data is protected in the event of a failure or other catastrophic event, Thales recommends that you use the following best practices as part of a comprehensive backup strategy:

**CAUTION!** Failure to develop and exercise a comprehensive backup and recovery plan may prevent you from being able to recover from a catastrophic event. Although Thales provides a robust set of backup hardware and utilities, we cannot guarantee the integrity of your backed-up key material, especially if stored for long periods. Thales strongly recommends that you exercise your recovery plan at least semi-annually (every six months) to ensure that you can fully recover your key material.

### Develop and document a backup and recovery plan

This plan should include the following:

- > What is being backed up
- > The backup frequency
- > Where the backups are stored
- > Who is able to perform backup and restore operations
- > Frequency of exercising the recovery test plan

### Make multiple backups

To ensure that your backups are always available, build redundancy into your backup procedures.

### Use off-site storage

In the event of a local catastrophe, such as a flood or fire, you might lose both your working HSMs and locally-stored backup HSMs. To fully protect against such events, always store a copy of your backups at a remote location.

### Regularly exercise your disaster recovery plan

Execute your recovery plan at least semi-annually (every six months) to ensure that you can fully recover your key material. This involves retrieving your stored Backup HSMs and restoring their contents to a test partition, to ensure that the data is intact and that your recovery plan works as documented.

## Luna Backup HSM (G7) Hardware Installation

The following topics describe how to install and connect a Luna Backup HSM (G7). To ensure a successful installation, perform the following tasks in the order indicated:

1. Ensure that you have all of the required components, as listed in ["Luna Backup HSM Received Items" below](#)
2. Install and connect the hardware, as described in ["Installing the Luna Backup HSM Hardware" on page 414](#)

**CAUTION!** To ensure the security and integrity of your new device, refer to ["Verifying the Integrity of Your Shipment" on page 1](#) before unpacking your new Luna Backup HSM.

The Luna Backup HSM (G7) complies with the following:



### Luna Backup HSM Received Items

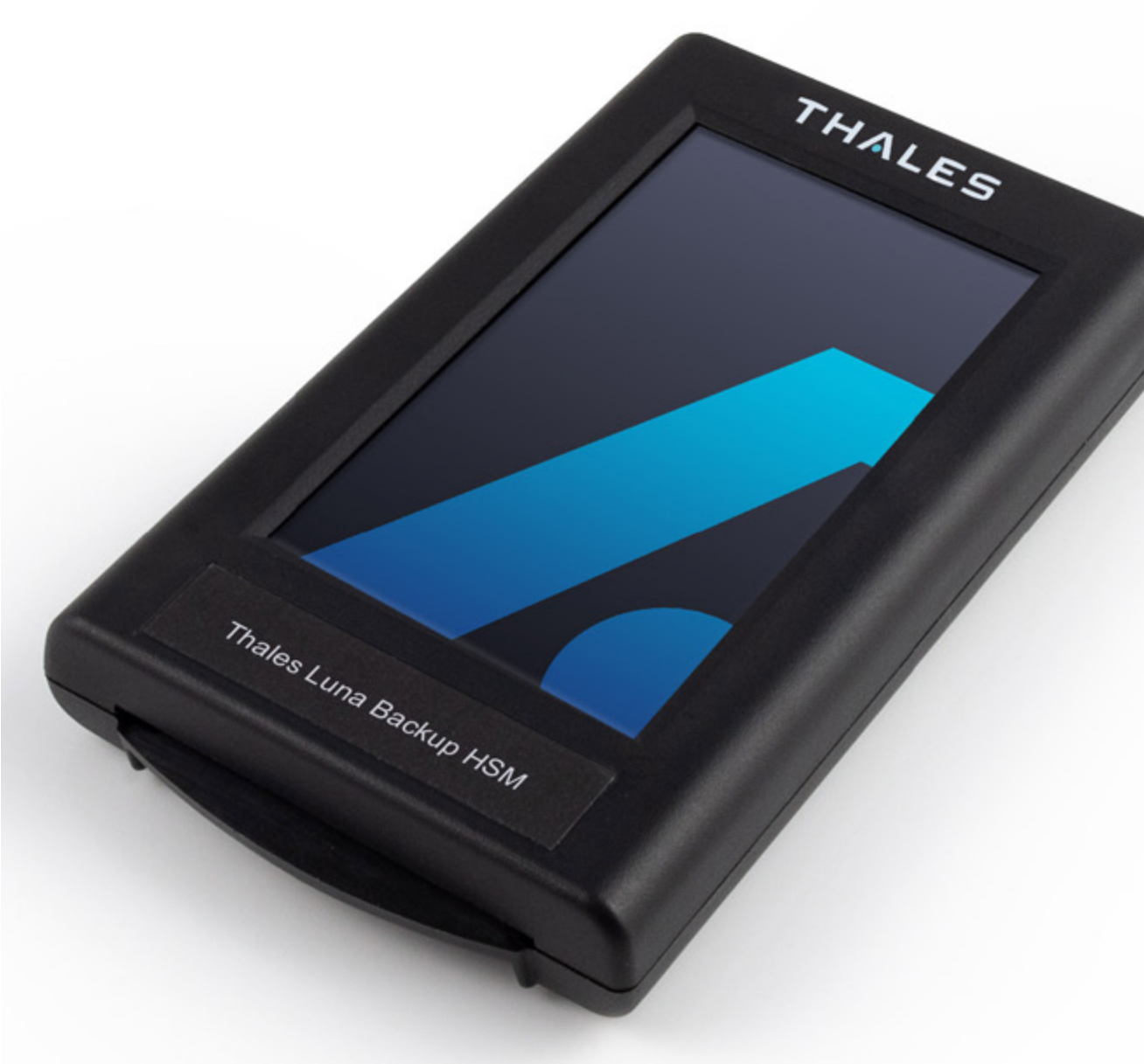
This section provides a list of the components you should have received with your order.

#### Included Items

The following items are included with your new backup HSM.

Quantity	Item
----------	------

1	Luna Backup HSM
---	-----------------



Quantity	Item
1	<b>USB 3.0 Cable: Type A to Type C</b> 
1	<b>5V Power Supply</b> with replaceable plug modules for international use. <p><b>NOTE</b> On most workstations, the USB connection provides adequate power to the backup HSM. If you are using a low-power workstation, such as a netbook, the USB connection may not provide adequate power, in which case you will also need to connect the external power supply.</p>

## Installing the Luna Backup HSM Hardware

The backup HSM is a USB device. To install the backup HSM, connect it to a Luna HSM Client workstation using the included USB cable. The workstation must be running Luna HSM Client software that supports the backup HSM and provides the required drivers. Refer to the release notes and see "[Backup and Restore Using a Luna Backup HSM \(G7\)](#)" on page 408 for more information.

**NOTE** On most workstations, the USB connection provides adequate power to the Backup HSM and it will begin the boot sequence. If you are using a low-power workstation, such as a netbook, the USB connection may not provide adequate power, in which case you will also need to connect the external power supply.

## Initializing a Client-Connected Luna Backup HSM (G7)

You must initialize the backup HSM prior to first use. Initialization does the following:

- > Recovers the HSM from Secure Transit Mode (STM). STM allows you to verify that the HSM was not tampered in transit. All new HSMs are shipped from the factory in Secure Transport Mode.
- > Creates the orange (Remote PED vector) key for the backup HSM (PED-authenticated HSMs only). You create the orange key using a one-time, password-secured connection between the PED and the backup HSM. You then use this orange key to secure all subsequent connections between the PED and the backup HSM.

- > Sets the authentication mode of the HSM. PED-authenticated backup HSMs can backup PED-authenticated partitions. Password-authenticated backup HSMs can backup password-authenticated partitions.
- > Sets the security domain of the HSM. You can only backup partitions that share the same domain as the backup HSM.
- > Creates the HSM SO role on the HSM (see [HSM Roles and Procedures](#)). This role is required to create or modify a backup partition, and must be logged in to perform a backup.

The procedure is different for PED-authenticated and password-authenticated backups, as detailed in the following sections:

- > ["Initializing a PED-Authenticated HSM" below](#)
- > ["Initializing a Password-Authenticated HSM" on page 418](#)

**NOTE** This feature requires minimum client version 10.1. See [Version Dependencies by Feature](#) for more information.

## Initializing a PED-Authenticated HSM

Initializing your backup HSM as PED authenticated allows you to backup PED-authenticated partitions.

### Summary

To initialize a PED-authenticated HSM you connect it and a remote PED (using a USB or network connection) to a Luna HSM Client workstation, and performing the following tasks:

- > Recover the HSM from Secure Transport Mode.
- > Create the orange (Remote PED vector) key for the backup HSM.
- > Initialize the HSM to set the authentication mode (PED) and HSM domain, and create the HSM SO PED key.

### Prerequisites

Before beginning, ensure that you are familiar with the concepts in ["PED Authentication" on page 176](#). You will need the following PED keys:

- > A blank orange (PED vector) PED key, plus the number required to create duplicate PED keys as necessary.

**CAUTION!** Always make copies of your orange PED Keys, or declare MofN as one-of-several, and store at least one safely. For the Luna Backup HSM (G7), *the orange PED Key is as important as the HSM SO blue key or the Domain red key.* (This contrasts with other Luna HSMs, where a lost or damaged orange key can be easily replaced via a local PED connection.)

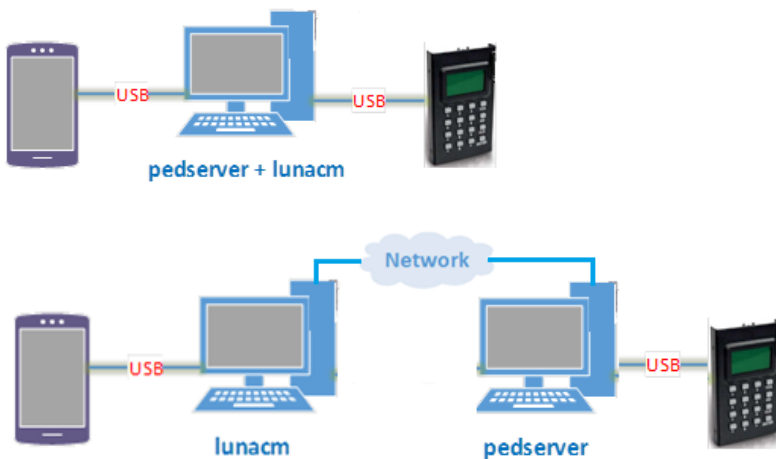
A Remote PED Vector (RPV), on an orange PED Key (RPK) or on an associated HSM, is not a role; it is required to set up the secure tunnel for Remote PED operation.

When used with a PED-authenticated Luna Backup HSM (G7), the PED *always* connects *remotely*. The single USB port on the Backup HSM is for the connection to a Client computer or to a Luna Network HSM appliance - the PED is never connected locally/directly to the Luna Backup HSM (G7). Therefore, losing the RPK for that Luna Backup HSM (G7), without access to a copy, would mean losing the material backed-up on that Backup HSM.

- > N number of blue (HSM SO) PED keys, as defined by the M of N scheme you choose for the HSM SO role, plus the number required to create duplicate PED keys as necessary.
- > An existing red (Domain) PED key for the cloning domain of the partitions you want to backup to the HSM. You can also insert a blank red (Domain) PED key if you want to create a new domain for the HSM (although you won't be able to backup any existing partitions if you do).

### To initialize a PED-authenticated Backup HSM

1. Configure your Luna HSM Client workstation using one of the following configurations:



- a. Install the required client software on the Luna HSM Client workstation. See "[Initializing a Client-Connected Luna Backup HSM \(G7\)](#)" on page 414 for details.
- b. Connect the backup HSM directly to the Luna HSM Client workstation using the included USB cable.

**NOTE** On most workstations, the USB connection provides adequate power to the backup HSM and it will begin the boot sequence. If you are using a low-power workstation, such as a netbook, the USB connection may not provide adequate power, in which case you will also need to connect the external power supply.



- c. Connect the PED to the Luna HSM Client workstation used to host the remote PED, using the PED USB cable.

**NOTE** You connect to the remote PED using the IP address of the workstation used to host the PED. This can be the same workstation that hosts the user and backup partition slots, or a different workstation. The workstation used to host the PED must be running pedServer.

2. Start the **pedserver** service on the workstation used to host the remote PED:

<b>Windows</b>	C:\Program Files\Safenet\LunaClient> <b>pedserver -mode start</b> on page 251
<b>Linux</b>	/usr/safenet/lunaclient> <b>pedserver -mode start</b> on page 251

3. Launch LunaCM on the workstation that hosts the user and backup partition slots.

4. Select the slot assigned to the backup HSM Admin partition.

```
lunacm:> slot set -slot <slot_id>
```

5. Recover the HSM from Secure Transport Mode. See [Secure Transport Mode](#) for more information:

```
lunacm:> stm recover -randomuserstring <string>
```

**NOTE** Recovering a Luna HSM (G7) from secure transport mode may take up to three minutes.

6. Connect to the Luna HSM Client workstation that hosts the PED. If defaults are not **ped set**, specify an IP address (and port if required; 1503 is default).

```
lunacm:> ped connect -ip <ip_address> -pwd
```

LunaCM generates and displays a one-time password that is used to set up a secure channel between the backup HSM and the PED, allowing you to securely initialize the orange (Remote PED Vector) key. Enter the displayed password on the PED when prompted to complete setup of the secure channel.

7. Create an orange (Remote PED vector) key for the backup HSM. The PED vector key is required for subsequent PED-authenticated sessions to the HSM. Ensure that you label any new PED keys that you create during this process.

```
lunacm:> ped vector init
```

**CAUTION!** The orange PED key is required for all Luna G7 Backup HSM operations. If this key is lost, your backups will become irretrievable. Thales recommends keeping multiple backups of all PED keys stored in a secure location.

8. Tear down the one-time, password-protected secure channel between the backup HSM and the PED you used to create the orange (Remote PED vector) key.

```
lunacm:> ped disconnect
```

You are prompted to enter the one-time password that was generated when you performed the **ped connect**. Enter the password and press Enter to proceed.

- Set up a new secure channel between the backup HSM and the PED. If defaults are not [ped set](#), specify an IP address (and port if required; 1503 is default). You are prompted to insert the orange PED key you created in step 7.

```
lunacm:> ped connect
```

- Initialize the selected backup HSM in PED-authenticated mode. You are prompted by the PED for the red Domain key(s) (existing or new) and blue HSM SO key(s) (new). Respond to the PED prompts and insert and set the PINs on the required keys when requested. Ensure that you label any new PED keys that you create during this process.

```
lunacm:> hsm init -iped -label <label>
```

```
lunacm:> hsm init -iped -label USB_BACKUP_HSM_G7
```

- Use the **Duplicate** function on the PED to create and label duplicates of the new PED keys, as required. See ["Duplicating Existing PED Keys" on page 234](#) for details.
- Disconnect the PED when done.

```
lunacm:> ped disconnect
```

## Initializing a Password-Authenticated HSM

Initializing your backup HSM as password-authenticated allows you to backup password-authenticated partitions.

### Summary

To initialize a password-authenticated HSM you connect it to a Luna HSM Client workstation and perform the following tasks:

- > Recover the HSM from Secure Transport Mode.
- > Initialize the HSM to set the authentication mode (password), the HSM domain, and the initial password for the HSM SO role.

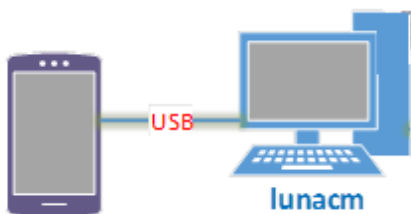
### Prerequisites

Before beginning, ensure that you have the following:

- > The password for the cloning domain of the partitions you want to backup to the HSM. You can also enter a new password to create a new domain for the HSM (although you won't be able to backup any existing partitions if you do).

## To initialize a password-authenticated HSM

- Configure your Luna HSM Client workstation as illustrated below:



- a. Install the required client software on the Luna HSM Client workstation. See ["Initializing a Client-Connected Luna Backup HSM \(G7\)" on page 414](#) for details.
- b. Connect the backup HSM directly to the Luna HSM Client workstation using the included USB cable.

**NOTE** On most workstations, the USB connection provides adequate power to the backup HSM and it will begin the boot sequence. If you are using a low-power workstation, such as a netbook, the USB connection may not provide adequate power, in which case you will also need to connect the external power supply.

2. Launch LunaCM on the workstation that hosts the user and backup partition slots.
3. Select the slot assigned to the backup HSM Admin partition:  
lunacm:> **slot set -slot** <slot\_id>
4. Recover the HSM from Secure Transport Mode. See [Secure Transport Mode](#) for more information:  
lunacm:> **stm recover**

**NOTE** Recovering a Luna HSM (G7) from secure transport mode may take up to three minutes.

5. Initialize the selected backup HSM in password-authenticated mode. You are prompted for the new HSM SO password and the HSM domain string (existing or new):  
lunacm:> **hsm init -ipwd -label** <label>

## Backing Up to a Client-Connected Luna Backup HSM (G7)

To perform a backup, you connect the backup HSM to the Luna HSM Client workstation that hosts the slot for the partition you want to backup, and run the LunaCM [partition archive backup](#) command. Backups are created and stored as partitions within the Admin partition on the backup HSM.

A new backup partition is created on initial backup. For subsequent backups, you can choose to replace the contents of the existing <target> backup partition with the current <source> user partition objects, or append new objects in the <source> user partition to the existing <target> backup partition.

The procedure is different for PED-authenticated and password-authenticated backups, as detailed in the following sections:

- > ["Backing Up a Multi-factor- \(PED-\) Authenticated Partition" below](#)
- > ["Backing Up a Password-Authenticated Partition" on page 424](#)

**NOTE** This feature requires minimum Luna HSM Client 10.1.0. See [Version Dependencies by Feature](#) for more information.

### Backing Up a Multi-factor- (PED-) Authenticated Partition

You require a PED-authenticated backup HSM to backup a PED-authenticated user partition.

## Summary

To perform a backup, you connect the backup HSM and a remote PED to the Luna HSM Client workstation that hosts the slot for the user partition you want to backup, and perform the following tasks:

1. Log in to the <source> user partition as the Crypto Officer (CO):
  - If the <source> user partition is activated, you need to provide the challenge secret.
  - If the <source> user partition is not activated, you need to open a remote PED connection to the <source> HSM and use the required PED keys to log in to the <source> user partition as the Crypto Officer (CO).
2. Open a remote PED connection to the <target> backup HSM. You are prompted for the orange (Remote PED vector) key for the backup HSM.
3. Perform the backup operation and respond to the prompts for the HSM SO, partition SO (PO), crypto officer (CO), and domain PED keys for the backup HSM/partition. The backup HSM and the partition you want to restore to must be members of the same domain.

## Prerequisites

Before beginning, ensure that you have satisfied the following prerequisites:

- > You are familiar with the concepts in ["PED Authentication" on page 176](#).
- > You have the required credentials as listed in the summary above.

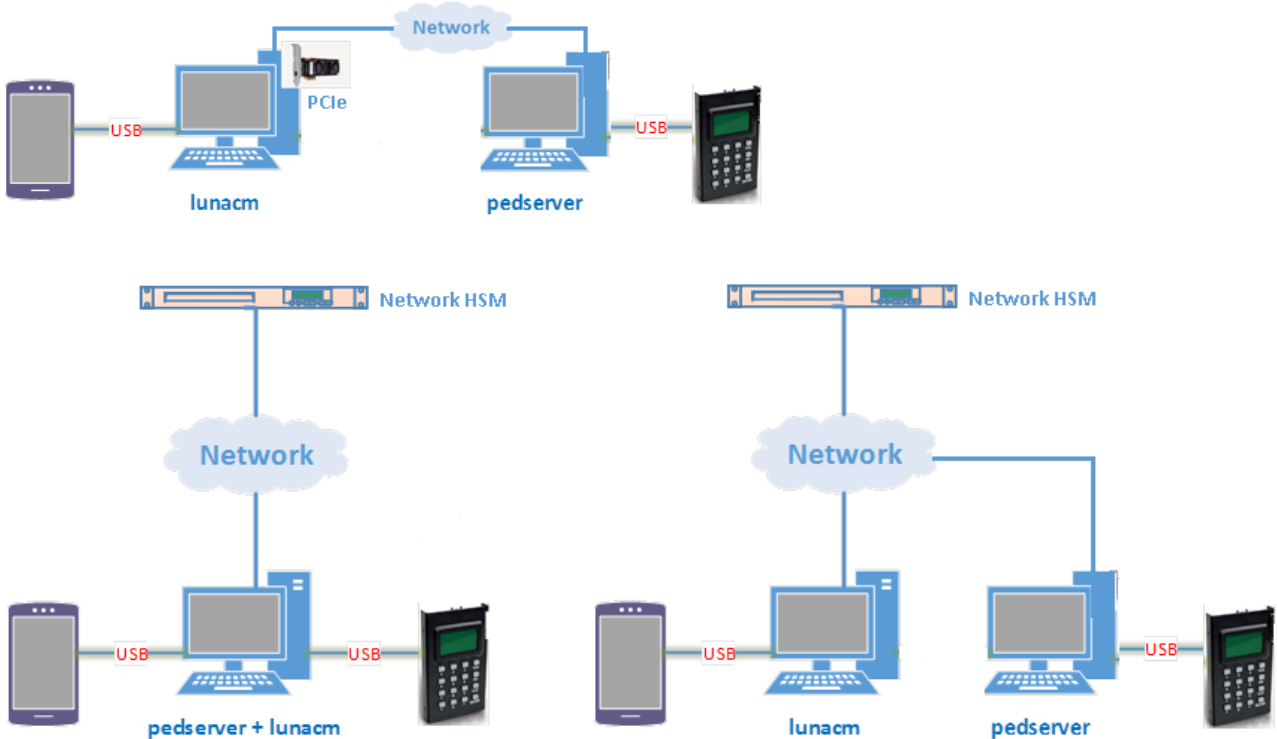
**TIP** To simplify the backup process and minimize interactions with the PED, it is recommended that you activate the CO role on the user partitions you want to backup. See ["Activation and Auto-activation on Multi-factor- \(PED-\) Authenticated Partitions" on page 299](#) for more information.

- > The following policies are set (see [HSM Capabilities and Policies](#) and ["Partition Capabilities and Policies" on page 272](#) for more information):
  - HSM policy **16: Enable network replication** must be set to **1 (ON)** on the HSM that hosts the user partition.
  - [Pre-7.7.0 and V0 partitions only] Partition policy **0: Allow private key cloning** is set to **1 (ON)** on the user partition.
  - [Pre-7.7.0 and V0 partitions only] Partition policy **4: Allow secret key cloning** is set to **1 (ON)** on the user partition.

## To backup a PED-authenticated partition

1. Configure your Luna HSM Client workstation using one of the following configurations:





- a. Install the required client software on the Luna HSM Client workstation. See ["Backing Up to a Client-Connected Luna Backup HSM \(G7\)" on page 419](#) for details.
- b. Connect the backup HSM directly to the Luna HSM Client workstation using the included USB cable.

**NOTE** On most workstations, the USB connection provides adequate power to the backup HSM and it will begin the boot sequence. If you are using a low-power workstation, such as a netbook, the USB connection may not provide adequate power, in which case you will also need to connect the external power supply.

- c. Connect the PED to the Luna HSM Client workstation used to host the remote PED, using the PED USB cable.

**NOTE** You connect to the remote PED using the IP address of the workstation used to host the PED. This can be the same workstation that hosts the user and backup partition slots, or a different workstation. The workstation used to host the PED must be running pedServer.

2. Start the **pedserver** service on the workstation used to host the remote PED:

<b>Windows</b>	C:\Program Files\Safenet\LunaClient> <b>"pedserver -mode start" on page 251</b>
<b>Linux</b>	/usr/safenet/lunaclient> <b>"pedserver -mode start" on page 251</b>

3. Launch LunaCM on the workstation that hosts the user and backup partition slots.
4. Identify the slot assignments for:
  - The <source> user partition you want to backup.

- The <target> admin partition (where all backups are stored).

lunacm:> **slot list**

If you cannot see both slots, check your connections or configure your client as required.

5. Select the <source> user partition:

lunacm:> **slot set -slot** <slot\_id>

6. Authenticate as the Crypto Officer (CO) to the <source> user partition:

- If the partition is activated, proceed as follows:

- i. Log in to the selected <source> user partition as the Crypto Officer (CO):

lunacm:> **role login -name co**

- If the partition is not activated, proceed as follows:

- i. Connect to the Luna HSM Client workstation that hosts the PED. If defaults are not **ped set**, specify an IP address (and port if required; 1503 is default).

lunacm:> **ped connect [-ip <pedserver\_host\_ip>]**

- ii. Log in to the selected <source> user partition as the Crypto Officer (CO):

lunacm:> **role login -name co**

- iii. Respond to the prompts on the PED to provide the orange (PED vector) key(s) and PIN for the <source> HSM and the black (CO) key(s) and PIN for the CO role on the <source> user partition.

- iv. Disconnect the PED session. Note that you will remain logged in to the <source> user partition:

lunacm:> **ped disconnect**

7. Select the backup HSM Admin partition:

lunacm:> **slot set -slot** <slot\_id>

8. Connect to the Luna HSM Client workstation that hosts the PED. If defaults are not **ped set**, specify an IP address (and port if required; 1503 is default):

lunacm:> **ped connect [-ip <pedserver\_host\_ip>]**

9. Select the <source> user partition:

lunacm:> **slot set -slot** <slot\_id>

10. Initiate the backup:

lunacm:> **partition archive backup -slot** <backup\_HSM\_admin\_slot> **[-partition** <target\_partition\_label>] **[-append] [-replace] [-smkonly]**

If you omit the **-partition** option when creating a new backup, the partition is assigned a default name (<source\_partition\_name>\_<YYYYMMDD>) based on the source HSM's internally-set time and date.

If you are backing up a V1 partition, include **-smkonly** to back up the SMK only. By default, the SMK and any encrypted cryptographic material on the partition are backed up.

The backup begins once you have completed the authentication process. Objects are backed up one at a time. For existing backups, you can use the following options to define how individual objects are backed up:

<b>-append</b>	Add only new objects to an existing backup.
<b>-replace</b>	Delete the existing objects in a target backup partition and replace them with the contents of the source user partition. This is the default.
<b>-append and -replace</b>	Add new objects and replace existing objects that have the same OUID but a different fingerprint (such as would occur if any of the object attributes were changed since the previous backup).

**NOTE** If the backup operation is interrupted (if the Backup HSM is unplugged, or if you fail to respond to PED prompts, for example), the Backup HSM's full available space can become occupied with a single backup partition. If this occurs, delete the backup partition with `lunacm:> partition archive delete` before reattempting the backup operation.

**11.** Respond to the prompts on the PED to insert the following keys:

- a. The blue (HSM SO) key for the backup HSM. This is an existing key that was created when the backup HSM was initialized.
- b. The blue (Partition SO) key for the <target> backup partition.
  - If this is the first time the <source> user partition is being backed up to this backup HSM, you are prompted to initialize the backup Partition SO role by creating a new key or reusing an existing key (SETTING SO PIN). After you initialize the role, you are prompted to insert the key again to log in to the role (SO LOGIN).
  - For all subsequent backups, you must present the key used to initialize the backup partition SO role.
- c. The red (Domain) key. This must be the same key used for the <source> user partition, otherwise the backup will fail.
- d. The black (Crypto Officer) key for the <target> backup partition.
  - If this is the first time the <source> user partition is being backed up to this backup HSM, you must first initialize the backup partition CO role. This requires partition SO credentials, so you are prompted for the blue (Partition SO) key. After authenticating as the partition SO, you are prompted to initialize the backup partition CO role by creating a new key or reusing an existing key (SETTING SO PIN). After you initialize the partition CO role, you are prompted to insert the key again to log in to the role (SO LOGIN).
  - For all subsequent backups, you must present the key used to initialize the backup partition CO role.

**12.** Disconnect the PED from the <source> and <target> HSMs:

- a. Disconnect the PED from the <target> backup HSM:  
`lunacm:> ped disconnect`
- b. Select the slot for the <source> user partition:  
`lunacm:> slot set -slot <slot_id>`
- c. Disconnect the PED from the <source> user partition:  
`lunacm:> ped disconnect`

13. If this is the first backup to the <target> backup partition, use the **Duplicate** function on the PED to create and label a set of backup keys for the new <target> backup partition PSO (blue) and CO (black) keys. See ["Duplicating Existing PED Keys" on page 234](#) for details.

## Backing Up a Password-Authenticated Partition

You require a password-authenticated backup HSM to backup a password-authenticated user partition.

### Summary

To perform a backup, you connect the backup HSM to the Luna HSM Client workstation that hosts the slot for the partition you want to backup, and perform the following tasks:

1. Log in to the <source> user partition as the Crypto Officer (CO).
2. Perform the backup operation and respond to the prompts for the HSM SO, partition SO (PO), crypto officer (CO), and domain passwords for the backup HSM/partition. The backup HSM and the partition you want to restore to must be members of the same domain.

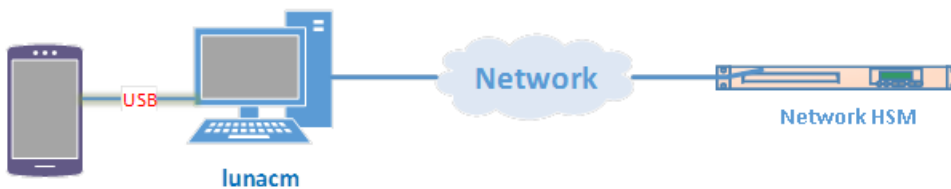
### Prerequisites

Before beginning, ensure that you have satisfied the following prerequisites:

- > You have the required credentials as listed in the summary above.
- > The following policies are set (see [HSM Capabilities and Policies](#) and ["Partition Capabilities and Policies" on page 272](#) for more information):
  - HSM policy **16: Enable network replication** must be set to **1 (ON)** on the HSM that hosts the user partition.
  - [Pre-7.7.0 and V0 partitions only] Partition policy **0: Allow private key cloning** is set to **1 (ON)** on the user partition.
  - [Pre-7.7.0 and V0 partitions only] Partition policy **4: Allow secret key cloning** is set to **1 (ON)** on the user partition.

### To backup a password-authenticated partition

1. Configure your Luna HSM Client workstation as illustrated below:



- a. Install the required client software on the Luna HSM Client workstation and start LunaCM. See ["Backing Up to a Client-Connected Luna Backup HSM \(G7\)" on page 419](#) for more information.
- b. Connect the backup HSM directly to the Luna HSM Client workstation using the included USB cable.



**NOTE** On most workstations, the USB connection provides adequate power to the backup HSM and it will begin the boot sequence. If you are using a low-power workstation, such as a netbook, the USB connection may not provide adequate power, in which case you will also need to connect the external power supply.

2. Identify the slots assigned to:

- The <source> user partition slot (to be backed up).
- The <target> admin slot (where all backups are stored).

lunacm:> **slot list**

If you cannot see both slots, check your connections or configure your client as required.

3. Select the <source> user partition:

lunacm:> **slot set -slot** <slot\_id>

4. Log in to the <source> user partition as the Crypto Officer (CO):

lunacm:> **role login -name co**

5. Initiate backup of the <source> user partition to the <target> backup partition:

lunacm:> **partition archive backup -slot** <backup\_hsm\_admin\_partition\_slot\_id> [**-partition** <target\_backup\_partition\_label>] [**-append**] [**-replace**] [**-smkonly**]

If you omit the **-partition** option when creating a new backup, the partition is assigned a default name (<source\_partition\_name>\_<YYYYMMDD>) based on the source HSM's internally-set time and date.

If you are backing up a V1 partition, include **-smkonly** to back up the SMK only. By default, the SMK and any encrypted cryptographic material on the partition are backed up.

The backup begins once you have completed the authentication process. Objects are backed up one at a time. For existing backups, you can use the following options to define how individual objects are backed up:

<b>-append</b>	Add only new objects to the existing backup.
<b>-replace</b>	Delete the existing objects in the target backup partition and replace them with the contents of the source user partition. This is the default.
<b>-append</b> and <b>-replace</b>	Add new objects and replace existing objects that have the same OUID but a different fingerprint (such as would occur if any of the object attributes were changed since the previous backup).

**NOTE** If the backup operation is interrupted (if the Backup HSM is unplugged, for example), the Backup HSM's full available space can become occupied with a single backup partition. If this occurs, delete the backup partition with lunacm:> **partition archive delete** before reattempting the backup operation.

6. You are prompted for the following (you can also enter these options on the command line, although doing so exposes the strings, whereas using the prompts obscures the strings):

- The domain string for the <target> backup partition. The domain must match the domain configured on the <source> user partition.

- The <target> backup partition password. You will create a new password on the initial backup, and use the password for subsequent backups to the <target> backup partition.
- The backup HSM SO password. This is required to create or access the backup partition in the Admin slot.

## Restoring From a Client-Connected Luna Backup HSM (G7)

Restoring objects from a backup is essentially the same as the backup procedure, except in reverse. That is, a Crypto Officer can restore the objects from a backup partition to a new or existing user partition, provided they have the credentials required to access the objects in the backup and user partitions.

The procedure is different for PED-authenticated and password-authenticated backups, as detailed in the following sections:

- > ["Restoring a Multi-factor- \(PED-\) Authenticated Partition" below](#)
- > ["Restoring a Password-Authenticated Partition" on page 429](#)

**NOTE** This feature requires minimum Luna HSM Client 10.1.0. See [Version Dependencies by Feature](#) for more information.

### Restoring a Multi-factor- (PED-) Authenticated Partition

You can restore the objects from a PED-authenticated backup partition to a PED-authenticated user partition. You can restore to an existing user partition, or you can create a new user partition and restore the objects to the new partition.

#### Summary

To restore the objects from a backup, you connect the backup HSM and a remote PED to the Luna HSM Client workstation that hosts the slot for the user partition you want to restore from backup and perform the following tasks.

1. Log in to the user partition you want to restore to as the Crypto Officer (CO):
  - If the user partition is activated, you need to provide the challenge secret.
  - If the user partition is not activated, you need to open a remote PED connection to the HSM that hosts the user partition you want to restore to, and use the required PED keys to log in to the user partition as the Crypto Officer (CO).
2. Open a remote PED connection to the backup HSM.
3. Perform the restore operation and respond to the prompts for the HSM SO, partition SO (PO), crypto officer (CO), and domain PED keys for the backup HSM/partition. The backup HSM and the partition you want to restore to must be members of the same domain.

#### Prerequisites

Before beginning, ensure that you have satisfied the following prerequisites:

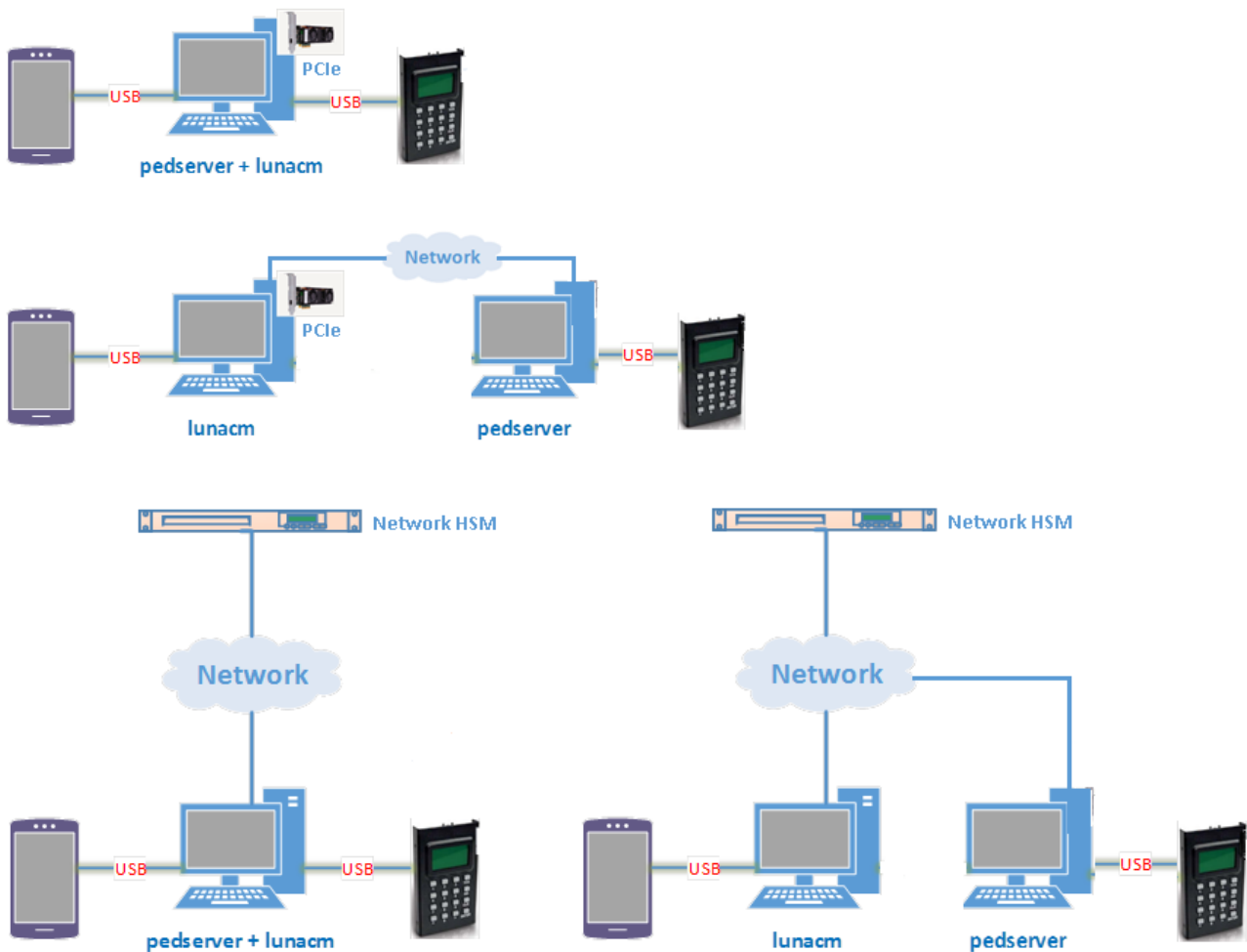
- > You are familiar with the concepts in ["PED Authentication" on page 176](#).
- > You have the credentials listed in the summary above.

**TIP** To simplify the restore process and minimize interactions with the PED, it is recommended that you activate the CO role on the user partitions you want to restore to. See "[Activation and Auto-activation on Multi-factor- \(PED-\) Authenticated Partitions](#)" on page 299 for more information.

- > The following policies are set (see [HSM Capabilities and Policies](#) and "[Partition Capabilities and Policies](#)" on page 272 for more information):
- HSM policy **16: Enable network replication** must be set to **1 (ON)** on the HSM that hosts the target user partition.
  - [Pre-7.7.0 and V0 partitions only] Partition policy **0: Allow private key cloning** must be set to **1 (ON)** on the target user partition.
  - [Pre-7.7.0 and V0 partitions only] Partition policy **4: Allow secret key cloning** must be set to **1 (ON)** on the target user partition.

### To restore a PED-authenticated partition

1. Configure your Luna HSM Client workstation using one of the following configurations:



- a. Install the required client software on the Luna HSM Client workstation. See ["Luna HSM Client Software Installation" on page 17](#) for details.
- b. Connect the backup HSM directly to the Luna HSM Client workstation using the included USB cable.

**NOTE** On most workstations, the USB connection provides adequate power to the backup HSM and it will begin the boot sequence. If you are using a low-power workstation, such as a netbook, the USB connection may not provide adequate power, in which case you will also need to connect the external power supply.

- c. Connect the PED to the Luna HSM Client workstation used to host the remote PED, using the PED USB cable.

**NOTE** You connect to the remote PED using the IP address of the workstation used to host the PED. This can be the same workstation that hosts the user and backup partition slots, or a different workstation. The workstation used to host the PED must be running **pedserver**.

2. Ensure that HSM policy **16: Enable network replication** is set to **1** on the HSM that hosts the user partition you want to restore to. See [HSM Capabilities and Policies](#) for more information.
3. Start the **pedserver** service on the workstation used to host the remote PED:

<b>Windows</b>	C:\Program Files\Safenet\LunaClient> <a href="#">"pedserver -mode start" on page 251</a>
<b>Linux</b>	/usr/safenet/lunaclient> <a href="#">"pedserver -mode start" on page 251</a>

4. Launch LunaCM on the workstation that hosts the user and backup partition slots.
5. Identify the slot assignments for:
  - the user partition you want to restore to.
  - the backup HSM admin partition (where all backups are stored).

lunacm:> [slot list](#)

If you cannot see both slots, check your connections or configure your client as required.

6. Select the user partition you want to restore from backup:

lunacm:> [slot set -slot](#) <slot\_id>

7. Authenticate as the Crypto Officer (CO) to the selected user partition:

- If the partition is activated, proceed as follows:
  - i. Log in to the selected user partition as the Crypto Officer (CO):
 

lunacm:> [role login -name co](#)
- If the partition is not activated, proceed as follows:
  - i. Connect to the Luna HSM Client workstation that hosts the PED. If defaults are not [ped set](#), specify an IP address (and port if required; 1503 is default).
 

lunacm:> [ped connect \[-ip <pedserver\\_host\\_ip>\]](#)
  - ii. Log in to the selected user partition as the Crypto Officer (CO).
 

lunacm:> [role login -name co](#)

iii. Respond to the prompts on the PED to provide the the orange (PED vector) key(s) and PIN for the HSM that hosts the user partition you want to restore from backup and the black (CO) key(s) and PIN for the CO role on the user partition you want to restore from backup.

iv. Disconnect the PED session. Note that you will remain logged in to the selected user partition.

```
lunacm:> ped disconnect
```

8. Connect the PED to the backup HSM. If defaults are not [ped set](#), specify an IP address (and port if required; 1503 is default):

```
lunacm:> ped connect [-ip <pedserver_host_ip>]
```

9. Initiate the restore operation. Respond to the prompts on the PED to insert the required PED keys.

```
lunacm:> partition archive restore -slot <backup_HSM_admin_slot> -partition <target_partition_label>
[-replace] [-smkonly]
```

The restore operation begins once you have completed the authentication process. Objects are restored one at a time. If you wish to restore previous versions of keys with the same OUID (where attributes have changed, for example), include the **-replace** option.

**NOTE** If you are restoring a V1 backup to a V1 partition, include **-smkonly** to restore the SMK only (see ["What are "pre-firmware 7.7.0", and V0, and V1 partitions?"](#) on page 126 for more information). By default, the SMK and any cryptographic material on the backup are restored.

## Restoring a Password-Authenticated Partition

You can restore the objects from a password-authenticated backup partition to a password-authenticated user partition. You can restore to an existing user partition, or you can create a new user partition and restore the objects to the new partition.

### Summary

To restore the objects from a backup, you connect the backup HSM to the Luna HSM Client workstation that hosts the slot for the user partition you want to restore from backup and perform the following tasks.

1. Log in to the user partition you want to restore to as the Crypto Officer (CO):
2. Perform the restore operation. You are prompted for the HSM SO, partition SO (PO), crypto officer (CO), and domain passwords for the backup partition. The backup partition and the partition you want to restore to must be members of the same domain.

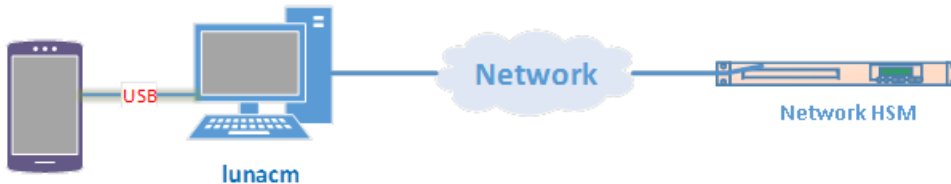
### Prerequisites

- > You have the credentials listed in the summary above.
- > The following policies are set (see [HSM Capabilities and Policies](#) and ["Partition Capabilities and Policies"](#) on page 272 for more information):
  - HSM policy **16: Enable network replication** must be set to **1 (ON)** on the HSM that hosts the target user partition.
  - [Pre-7.7.0 and V0 partitions only] Partition policy **0: Allow private key cloning** must be set to **1 (ON)** on the target user partition.

- [Pre-7.7.0 and V0 partitions only] Partition policy **4: Allow secret key cloning** must be set to **1 (ON)** on the target user partition.

### To restore a password-authenticated partition

1. Configure your Luna HSM Client workstation as illustrated below:



- a. Install the required client software on the Luna HSM Client workstation and start LunaCM. See ["Restoring From a Client-Connected Luna Backup HSM \(G7\)"](#) on page 426 for more information.
- b. Connect the backup HSM directly to the Luna HSM Client workstation using the included USB cable.

**NOTE** On most workstations, the USB connection provides adequate power to the backup HSM and it will begin the boot sequence. If you are using a low-power workstation, such as a netbook, the USB connection may not provide adequate power, in which case you will also need to connect the external power supply.

2. Ensure that HSM policy **16: Enable network replication** is set to **1** on the HSM that hosts the user partition you want to restore to. See [HSM Capabilities and Policies](#) for more information.
3. Identify the slots assigned to:
  - The user partition slot (to be restored).
  - The backup HSM admin slot (where all backups are stored).

```
lunacm:> slot list
```

If you cannot see both slots, check your connections or configure your client as required.

4. Select the user partition you want to restore to:
 

```
lunacm:> slot set -slot <slot_id>
```
5. Log in to the user partition as the Crypto Officer (CO):
 

```
lunacm:> role login -name co
```
6. List the available backups on the Backup HSM by specifying the Backup HSM's slot number. You will require the backup partition label to perform the restore operation.
 

```
lunacm:> partition archive list -slot <backup_HSM_slot>
```
7. Initiate the restore operation. Respond to the prompts to provide the required passwords, as detailed in the summary above.
 

```
lunacm:> partition archive restore -slot <backup_HSM_admin_slot> -partition <backup_partition_label> [-replace] [-smkonly]
```

The restore operation begins once you have completed the authentication process. Objects are restored one at a time. If you wish to restore previous versions of keys with the same OUID (where attributes have changed, for example), include the **-replace** option.

**NOTE** If you are restoring a V1 backup to a V1 partition, include **-smkonly** to restore the SMK only (see ["What are 'pre-firmware 7.7.0', and V0, and V1 partitions?"](#) on page 126 for more information). By default, the SMK and any encrypted cryptographic material on the backup are restored.

## Initializing an Appliance-Connected Luna Backup HSM (G7)

You must initialize the backup HSM prior to first use. You can initialize the backup HSM by connecting it to a Luna Network HSM and using LunaSH commands to perform the initialization. Initialization does the following:

- > Creates the orange (Remote PED vector) key for the backup HSM (PED-authenticated HSMs only). You create the orange key using a one-time, password-secured connection between the PED and the backup HSM. You then use this orange key to secure all subsequent connections between the PED and the backup HSM.
- > Sets the authentication mode of the HSM. The authentication mode is set automatically to the same mode as the Luna Network HSM the backup HSM is connected to when it is initialized. PED-authenticated backup HSMs can backup PED-authenticated partitions. Password-authenticated backup HSMs can backup password-authenticated partitions.
- > Sets the security domain of the HSM. You can only backup partitions that share the same domain as the backup HSM.
- > Creates the HSM SO role on the HSM (see [HSM Roles and Procedures](#).) This role is required to create or modify a backup partition, and must be logged in to perform a backup.

**NOTE** This functionality requires minimum Luna Network HSM appliance software 7.7.0. See [Version Dependencies by Feature](#) for more information. If you are using an older appliance software version, you must connect the Luna Backup HSM (G7) to a client workstation with Luna HSM Client 10.1.0 or newer.

The procedure is different for PED-authenticated and password-authenticated backups, as detailed in the following sections:

- > ["Recovering the Luna Backup HSM \(G7\) from Secure Transport Mode" below](#)
- > ["Initializing a PED-Authenticated HSM" on the next page](#)
- > ["Initializing a Password-Authenticated HSM" on page 434](#)

### Recovering the Luna Backup HSM (G7) from Secure Transport Mode

The Luna Backup HSM (G7) is shipped in Secure Transport Mode (STM). STM provides a logical check on the G7 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. For a more detailed description of STM, see [Secure Transport Mode](#).

**NOTE** Recovering the Luna Backup HSM (G7) from STM requires connecting it to a client workstation running Luna HSM Client 10.1.0 or newer.

### To recover the Luna Backup HSM (G7) from STM

1. Connect the Luna Backup HSM (G7) to a USB port on a client workstation running Luna HSM Client 10.1 or newer, with the **Backup** option installed (refer to "[Luna HSM Client Software Installation](#)" on page 17 for your client operating system).
2. Launch LunaCM on the client workstation.
3. Select the slot assigned to the Luna Backup HSM (G7) Admin partition.

```
lunacm:> slot set -slot <slot_id>
```

4. Recover the HSM from Secure Transport Mode. See [Secure Transport Mode](#) for more information about the Random User String:

```
lunacm:> stm recover -randomuserstring <string>
```

**NOTE** Recovering a Luna Backup HSM (G7) from STM may take up to three minutes.

## Initializing a PED-Authenticated HSM

Initializing your backup HSM as PED authenticated allows you to backup PED-authenticated partitions.

### Summary

To initialize a PED-authenticated HSM you connect it and a remote PED (using a USB or network connection) to a PED-authenticated Luna Network HSM, and performing the following tasks:

- > Create the orange (Remote PED vector) key for the backup HSM.
- > Initialize the HSM to set the HSM domain, and create the HSM SO PED key.

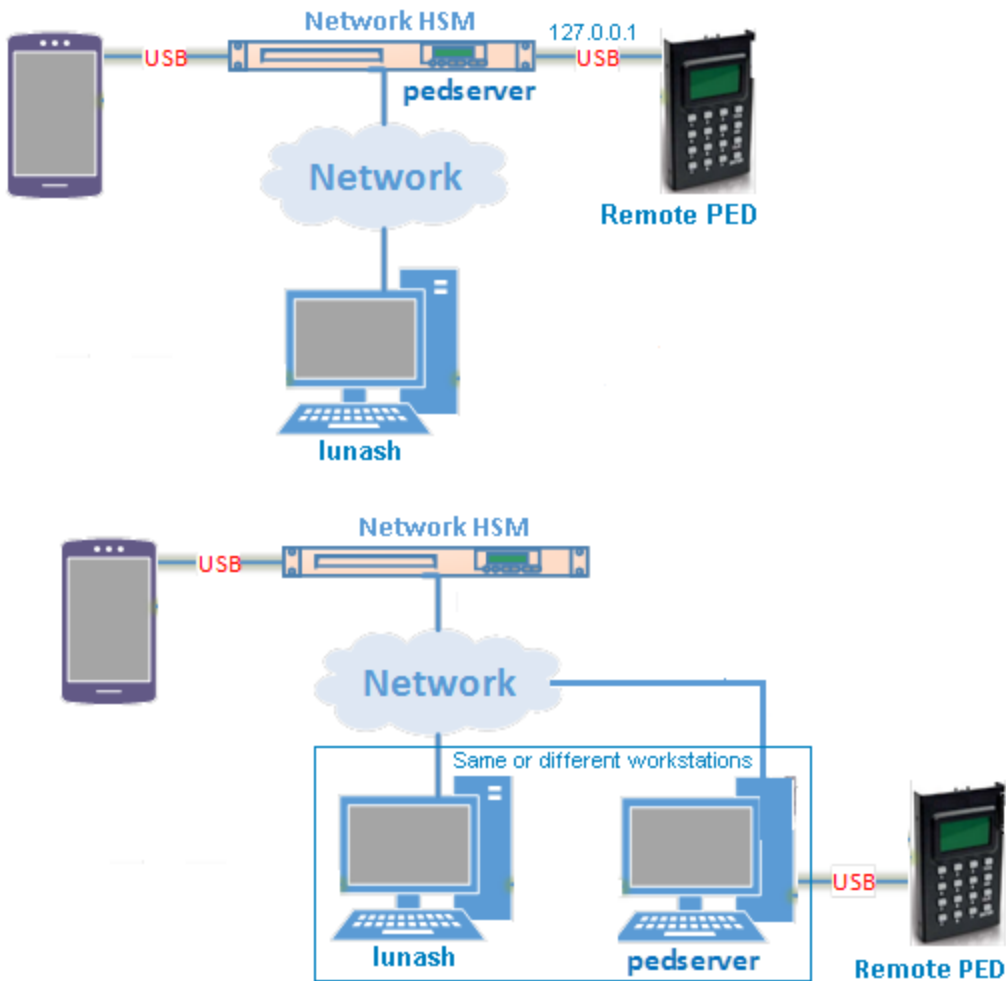
### Prerequisites

- > If necessary, recover the Luna Backup HSM (G7) from Secure Transport Mode as described in "[Recovering the Luna Backup HSM \(G7\) from Secure Transport Mode](#)" on the previous page.
- > Before beginning, ensure that you are familiar with the concepts in "[PED Authentication](#)" on page 176. You will need the following PED keys:
  - A blank orange (PED vector) PED key, plus the number required to create duplicate PED keys as necessary.
  - N number of blue (HSM SO) PED keys, as defined by the M of N scheme you choose for the HSM SO role, plus the number required to create duplicate PED keys as necessary.
  - An existing red (Domain) PED key for the cloning domain of the partitions you want to backup to the HSM. You can also insert a blank red (Domain) PED key if you want to create a new domain for the HSM (although you won't be able to backup any existing partitions if you do).

### To initialize a PED-authenticated Backup HSM

1. Configure your PED-authenticated Luna Network HSM using one of the following configurations:





- a. Open a network (SSH) or serial connection to the appliance and log in as **admin**, or other admin-level user, to start a LunaSH session.
- b. Connect the backup HSM directly to one of the USB ports on the Luna Network HSM appliance using the included USB cable.
- c. Connect the Remote PED to the Luna Network HSM appliance. You can connect a Remote PED directly to one of the USB ports on the Luna Network HSM appliance using the included USB cable, or you can connect to a network-attached Luna HSM Client workstation that hosts a remote PED:
  - If you connect the Remote PED directly to a USB port on the appliance, use the appliance loopback IP address (127.0.0.1) to connect to the local **pedserver** service running on the appliance, and specify the serial number of the connected backup HSM you want to use. You can read the serial number from the Backup HSM display screen. The **pedserver** service must be running on the appliance. You can use the `lunash:> service` commands to administer the service:
 

```
lunash:> hsm ped connect -ip 127.0.0.1 -serial <backup_hsm_serial_number>
```
  - If you are using a network-attached Remote PED, connect to the IP address of the workstation used to host the Remote PED. This can be the same workstation you are using to host the LunaSH session, or a different workstation.
 

```
lunash:> hsm ped connect -ip <pedserver_host>
```

**NOTE** You can connect the backup HSM to any USB port on the Luna Network HSM appliance (see [Physical Features](#)). Do not attempt to connect the backup HSM to the USB port on the HSM card.

- Get the serial number of the backup HSM, or read the serial number from the Backup HSM display screen.

```
lunash:> token backup list
```

- Create a Remote PED Vector (orange) PED key for the backup HSM:

```
lunash:> hsm ped vector init -serial <backup_hsm_serial_number>
```

LunaSH generates and displays a one-time password that is used to set up a secure channel between the backup HSM and the PED, allowing you to securely initialize the orange (Remote PED Vector) key. Enter the displayed password on the PED when prompted to complete setup of the secure channel and respond to the prompts to create the Remote PED Vector (orange) PED key.

Please attend to the PED and enter following password: 94485995

**CAUTION!** The orange PED key is required for all Luna G7 Backup HSM operations. If this key is lost, your backups will become irretrievable. Thales recommends keeping multiple backups of all PED keys stored in a secure location.

- Initialize the backup HSM:

```
lunash:> token backup init -label <backup_hsm_label> -serial <backup_hsm_serial_number>
```

You are prompted by the PED for the red Domain key(s) (existing or new) and black HSM SO key(s) (new). Respond to the PED prompts and insert and set the PINs on the required keys when requested. Ensure that you label any new PED keys that you create during this process.

- Use the **Duplicate** function on the PED to create and label duplicates of the new PED keys, as required. See ["Duplicating Existing PED Keys"](#) on page 234 for details.

- Disconnect the PED when done:

- If you connected the Remote PED directly to a USB port on the appliance:

```
lunash:> hsm ped disconnect -serial <backup_hsm_serial_number>
```

- If you connected to a network-attached Remote PED:

```
lunash:> hsm ped disconnect
```

## Initializing a Password-Authenticated HSM

Initializing your backup HSM as password-authenticated allows you to backup password-authenticated partitions.

### Summary

To initialize a password-authenticated HSM you connect it to a password-authenticated Luna Network HSM and perform the following tasks:

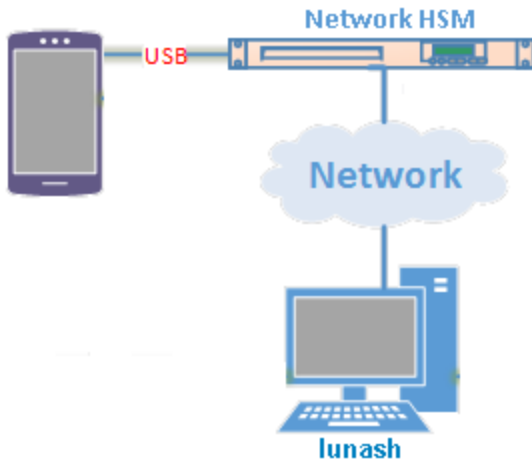
- > Initialize the HSM to set the HSM domain, and set the initial password for the HSM SO role.

## Prerequisites

- > If necessary, recover the Luna Backup HSM (G7) from Secure Transport Mode as described in ["Recovering the Luna Backup HSM \(G7\) from Secure Transport Mode" on page 431](#).
- > You require the password for the cloning domain of the partitions you want to backup to the HSM. You can also enter a new password to create a new domain for the HSM (although you won't be able to backup any existing partitions if you do).

## To initialize a password-authenticated HSM

1. Configure your password-authenticated Luna Network HSM as illustrated below:



- a. Open a network (SSH) or serial connection to the appliance and log in as **admin**, or other admin-level user, to start a LunaSH session.
  - b. Connect the backup HSM directly to the Luna Network HSM using the included USB cable.
2. Get the serial number of the backup HSM, or read the serial number from the Backup HSM display screen.

```
lunash:> token backup list
```

3. Initialize the backup HSM:

```
lunash:> token backup init -label <backup_hsm_label> -serial <backup_hsm_serial_number>
```

You are prompted for the new HSM SO password and the HSM domain string (existing or new).

## Backing Up to an Appliance-Connected Luna Backup HSM (G7)

You can connect a Luna Backup HSM (G7) to a USB port on the Luna Network HSM appliance to allow a Crypto Officer (CO) to use LunaSH (via a serial or SSH connection to the appliance) to backup the objects on any partition the CO can log in to on the appliance. You can connect the backup HSM to the Luna Network HSM only when you want to perform a backup/restore, or you can leave the backup HSM connected to the appliance to enable remote backups.

**NOTE** This functionality requires minimum Luna appliance software 7.7.0. See [Version Dependencies by Feature](#) for more information.

- > If you are backing up or restoring encrypted blobs stored on a V1 partition, the Backup HSM must be connected to the client (see ["Backup/Restore Using a Client-Connected Luna Backup HSM \(G5\)" on page 401](#)). Only the SMK can be backed up/restored using an appliance-connected Backup HSM.
- > If partition policy **37: Force Secure Trusted Channel** is enabled on the partition, the Backup HSM must be connected to the client (see ["Backup/Restore Using a Client-Connected Luna Backup HSM \(G5\)" on page 401](#)).

To perform a backup/restore, you connect the backup HSM to a USB port on the Luna Network HSM that hosts the partition you want to backup, and run the LunaSH **partition backup** or **partition restore** commands.

Backups are created and stored as partitions within the Admin partition on the backup HSM. A new backup partition is created on initial backup. For subsequent backups, you can choose to replace the contents of the existing <target> backup partition with the current <source> user partition objects, or add new objects in the <source> user partition to the existing <target> backup partition. You can restore a backup to a new or existing user partition that shares the same domain as the backup partition.

In addition to the credentials listed in ["Backup and Restore Using a Luna Backup HSM \(G7\)" on page 408](#), the Crypto Officer requires **admin**-level access to the appliance to access the LunaSH **partition backup** and **partition restore** commands (see [Appliance Roles and Procedures](#)).

**NOTE** To perform backup operations on HSM firmware 7.7.0 or newer (V0 or V1 partitions):

- > Luna Backup HSM (G7) requires minimum firmware version 7.7.1
- > Luna Backup HSM (G5) requires minimum firmware version 6.28.0

You can use a Luna Backup HSM with older firmware to restore objects to a V0 or V1 partition, but this is supported for purposes of getting your objects from the older partitions onto the newer V0 or V1 partitions only.

V0 and V1 partitions are considered more secure than partitions at earlier firmware versions - any attempt to restore from a higher-security status to lower-security status fails gracefully.

SMK backup for appliance is supported only with local connection.

The procedure is different for PED-authenticated and password-authenticated backups, as detailed in the following sections:

- > ["Backing Up a PED-Authenticated Partition" below](#)
- > ["Backing Up a Password-Authenticated Partition" on page 440](#)

## Backing Up a PED-Authenticated Partition

You require a PED-authenticated backup HSM to backup a PED-authenticated user partition. You also require a remote PED, which you connect directly to one of the USB ports on the Luna Network HSM appliance using the included USB cable, or remotely to a network-attached Luna HSM Client workstation that hosts a remote PED:

**NOTE** A remote PED connected to the USB port on the appliance uses the appliance **pedserver** service. If the PED is not responding, use the `lunash:> service` commands to verify the service status and restart if necessary. The PED must be in Remote mode.

### Summary

To perform a backup, you connect the backup HSM and a remote PED (using a USB or network connection) to the Luna Network HSM appliance that hosts the slot for the user partition you want to backup, and perform the following tasks, as detailed in ["To backup a PED-authenticated partition" on the next page](#):

1. Log in to the appliance (LunaSH) as **admin**, or other admin-level user.
2. Connect the Remote PED (**hsm ped connect**) to the appliance loopback IP (127.0.0.1) or remote host IP.
3. Perform the backup operation (**partition backup**) and respond to the prompts for the following PED keys:

<b>&lt;source&gt; partition</b>	<ul style="list-style-type: none"> <li>&gt; Remote PED Vector (orange)</li> <li>&gt; Crypto officer (CO) (black)</li> </ul>
<b>&lt;target&gt; backup partition</b>	<ul style="list-style-type: none"> <li>&gt; Remote PED Vector (orange)</li> <li>&gt; HSM SO (blue)</li> <li>&gt; Partition SO (PO) (blue)</li> <li>&gt; Crypto officer (CO) (black)</li> <li>&gt; Domain (red).</li> </ul>

### Prerequisites

Before beginning, ensure that you have satisfied the following prerequisites:

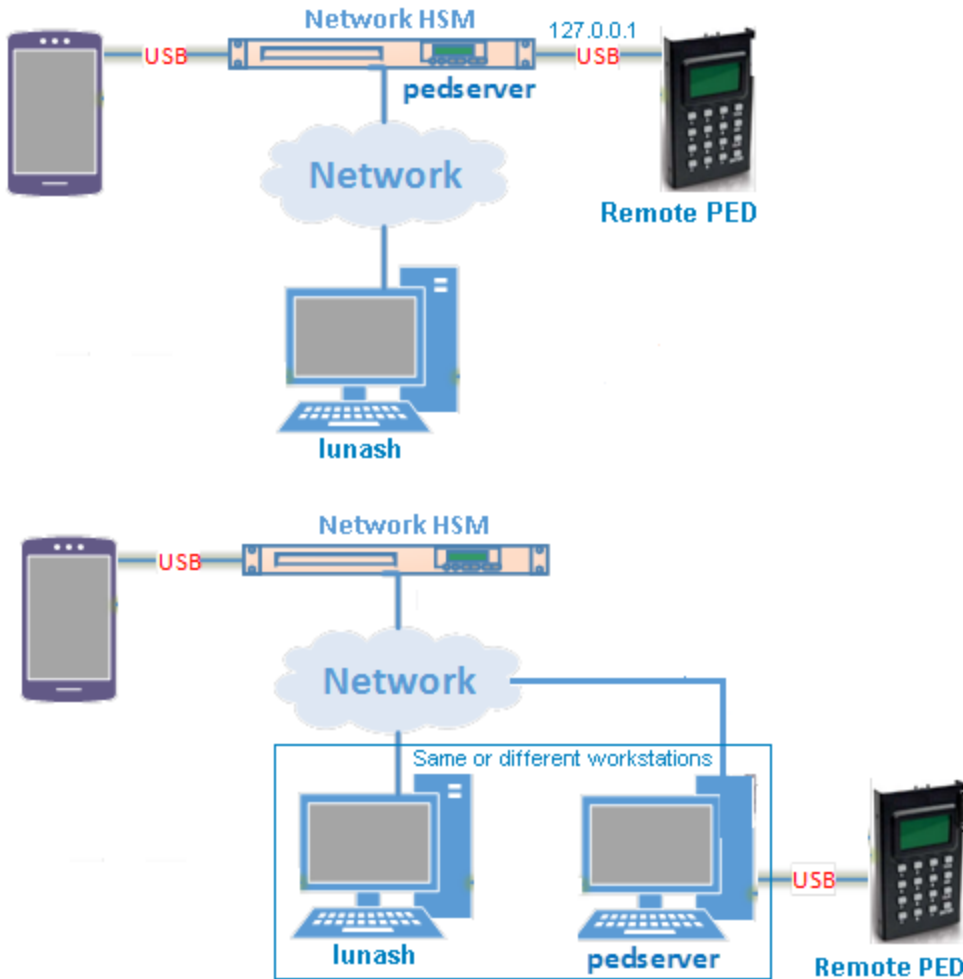
- > You are familiar with the concepts in ["PED Authentication" on page 176](#).

**TIP** To simplify the backup process and minimize interactions with the PED, it is recommended that you activate the CO role on the user partitions you want to backup. See ["Activation and Auto-activation on Multi-factor- \(PED-\) Authenticated Partitions" on page 299](#) for more information.

- > You are able to log in to the Luna Network HSM using an **admin**-level account to access LunaSH.
- > You have the required credentials as listed in the summary above.
- > The following policies are set (see [HSM Capabilities and Policies](#) and ["Partition Capabilities and Policies" on page 272](#) for more information):
  - HSM policy **16: Enable network replication** must be set to **1 (ON)** on the HSM that hosts the user partition.
  - [Pre-7.7.0 and V0 partitions only] Partition policy **0: Allow private key cloning** is set to **1 (ON)** on the user partition.
  - [Pre-7.7.0 and V0 partitions only] Partition policy **4: Allow secret key cloning** is set to **1 (ON)** on the user partition.

## To backup a PED-authenticated partition

1. Configure your Luna Network HSM appliance using one of the following configurations:



- a. Open a network (SSH) or serial connection to the appliance and log in as **admin**, or other admin-level user, to start a LunaSH session.
- b. Connect the backup HSM directly to one of the USB ports on the Luna Network HSM appliance using the included USB cable.
- c. Connect the Remote PED to the Luna Network HSM appliance. You can connect a Remote PED directly to one of the USB ports on the Luna Network HSM appliance using the included USB cable, or you can connect to a network-attached Luna HSM Client workstation that hosts a remote PED:
  - If you connect the Remote PED directly to a USB port on the appliance, use the appliance loopback IP address (127.0.0.1) to connect to the local **pedserver** service running on the appliance, and specify the serial number of the connected backup HSM you want to use. The **pedserver** service must be running on the appliance. You can use the `lunash:> service` commands to administer the service:
 

```
lunash:> hsm ped connect -ip 127.0.0.1 -serial <backup_hsm_serial_number>
```
  - If you are using a network-attached Remote PED, connect to the IP address of the workstation used to host the Remote PED. This can be the same workstation you are using to host the LunaSH session, or a different workstation.

```
lunash:> hsm ped connect -ip <remote_ped_host_ip_address>
```

**NOTE** You can connect the backup HSM to any USB port on the Luna Network HSM appliance (see [Physical Features](#)). Do not attempt to connect the backup HSM to the USB port on the HSM card.

- Get the serial number of the backup HSM, or read the serial number from the backup HSM display screen.

```
lunash:> token backup list
```

- Initiate the backup operation:

```
lunash:> partition backup -partition <source_partition_label> -serial <backup_hsm_serial_number> [-tokenpar <target_backup_partition_label>] [-add | -replace]
```

**NOTE** You must specify **-add** or **-replace** when backing up to an existing backup partition. Use **-add** to add only new objects. Use **-replace** to add new objects and overwrite existing objects. You do not need to specify these options when backing up a V1 partition, as only the SMK is backed up.

If you omit the **-tokenpar** option when creating a new backup, the partition is assigned a default name (<source\_partition\_name>\_<YYYYMMDD>) based on the source HSM's internally-set time and date.

If the backup operation is interrupted (if the Backup HSM is unplugged, or if you fail to respond to PED prompts, for example), the Backup HSM's full available space can become occupied with a single backup partition. If this occurs, delete the backup partition with `lunash:> token backup partition delete` before reattempting the backup operation.

- Respond to the prompts on the PED to insert the following keys:

<b>&lt;source&gt; partition</b>	<ul style="list-style-type: none"> <li>&gt; Remote PED Vector (orange)</li> <li>&gt; Crypto officer (CO) (black). If the partition is activated, you are prompted to provide the challenge password only. You do not need to provide the PED key.</li> </ul>
-------------------------------------	--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

<b>&lt;target&gt; backup partition</b>	<ul style="list-style-type: none"> <li>&gt; Remote PED Vector (orange). This is an existing key that was created when the backup HSM was initialized.</li> <li>&gt; HSM SO (blue). This is an existing key that was created when the backup HSM was initialized.</li> <li>&gt; Partition SO (PO) (blue). <ul style="list-style-type: none"> <li>• If this is the first time the &lt;source&gt; user partition is being backed up to this backup HSM, you are prompted to initialize the backup Partition SO role by creating a new key or reusing an existing key (SETTING SO PIN). After you initialize the role, you are prompted to insert the key again to log in to the role (SO LOGIN).</li> <li>• For all subsequent backups, you must present the key used to initialize the backup partition SO role.</li> </ul> </li> <li>&gt; Crypto officer (CO) (black): <ul style="list-style-type: none"> <li>• If this is the first time the &lt;source&gt; user partition is being backed up to this backup HSM, you must first initialize the backup partition CO role. This requires partition SO credentials, so you are prompted for the blue (Partition SO) key. After authenticating as the partition SO, you are prompted to initialize the backup partition CO role by creating a new key or reusing an existing key (SETTING SO PIN). After you initialize the partition CO role, you are prompted to insert the key again to log in to the role (SO LOGIN).</li> <li>• For all subsequent backups, you must present the key used to initialize the backup partition CO role.</li> </ul> </li> <li>&gt; Domain (red). The backup HSM and the partition you want to backup must be members of the same domain.</li> </ul>
------------------------------------------------	------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

The backup begins once you have completed the authentication process. Objects are backed up one at a time.

**5.** Disconnect the PED when done:

- If you connected the Remote PED directly to a USB port on the appliance:

```
lunash:> hsm ped disconnect -serial <backup_hsm_serial_number>
```

- If you connected to a network-attached Remote PED:

```
lunash:> hsm ped disconnect
```

**6.** If this is the first backup to the <target> backup partition, use the **Duplicate** function on the PED to create and label a set of backup keys for the new <target> backup partition PSO (blue) and CO (black) keys. See ["Duplicating Existing PED Keys" on page 234](#) for details.

## Backing Up a Password-Authenticated Partition

You require a password-authenticated backup HSM to backup a password-authenticated user partition.

### Summary

To perform a backup, you connect the backup HSM and a remote PED (using a USB or network connection) to the Luna Network HSM appliance that hosts the slot for the user partition you want to backup, and perform the following tasks, as detailed in ["To backup a password-authenticated partition " on the next page](#):

1. Log in to the appliance (LunaSH) as **admin**, or other admin-level user.
2. Perform the backup operation (**partition backup**) and respond to the prompts for the following passwords:



<source> partition	> Crypto officer (CO)
<target> backup partition	> HSM SO > Partition SO (PO) > Domain. The backup HSM and the partition you want to backup must be members of the same domain.

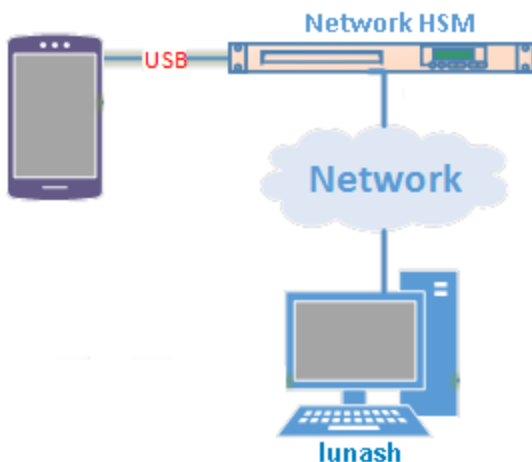
## Prerequisites

Before beginning, ensure that you have satisfied the following prerequisites:

- > You are able to log in to the Luna Network HSM using an **admin**-level account to access LunaSH.
- > You have the required credentials as listed in the summary above.
- > The following policies are set (see [HSM Capabilities and Policies](#) and "[Partition Capabilities and Policies](#)" on page 272 for more information):
  - HSM policy **16: Enable network replication** must be set to **1 (ON)** on the HSM that hosts the user partition.
  - [Pre-7.7.0 and V0 partitions only] Partition policy **0: Allow private key cloning** is set to **1 (ON)** on the user partition.
  - [Pre-7.7.0 and V0 partitions only] Partition policy **4: Allow secret key cloning** is set to **1 (ON)** on the user partition.

## To backup a password-authenticated partition

1. Configure your Luna Network HSM as illustrated below:



- a. Open a network (SSH) or serial connection to the appliance and log in as **admin**, or other admin-level user, to start a LunaSH session.
  - b. Connect the backup HSM directly to the Luna Network HSM using the included USB cable.
2. Get the serial number of the backup HSM, or read the serial number from the Backup HSM display screen.

```
lunash:> token backup list
```

3. Initiate the backup operation:

```
lunash:> partition backup -partition <source_partition_label> -serial <backup_hsm_serial_number> [-tokenpar <target_backup_partition_label>] [-add | -replace]
```

**NOTE** You must specify **-add** or **-replace** when backing up to an existing backup partition. Use **-add** to add only new objects. Use **-replace** to add new objects and overwrite existing objects. You do not need to specify these options when backing up a V1 partition, as only the SMK is backed up.

If you omit the **-tokenpar** option when creating a new backup, the partition is assigned a default name (<source\_partition\_name>\_<YYYYMMDD>) based on the source HSM's internally-set time and date.

If the backup operation is interrupted (if the Backup HSM is unplugged, for example), the Backup HSM's full available space can become occupied with a single backup partition. If this occurs, delete the backup partition with lunash:> **token backup partition delete** before reattempting the backup operation.

#### 4. Respond to the prompts for the following passwords:

<b>&lt;source&gt; partition</b>	> Crypto officer (CO)
<b>&lt;target&gt; backup partition</b>	<ul style="list-style-type: none"> <li>&gt; HSM SO. This is an existing password that was created when the backup HSM was initialized. It is required to create or access the backup partition in the Admin slot.</li> <li>&gt; Partition SO (PO). You will create a new password on the initial backup, and use the password for subsequent backups to the &lt;target&gt; backup partition.</li> <li>&gt; Domain. The backup HSM and the partition you want to backup must be members of the same domain.</li> </ul>

The backup begins once you have completed the authentication process. Objects are backed up one at a time.

## Restoring From an Appliance-Connected Luna Backup HSM (G7)

Restoring objects from a backup is essentially the same as the backup procedure, except in reverse. That is, a Crypto Officer can restore the objects from a backup partition to a new or existing user partition, provided they have the credentials required to access the objects in the backup and user partitions.

**NOTE** This functionality requires minimum Luna appliance software 7.7.0. See [Version Dependencies by Feature](#) for more information.

- > If you are backing up or restoring encrypted blobs stored on a V1 partition, the Backup HSM must be connected to the client (see "[Backup/Restore Using a Client-Connected Luna Backup HSM \(G5\)](#)" on page 401). Only the SMK can be backed up/restored using an appliance-connected Backup HSM.
- > If partition policy **37: Force Secure Trusted Channel** is enabled on the partition, the Backup HSM must be connected to the client (see "[Backup/Restore Using a Client-Connected Luna Backup HSM \(G5\)](#)" on page 401).

The procedure is different for PED-authenticated and password-authenticated backups, as detailed in the following sections:

- > ["Restoring a PED-Authenticated Partition" below](#)
- > ["Restoring a Password-Authenticated Partition" on page 446](#)

## Restoring a PED-Authenticated Partition

You can restore the objects from a PED-authenticated backup partition to a PED-authenticated user partition. You can restore to an existing user partition, or you can create a new user partition and restore the objects to the new partition.

### Summary

To restore the objects from a backup, you connect the backup HSM and a remote PED (either locally using USB or remotely using [hsm ped connect](#)) to the Luna Network HSM appliance that hosts the slot for the user partition you want to restore to, and perform the following tasks, as detailed in ["To restore a PED-authenticated partition" on the next page](#):

1. Log in to the appliance (LunaSH) as **admin**, or other admin-level user.
2. Perform the restore operation ([partition restore](#)) and respond to the prompts for the following PED keys:

<b>&lt;source&gt; backup partition</b>	<ul style="list-style-type: none"> <li>&gt; Remote PED Vector (orange)</li> <li>&gt; HSM SO (blue)</li> <li>&gt; Partition SO (PO) (blue)</li> <li>&gt; Crypto officer (CO) (black)</li> <li>&gt; Domain (red)</li> </ul>
<b>&lt;target&gt; user partition</b>	<ul style="list-style-type: none"> <li>&gt; Remote PED Vector (orange)</li> <li>&gt; Crypto officer (CO) (black)</li> </ul>

### Prerequisites

Before beginning, ensure that you have satisfied the following prerequisites:

- > You are familiar with the concepts in ["PED Authentication" on page 176](#).
- > You have the required credentials listed in the summary above.

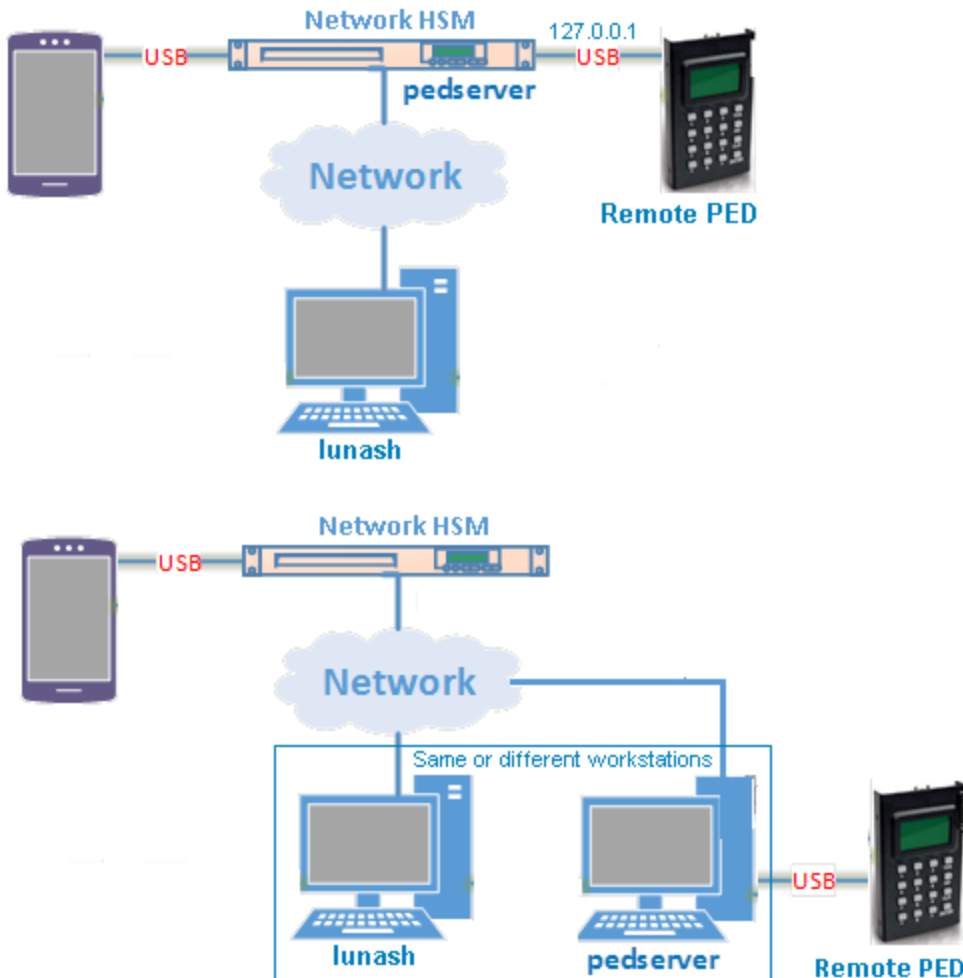
**TIP** To simplify the restore process and minimize interactions with the PED, it is recommended that you activate the CO role on the user partitions you want to restore to. See ["Activation and Auto-activation on Multi-factor- \(PED-\) Authenticated Partitions" on page 299](#) for more information.

- > You are able to log in to the Luna Network HSM using an **admin**-level account to access LunaSH.
- > The following policies are set (see [HSM Capabilities and Policies](#) and ["Partition Capabilities and Policies" on page 272](#) for more information):
  - HSM policy **16: Enable network replication** must be set to **1 (ON)** on the HSM that hosts the user partition you want to restore to.

- [Pre-7.7.0 and V0 partitions only] Partition policy **0: Allow private key cloning** must be set to **1 (ON)** on the user partition you want to restore to.
- [Pre-7.7.0 and V0 partitions only] Partition policy **4: Allow secret key cloning** must be set to **1 (ON)** on the user partition you want to restore to.

### To restore a PED-authenticated partition

1. Configure your Luna HSM Client workstation using one of the following configurations:



- a. Open a network (SSH) or serial connection to the appliance and log in as **admin**, or other admin-level user, to start a LunaSH session.
- b. Connect the backup HSM directly to one of the USB ports on the Luna Network HSM appliance using the included USB cable.
- c. Connect the Remote PED to the Luna Network HSM appliance. You can connect a Remote PED directly to one of the USB ports on the Luna Network HSM appliance using the included USB cable, or you can connect to a network-attached Luna HSM Client workstation that hosts a remote PED.
  - If you connect the Remote PED directly to a USB port on the appliance, use the appliance loopback IP address (127.0.0.1) to connect to the local **pedserver** service running on the appliance, and specify

the serial number of the connected backup HSM you want to use. The **pedserver** service must be running on the appliance. You can use the `lunash:> service` commands to administer the service:

```
lunash:> hsm ped connect -ip 127.0.0.1 -serial <backup_hsm_serial_number>
```

- If you are using a network-attached Remote PED, use to connect to the IP address of the workstation used to host the Remote PED. This can be the same workstation you are using to host the LunaSH session, or a different workstation.

```
lunash:> hsm ped connect
```

**NOTE** You can connect the backup HSM to any USB port on the Luna Network HSM appliance (see [Physical Features](#)). Do not attempt to connect the backup HSM to the USB port on the HSM card.

2. Get the serial number of the backup HSM, or read the serial number from the Backup HSM display screen:

```
lunash:> token backup list
```

3. Initiate the restore operation:

```
lunash:> partition restore -partition <target_user_partition_label> -tokenpar <source_backup_partition_label> -serial <backup_hsm_serial_number> {-add | -replace}
```

Use the **-add** option to add only new objects, or the **-replace** option to add new objects and overwrite existing objects.

**CAUTION!** If you are restoring a V1 backup to a V1 partition, use **-add** to restore the SMK. Use **-replace** only if you wish to erase any existing cryptographic material on the target partition. By default, V1 backups only include the SMK.

4. Respond to the prompts on the PED to insert the following keys:

<b>&lt;source&gt; backup partition</b>	<ul style="list-style-type: none"> <li>&gt; Remote PED Vector (orange). This is an existing key that was created when the backup HSM was initialized.</li> <li>&gt; HSM SO (blue). This is an existing key that was created when the backup HSM was initialized.</li> <li>&gt; Partition SO (PO) (blue). This is an existing key that was created when the backup partition was created.</li> <li>&gt; Crypto officer (CO) (black). This is an existing key that was created when the backup partition was created.</li> <li>&gt; Domain (red). The backup HSM and the partition you want to backup must be members of the same domain.</li> </ul>
<b>&lt;target&gt; user partition</b>	<ul style="list-style-type: none"> <li>&gt; Remote PED Vector (orange). This is an existing key that was created when the Luna Network HSM was initialized.</li> <li>&gt; Crypto officer (CO) (black). This is an existing key that was created when the user partition was created. If the partition is activated, you are prompted to provide the challenge password only. You do not need to provide the PED key.</li> </ul>

The restore operation begins once you have completed the authentication process. Objects are restored one at a time.

5. Disconnect the PED when done:

- If you connected the Remote PED directly to a USB port on the appliance:  
lunash:> **hsm ped disconnect -serial** <backup\_hsm\_serial\_number>
- If you connected to a network-attached Remote PED:  
lunash:> **hsm ped disconnect**

## Restoring a Password-Authenticated Partition

You can restore the objects from a password-authenticated backup partition to a password-authenticated user partition. You can restore to an existing user partition, or you can create a new user partition and restore the objects to the new partition.

### Summary

To restore the objects from a backup, you connect the backup HSM to the Luna Network HSM appliance that hosts the slot for the user partition you want to restore to, and perform the following tasks, as detailed in ["To restore a password-authenticated partition" below](#):

1. Log in to the appliance (LunaSH) as **admin**, or other admin-level user.
2. Perform the restore operation (**partition restore**) and respond to the prompts for the following passwords:

<source> backup partition	<ul style="list-style-type: none"> <li>&gt; HSM SO.</li> <li>&gt; Partition SO (PO).</li> <li>&gt; Crypto officer (CO).</li> <li>&gt; Domain.</li> </ul>
<target> user partition	<ul style="list-style-type: none"> <li>&gt; Crypto officer (CO).</li> </ul>

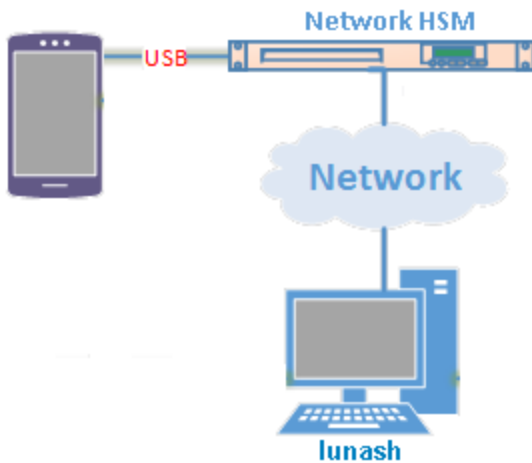
### Prerequisites

Before beginning, ensure that you have satisfied the following prerequisites:

- > You have the credentials listed in the summary above.
- > You are able to log in to the Luna Network HSM appliance using an **admin**-level account to access LunaSH.
- > [Pre-7.7.0 and V0 partitions only] The following policies are set (see [HSM Capabilities and Policies](#) and ["Partition Capabilities and Policies" on page 272](#) for more information):
  - HSM policy **16: Enable network replication** must be set to **1 (ON)** on the HSM that hosts the user partition you want to restore to.
  - Partition policy **0: Allow private key cloning** must be set to **1 (ON)** on the user partition you want to restore to.
  - Partition policy **4: Allow secret key cloning** must be set to **1 (ON)** on the user partition you want to restore to.

### To restore a password-authenticated partition

1. Configure your Luna Network HSM as illustrated below:



- a. Open a network (SSH) or serial connection to the appliance and log in as **admin**, or other admin-level user, to start a LunaSH session.
  - b. Connect the backup HSM directly to the Luna Network HSM using the included USB cable.
2. Initiate the restore operation:

```
lunash:> partition restore -partition <target_user_partition_label> -tokenpar <backup_partition_label> -serial <backup_hsm_serial_number> {-add | -replace}
```

Use the **-add** option to add only new objects, or the **-replace** option to add new objects and overwrite existing objects.

**CAUTION!** If you are restoring a V1 backup to a V1 partition, use **-add** to restore the SMK. Use **-replace** only if you wish to erase any existing cryptographic material on the target partition. By default, V1 backups only include the SMK.

3. Respond to the prompts for the following passwords:

<source> backup partition	> Crypto officer (CO). This is an existing password that was created when the backup partition was created.
<target> user partition	> Crypto officer (CO). This is an existing password that was created when the user partition was created.

The restore operation begins once you have completed the authentication process. Objects are restored one at a time.

## Backup and Restore to a Remote Backup Service (RBS)-Connected Luna Backup HSM (G7)

The Remote Backup Service (RBS) is an optional Luna client component that allows you to connect one or more backup HSMs to a remote Luna client workstation to backup the slots on any local Luna HSM Client workstations that are registered with the RBS server. RBS is useful in deployments where backups are stored in a separate location from the Luna Network HSM, to protect against catastrophic loss (fire, flood, etc).

RBS is a utility, included with the Luna HSM Client software, that runs on a workstation hosting one or more Backup HSMs. When RBS is configured and running, other clients or HSMs registered to it can see its Backup HSM(s) as slots in LunaCM.

## Installing and Configuring the Remote Backup Service

RBS is installed using the Luna HSM Client installer. You must create a certificate for the RBS workstation and register it on all clients/appliances that will use the remote Backup HSMs. These instructions will allow you to install and configure RBS.

**NOTE** The Luna HSM Client version installed on the RBS workstation must be the same version installed on the client workstation(s). Ensure that you use a client version that is compatible with your Backup HSM firmware.

This feature requires minimum Luna HSM Client version 10.1.0, or 10.3.0 if you are using Luna Backup HSM (G7) firmware 7.7.1 or newer. See [Version Dependencies by Feature](#) for more information.

### Prerequisites

- > Install the following Luna HSM Client components on any Luna Network HSM client workstation that hosts slots for the partitions you want to backup using RBS (see "[Luna HSM Client Software Installation](#)" on [page 17](#)):
  - **Network**
  - **Remote PED:** if you are backing up PED-authenticated partitions.
- > Connect the backup HSM(s) directly to the Luna HSM Client workstation that will host RBS using the included USB cable.

**NOTE** On most workstations, the USB 3.0 connection provides adequate power to the backup HSM and it will begin the boot sequence. If you are using a low-power workstation, such as a netbook, the USB connection may not provide adequate power, in which case you will also need to connect the external power supply. It is recommended that you use the power supply for all backup HSMs connected to the RBS host workstation. If you are connecting multiple backup HSMs, you can use an external USB 3.0 hub if required.

- > Initialize the backup HSMs if necessary. See "[Initializing a Client-Connected Luna Backup HSM \(G7\)](#)" on [page 414](#).
- > Ensure that **HSM Policy 16: Enable Network Replication** is allowed on the HSMs used to host the partitions you want to backup. This is the default setting.

### To install and configure RBS

1. On the workstation hosting the Backup HSM(s), install the **Backup** component of the Luna HSM Client (see "[Luna HSM Client Software Installation](#)" on [page 17](#)). If this workstation will also host a Remote PED, install the **Remote PED** component as well (Windows only).
2. Navigate to the Luna HSM Client home directory (`/usr/safenet/lunaclient/rbs/bin` on Linux/Unix) and generate a certificate for the RBS host.



**> rbs --genkey**

You are prompted to enter and confirm an RBS password. The certificate is generated in:

- Linux/UNIX: <LunaClient\_install\_directory>/rbs/server/**server.pem**
- Windows: <LunaClient\_install\_directory>\cert\server\**server.pem**

**3.** Specify the Backup HSM(s) that RBS will make available to clients.**> rbs --config**

RBS displays a list of Backup HSMs currently connected to the workstation. Select the ones you want to provide remote backup services. When you have specified your selection, enter **X** to exit the configuration tool.

**4.** Launch the RBS daemon (Linux/UNIX) or console application (Windows).

- Linux/UNIX: # **rbs --daemon**
- Windows: Double-click the **rbs** application. A console window will remain open.

You are prompted to enter the RBS password.

**5.** Securely transfer the RBS host certificate (**server.pem**) to your Luna HSM Client workstation using **pscp** or **scp**.**6.** On the client workstation, register the RBS host certificate to the server list.

**> vtl addServer -n <Backup\_host\_IP> -c server.pem**

**7.** [Optional] Launch LunaCM on the client to confirm that the Backup HSM appears as an available slot.

**NOTE** If you encounter issues, try changing the RBS and PEDclient ports from their default values. Check that your firewall is not blocking ports used by the service.

You can now use the Backup HSM(s) as though they were connected to the client workstation locally, using Remote PED. See "[Backing Up to a Client-Connected Luna Backup HSM \(G7\)](#)" on page 419 and "[Restoring From a Client-Connected Luna Backup HSM \(G7\)](#)" on page 426 for detailed procedures.

## Updating the Luna Backup HSM (G7) Firmware

To update the Luna Backup HSM (G7) firmware, download the desired firmware version from the Thales Support Portal. If you are updating a Backup HSM connected to a Luna Network HSM appliance, the G7 firmware update file is included in the appliance software update package. See [Updating the Luna Network HSM Appliance Software](#) for the procedure.

Depending on whether the Backup HSM is connected to a Luna Network HSM appliance or a Luna HSM Client workstation, you can use LunaSH or LunaCM to perform the firmware update.

- > "[Updating the Client-Connected Luna Backup HSM \(G7\) Firmware](#)" on the next page
- > "[Updating the Appliance-Connected Luna Backup HSM \(G7\) Firmware](#)" on page 451

## Updating the Client-Connected Luna Backup HSM (G7) Firmware

Use the following procedure to update the Backup HSM firmware using LunaCM. The Backup HSM SO must complete this procedure.

**NOTE** This functionality requires minimum Luna HSM Client 10.3.0. See [Version Dependencies by Feature](#) for more information.

### Prerequisites

- > Luna Backup HSM (G7) firmware update file (<filename>.fuf)
- > firmware update authentication code file (<filename>.txt)
- > If you have backups currently stored on the Backup HSM, they must take up less than 60% of storage capacity, or the firmware upgrade will not proceed.

**NOTE** If you are updating the firmware to version 7.7.x or newer, objects and partitions must be re-sized to include additional object overhead associated with the new V1 partitions - this is included in the process, no additional action from you (see "[What are "pre-firmware 7.7.0", and V0, and V1 partitions?" on page 126](#)"). This conversion can take much longer than previous firmware updates, depending on the number of objects stored on the HSM (a few minutes to several hours). Ensure that you can leave the update operation uninterrupted for this amount of time. Do not interrupt the procedure even if the operation appears to have stalled.

### To update the Luna Backup HSM (G7) firmware using LunaCM

1. Copy the firmware file (<filename>.fuf) and the authentication code file (<filename>.txt) to the Luna HSM Client root directory.
  - Windows: C:\Program Files\SafeNet\LunaClient
  - Linux: /usr/safenet/lunaclient/bin
  - Solaris: /opt/safenet/lunaclient/bin

**NOTE** On some Windows configurations, you might not have authority to copy or unzip files directly into **C:\Program Files\...** If this is the case, put the files in a known location that you can reference in a LunaCM command.

2. Launch LunaCM.
3. If more than one HSM is installed, set the active slot to the Admin partition of the HSM you wish to update.

```
lunacm:> slot set -slot <slot_number>
```

4. [PED-Authenticated] If you are updating a PED-authenticated Backup HSM, connect to the Remote PED server.

```
lunacm:> ped connect [-ip <IP_address>] [-port <port#>]
```

5. Log in as HSM SO.

```
lunacm:> role login -name so
```

6. 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
```

The previous version of the firmware is stored in reserve on the HSM. To restore the previous firmware version, see "[Rolling Back the Luna Backup HSM \(G7\) Firmware](#)" on the next page.

## Updating the Appliance-Connected Luna Backup HSM (G7) Firmware

Use the following procedure to update the Backup HSM firmware using LunaSH. The Backup HSM SO must complete this procedure.

**NOTE** This functionality requires minimum Luna Network HSM appliance software 7.7.0. See [Version Dependencies by Feature](#) for more information.

### Prerequisites

- > The G7 firmware package is included with the Luna Network HSM appliance software package. See [Updating the Luna Network HSM Appliance Software](#) if you have not already updated the appliance software.
- > If you have backups currently stored on the Backup HSM, they must take up less than 60% of storage capacity, or the firmware upgrade will not proceed.

**NOTE** If you are updating the firmware to version 7.7.x or newer, objects and partitions must be re-sized to include additional object overhead associated with the new V1 partitions - this is included in the process, no additional action from you (see "[What are "pre-firmware 7.7.0", and V0, and V1 partitions?"](#)" on page 126). This conversion can take much longer than previous firmware updates, depending on the number of objects stored on the HSM (a few minutes to several hours). Ensure that you can leave the update operation uninterrupted for this amount of time. Do not interrupt the procedure even if the operation appears to have stalled.

### To update the Luna Backup HSM (G7) firmware using LunaSH

1. Using a serial or SSH connection, log in to the appliance as **admin** (see [Logging In to LunaSH](#)).
2. [Optional] List the available Backup HSMs connected to the appliance and note the serial number of the one you wish to update.

```
lunash:> token backup list
```

3. [PED-Authenticated] If you are updating a PED-authenticated Backup HSM, connect to the PED server.

```
lunacm:> hsm ped connect [-ip <IP_address>] [-port <port#>]
```

4. Log in to the Backup HSM as HSM SO.

```
lunash:> token backup login -serial <serialnum>
```

5. Apply the Backup HSM firmware update.

```
lunash:> token backup update firmware -serial <serialnum>
```

## Rolling Back the Luna Backup HSM (G7) Firmware

When you update the Luna Backup HSM (G7) firmware, the previous version of the firmware is stored in reserve on the HSM. If required, you can use the following procedure to roll back the HSM firmware to the previous version. Firmware rollback must be initiated using LunaCM; the Backup HSM must be connected to a Luna HSM Client workstation.

**CAUTION!** Firmware rollback is destructive; earlier firmware versions might have older mechanisms and security vulnerabilities that a new version does not. Ensure that you do not have any important backups stored on the HSM before you proceed. This procedure zeroes the HSM and all backups are erased.

### Prerequisites

- > Connect the Luna Backup HSM (G7) to a Luna HSM Client workstation.

### To roll back the Luna Backup HSM (G7) firmware to the previous version

1. At the LunaCM prompt, set the active slot to the Backup HSM.  
lunacm:> **slot set -slot** <slot\_number>
2. Check the previous firmware version that is available on the HSM.  
lunacm:> **hsm showinfo**
3. [PED-Authenticated] If you are rolling back a PED-authenticated Backup HSM, connect to the Remote PED server.  
lunacm:> **ped connect [-ip <IP\_address>] [-port <port#>]**
4. Log in as HSM SO.  
lunacm:> **role login -name so**
5. Roll back the Backup HSM firmware.  
lunacm:> **hsm rollbackfw**

# CHAPTER 16: Slot Numbering and Behavior

Administrative partitions and application partitions are identified as PKCS#11 cryptographic slots in SafeNet utilities, such as LunaCM and **multitoken**, and for applications that use the Luna library.

## Order of Occurrence for Different Luna HSMs

A host computer with Luna HSM Client software and Luna libraries installed can have Luna HSMs connected in any of three ways:

- > PCIe embedded/inserted Luna PCIe HSM card (one or multiple HSMs installed - administrative partitions and application partitions are shown separately)
- > USB-connected Luna USB HSMs (one or multiple - administrative partitions and application partitions are shown separately)
- > Luna Network HSM application partitions\*, registered and connected via NTLS or STC.

Any connected HSM partitions are shown as numbered slots. Slots are numbered from zero or from one, depending on configuration settings (see "[Settings Affecting Slot Order](#)" on the next page, below), and on the firmware version of the HSM(s).

\* One or multiple application partitions. Administrative partitions on Luna Network HSMs are not visible via LunaCM or other client-side tools. Only registered, connected application partitions are visible. The number of visible partitions (up to 100) depends on your model's capabilities. That is, a remote Luna Network HSM might support 100 application partitions, but your application and LunaCM will only see partitions that have established certificate-exchange NTLS links with the current Client computer.

In LunaCM, a slot list would normally show:

- > Luna Network HSM application partitions for which NTLS links are established with the current host, followed by
- > Luna PCIe HSM cards, followed by
- > Luna USB HSMs

For Luna Network HSM, as seen from a client (via NTLS), only application partitions are visible. The HSM administrative partition of a remote Luna Network HSM is never seen by a Luna HSM Client. The Luna Network HSM slots are listed in the order they are polled, dictated by the entries in the **Luna Network HSM** section of the `Crystoki.ini / chrystoki.conf` file, like this:

```
ServerName00=192.20.17.200
ServerPort00=1792
ServerName01=192.20.17.220
ServerPort01=1793
```

For Luna PCIe HSM and Luna USB HSM, if you have multiple of either HSM type connected on a single host, then the order in which they appear is the hardware slot number, as discovered by the host computer.

For Luna PCIe HSM and Luna USB HSM, the HSM administrative slot always appears immediately after the application partition. If no application partition has yet been created, a space is reserved for it, in the slot numbering.

## Settings Affecting Slot Order

Settings in the **Presentation** section of the configuration file (Chrystoki.conf for UNIX/Linux, crystoki.ini for Windows) can affect the numbering that the API presents to Luna tools (like LunaCM) or to your application.

[Presentation]

ShowUserSlots=<slot>( <serialnumber>)

- > Sets starting slot for the identified partition.
- > Default, when ShowUserSlots is not specified, is that all available partitions are visible and appear in default order.
- > Can be applied, individually, to multiple partitions, by a single entry containing a comma-separated list (with partition serial numbers in brackets):  
ShowUserSlots=1(351970018022), 2(351970018021), 3(351970018020),....
- > If multiple partitions on the same HSM are connected to the Luna HSM Client host computer, redirecting one of those partitions with ShowUserSlots= causes all the others to disappear from the slot list, unless they are also explicitly re-ordered by the same configuration setting.

ShowAdminTokens=yes

- > Default is yes. Admin partitions of local HSMs are visible in a slot listing.
- > Remotely connected partitions (Luna Network HSM) are not affected by this setting, because NTLS connects only application partitions, not HSM SO (Admin) partitions to clients, so a Luna Network HSM SO administrative partition would never be visible in a client-side slot list, regardless.

ShowEmptySlots=1

- > Controls how C\_GetSlotList - as used by lunacm slot list command, or ckdemo command 14, and by your PKCS#11 application - displays, or does not display unused potential slots, when the number of partitions on an HSM is not at the limit.

OneBaseSlotId=1

- > Causes basic slot list to start at slot number 1 (one) instead of default 0 (zero).  
(Any submitted number other than zero is treated as "1". Any letter or other non-numeric character is treated as "0".)

### Effects of Settings on Slot List

Say, for example, you have multiple HSMs connected to your host computer (or installed inside), with any combination of firmware 6.22.0 (and newer) or pre-6.22.0 firmware, and no explicit entries exist for slot order in the config file. The defaults prevail and the slot list would start at zero.

If you set OneBaseSlotId=1 in the configuration file, then the slot list starts at "1" instead of at "0". You could set this for personal preference, or according to how your application might expect slot numbering to occur (or if you have existing scripted solutions that depend on slot numbering starting at zero or starting at one).

OneBaseSlotId affects the starting number for all slots, regardless of firmware.

If you set ShowUserSlots=20(17923506), then the identified token or HSM or application partition would appear at slot 20, regardless of the locations of other HSMs and partitions.

## Effects of New Firmware on Slot Login State

Slots retain login state when current-slot focus changes. You can use the LunaCM command **slot set** to shift focus among slots, and whatever login state existed when you were previously focused on a slot is still in effect when you return to that slot.