

SafeNet Luna Network HSM Client 10.1

ADMINISTRATION GUIDE



Document Information

Product Version	10.1
Document Part Number	007-000553-001
Release Date	23 January 2020

Revision History

Revision	Date	Reason
Rev. A	23 January 2020	Initial release

Trademarks, Copyrights, and Third-Party Software

Copyright 2001-2020 Thales. 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 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'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 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 reserves the right to make any change or improvement in the specifications data, information, and the like described herein, at any time.

Thales 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 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 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 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 disclaims any liability with respect to security for direct, indirect, incidental or consequential damages that result from any use of its products. It is further stressed that independent testing and verification by the person using the product is particularly encouraged, especially in any application in which defective, incorrect or insecure functioning could result in damage to persons or property, denial of service, or loss of privacy.

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

Regulatory Compliance

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

USA, FCC

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

Canada

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

Europe

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

CONTENTS

Preface: About the Administration Guide	13
Customer Release Notes	14
Audience	14
Document Conventions	14
Support Contacts	16
Chapter 1: Application Partitions	17
Creating or Deleting an Application Partition	17
Customizing Partition Sizes	18
Re-sizing an Existing Partition	19
Initializing an Application Partition	21
Activation and Auto-activation on Multi-factor- (PED-) Authenticated Partitions	23
Enabling Activation on a Partition	23
Activating a Role	24
Partition Utilization Metrics	26
Rules of acquisition	26
Availability of Partition Utilization Metrics	27
Chapter 2: Audit Logging	29
Audit Logging Overview	29
Audit limitations and Controlled tamper recovery state	31
The Audit Role	32
Audit Log Records	34
Audit Log Message Format	35
Configuring and Using Audit Logging	38
Configuring Audit Logging	38
Copying Log Files Off the Appliance	41
Exporting the Audit Logging Secret and Importing to a Verifying HSM	41
Reading the Audit Log Records	42
Audit Role Authentication Considerations	43
Audit Logging General Advice and Recommendations	43
Audit Log Categories and HSM Events	45
Remote Audit Logging	51
Audit log troubleshooting	52
Chapter 3: Backup and Restore Using a G5-Based Backup HSM	53
Backup and Restore Best Practices	53
Planning Your Backup HSM Deployment	54
Partition to Partition	54
Backup HSM Connected to the Appliance	55
Backup HSM Connected to the Client Workstation	55

Backup HSM Installed Using Remote Backup Service (RBS)	56
About the SafeNet Luna G5 Backup HSM	57
Physical Features	58
Backup HSM Functionality	58
Storage and Maintenance	59
Installing the Backup HSM	60
Installing or Replacing the Backup HSM Battery	60
Backup HSM Secure Transport and Tamper Recovery	63
Creating a Secure Recovery Key	64
Setting Secure Transport Mode	65
Recovering From a Tamper Event or Secure Transport Mode	65
Disabling Secure Recovery	66
Initializing the Backup HSM Remote PED Vector	66
Resetting the Backup HSM to Factory Conditions	68
Backup/Restore Using an Appliance-Connected Backup HSM	68
Initializing the Backup HSM	69
Backing Up an Application Partition	69
Restoring an Application Partition from Backup	70
Backup/Restore Using a Client-Connected Backup HSM	71
Initializing the Backup HSM	71
Backing Up an Application Partition	72
Restoring an Application Partition from Backup	73
Configuring a Remote Backup HSM Server	74
Installing/Configuring the Remote Backup Service	74
Chapter 4: Backup and Restore Using a G7-Based Backup HSM	76
Overview and Key Concepts	76
Overview	76
Credentials Required to Perform Backup and Restore Operations	77
Client Software Required to Perform Backup and Restore Operations From a Client Workstation	78
PED Authentication with the G7-Based Backup HSM	78
Backup and Restore Best Practices	78
Initializing a Client-Connected G7-Based Backup HSM	79
Initializing a PED-Authenticated HSM	79
Initializing a Password-Authenticated HSM	82
Backing Up to a Client-Connected G7-Based Backup HSM	83
Backing Up a Multi-factor- (PED-) Authenticated Partition	83
Backing Up a Password-Authenticated Partition	87
Restoring From a Client-Connected G7-Based Backup HSM	89
Restoring a Multi-factor- (PED-) Authenticated Partition	89
Restoring a Password-Authenticated Partition	91
Backup and Restore to a Remote Backup Service (RBS)-Connected G7-Based Backup HSM	93
Installing and Configuring the Remote Backup Service	93
Chapter 5: Capabilities and Policies	95
HSM Capabilities and Policies	95
Setting HSM Policies Manually	103

Setting HSM Policies Using a Template	104
Creating an HSM Policy Template	105
Editing an HSM Policy Template	105
Applying an HSM Policy Template	106
Partition Capabilities and Policies	106
Setting Partition Policies Manually	113
Setting Partition Policies Using a Template	114
Creating a Partition Policy Template	115
Editing a Partition Policy Template	115
Applying a Partition Policy Template	117
Chapter 6: Configuring the Partition for Cloning or Export of Private Keys	118
Cloning Mode	118
Key Export Mode	119
No Backup Mode	120
Chapter 7: Client-Partition Connections	122
Comparing NTLS and STC	122
Creating an NTLS Connection Using Self-Signed Certificates	127
Multi-Step NTLS Connection Procedure	127
One-Step NTLS Connection Procedure	130
Creating an NTLS Connection Using a Client Certificate Signed by a Trusted Certificate Authority	131
Registering the Appliance Certificate on the Client	131
Authenticating a Client Using a 3rd-Party CA	132
Registering the Client Certificate and CA Certificate Chain on the Appliance	133
Assigning or Revoking NTLS Client Access to a Partition	134
Creating a Client-Partition STC Connection	135
Preparing the HSM/Partition to Use STC	136
Connecting an Initialized STC Partition to Multiple Clients	139
Converting Initialized NTLS Partitions to STC	143
Using the STC Admin Channel	145
Configuring STC Identities and Settings	146
Restoring Broken NTLS or STC Connections	150
Restoring NTLS/STC Connections after Regenerating the HSM Server Certificate	150
Restoring Connections After HSM Zeroization	151
Restoring STC Connections After Partition Zeroization	151
Chapter 8: Configuration File Summary	153
Chapter 9: Decommissioning, Zeroizing, Re-imaging, or Resetting an HSM to Factory Conditions	165
Zeroization	165
Decommissioning the HSM Appliance	166
Disabling Decommissioning	167
Resetting to Factory Condition	167
Re-Imaging the Appliance to Factory Baseline	168
Comparing Zeroize, Decommission, Re-image, and Factory Reset	171

End of Service and Disposal	172
Comparison of Destruction/Denial Actions	174
Effects of Administrative Actions on Functionality Modules	176
RMA and Shipping Back to Thales Group	176
Chapter 10: Functionality Modules	177
FM Deployment Constraints	177
FMs and High-Availability (HA)	178
FMs and Backup/Restore/Cloning	178
FMs and Secure Trusted Channel (STC)	179
FMs and Appliance Re-imaging	179
FMs and HSM Firmware Rollback	179
FM Configuration and Remote PED	179
FM-Enabled HSM Cannot be Verified With CMU	180
Key Attributes	180
No EDDSA or EC_MONTGOMERY Private Keys with C_CreateObject	180
FM Sample Applications Dependent on General Cryptoki Samples	180
Space for FMs	180
Preparing the SafeNet Luna Network HSM to Use FMs	180
Step 1: Ensure You Have FM-Ready Hardware	181
Step 2: Update to Luna Appliance Software and HSM Firmware 7.4.0 or Higher	181
Step 3: Purchase and Apply the FM Capability License	181
Step 4: Apply HSM Policy Settings	182
Building and Signing an FM	183
Loading an FM Into the HSM Firmware	186
Deleting an FM From the HSM Firmware	187
Recovering the HSM After FM Failure	188
Chapter 11: High-Availability Groups	190
Application Object Handles	197
Example: Database Encryption	198
Planning Your HA Group Deployment	199
HSM and Partition Prerequisites	199
Sample Configurations	200
Setting Up an HA Group	203
Verifying an HA Group	207
Setting an HA Group Member to Standby	209
Configuring HA Auto-Recovery	211
Enabling/Disabling HA Only Mode	211
HA Logging	212
Configuring HA Logging	212
HA Log Messages	213
Adding/Removing an HA Group Member	216
Manually Recovering a Failed HA Group Member	219
Replacing an HA Group Member	220
Deleting an HA Group	222
HA Troubleshooting	223

Administration Tasks on HA Groups	223
Unique Object IDs (OID)	223
Client-Side Failures	223
Failures Between the HSM Appliance and Client	223
Effect of PED Operations	223
Chapter 12: HSM Initialization	224
Initializing a New or Factory-reset HSM	225
Re-initializing an Existing, Non-factory-reset HSM	227
PED-authenticated HSM Initialization Example	228
Password-authenticated HSM Initialization Example	234
Chapter 13: HSM Status Values	235
Chapter 14: Key Cloning	237
Key Cloning Overview and Key Concepts	237
Cloning Objects to Another Application Partition	237
Cloning Keys Between Luna 6, Luna 7, and HSM on Demand	238
Chapter 15: PED Authentication	242
PED Authentication Architecture	242
Comparing Password and PED Authentication	243
PED Keys	244
PED Key Types and Roles	244
Shared PED Key Secrets	246
M of N Split Secrets (Quorum)	247
SafeNet Luna PED Hardware Functions	248
Physical Features	248
Keypad Functions	249
Modes of Operation	250
Local PED Setup	251
About Remote PED	252
Remote PED Architecture	253
PEDserver-PEDclient Communications	256
Remote PED Setup	257
Initializing the Remote PED Vector (RPV) and Creating an Orange Remote PED Key (RPK)	258
Installing PEDserver and Setting Up the Remote Luna PED	261
Opening a Remote PED Connection	262
Ending or Switching the Remote PED Connection	271
Remote PED Troubleshooting	272
PED Key Management	276
Creating PED Keys	276
Performing PED Authentication	281
Consequences of Losing PED Keys	283
Identifying a PED Key Secret	285
Duplicating Existing PED Keys	286
Changing a PED Key Secret	287

PEDserver and PEDclient	289
The PEDserver Utility	290
The PEDclient Utility	290
pedclient	290
pedclient mode assignid	292
pedclient mode config	293
pedclient mode deleteid	295
pedclient mode releaseid	296
pedclient mode setid	297
pedclient mode show	298
pedclient mode start	299
pedclient mode stop	301
pedclient mode testid	302
pedserver	303
pedserver appliance	304
pedserver appliance delete	305
pedserver appliance list	306
pedserver appliance register	307
pedserver mode	308
pedserver mode config	309
pedserver mode connect	311
pedserver mode disconnect	312
pedserver mode show	313
pedserver mode start	315
pedserver mode stop	317
pedserver regen	319
Chapter 16: Performance Monitoring	320
Chapter 17: Security in Operation	321
Client to HSM Security Best Practices	321
Security around Password-authenticated systems	321
Security Effects of Administrative Actions	322
Security of Your Partition Challenge	326
Chapter 18: Secure Transport Mode	328
Placing an HSM Into Secure Transport Mode	330
Recovering an HSM From Secure Transport Mode	330
Chapter 19: Slot Numbering and Behavior	332
Order of Occurrence for Different SafeNet Luna HSMs	332
Settings Affecting Slot Order	333
Effects of Settings on Slot List	333
Effects of New Firmware on Slot Login State	334
Chapter 20: SNMP Monitoring	335
Overview and Installation	335

MIB	335
SafeNet SNMP Subagent	336
The SafeNet Chrysalis-UTSP MIB	337
The SafeNet Luna HSM MIB	338
hsmPolicyTable	341
hsmPartitionPolicyTable	341
hsmClientRegistrationTable	342
hsmClientPartitionAssignmentTable	342
SNMP output compared to SafeNet tools output	343
The SafeNet Appliance MIB	344
SNMP Operation and Limitations with SafeNet Luna Network HSM	344
SNMP-Related Commands	344
Coverage	345
HSM MIB	345
MIBS You Need for Network Monitoring of SafeNet Luna Network HSM	346
MIBS You Need for Monitoring the Status of the HSM	346
Frequently Asked Questions	346
Chapter 21: Tamper Events	348
Recovering from a Tamper Event	349
Chapter 22: Troubleshooting	351
General Troubleshooting Tips	351
System Operational and Error Messages	352
Extra slots that say "token not present"?	352
Error: 'hsm update firmware' failed. (10A0B : LUNA_RET_OPERATION_RESTRICTED) when attempting to perform hsm update firmware	352
KR_ECC_POINT_INVALID Error when decrypting a file encrypted from BSAFE through ECIES using ECC key with any of the curves from the x9_t2 section	352
Error during SSL Connect (RC_OPERATION_TIMED_OUT) logged to /var/log/messages by the SafeNet Luna HSM Client	352
Slow/interrupted response from the HSM, and the "hsm show" command shows LUNA_RET_SM_SESSION_REALLOC_ERROR	353
Low Battery Message	353
Keycard and Token Return Codes	353
Library Codes	371
Vendor-Defined Return Codes	376
HSM Alarm-codes overview	381
Alarm Generation and Handling	382
FRAM LOG	383
HSM Alarm Codes	383
HSM Alarm-codes samples	388
Temperature - High Warning	388
Temperature – High Soft Tamper	388
Temperature – High Hard Tamper	389
Hard Tamperers During Storage	390
Decommission with power on	390

Chapter 23: Updates and Upgrades	393
Update Considerations	393
Version Dependencies by Feature	393
Updating the SafeNet Luna HSM Client	396
Updating the SafeNet Luna Network HSM Appliance Software	397
Updating the SafeNet Luna HSM Firmware	398
Updating the SafeNet Luna Backup HSM Firmware	399
Rolling Back the SafeNet Luna HSM Firmware	400
Upgrading HSM Capabilities and Partition Licenses	401
Upgrade Options	402
Purchasing an Upgrade License	403
Activating a License on the Thales Group Licensing Portal	405
Managing Your Thales Group Licensing Portal Account	409
Applying an Upgrade License on the HSM	413
Upgrade Troubleshooting	415
Chapter 24: Users and Roles	416
Appliance Users and Roles	418
Logging In to LunaSH	421
Failed Appliance Login Attempts	422
Enabling/Disabling Appliance User Accounts	422
Changing Appliance User Passwords	423
Creating Custom Appliance User Accounts	423
Creating Custom Appliance Roles	424
Creating a One-Step NTLS Registration Role	425
Backing Up/Restoring the Appliance User Role Configuration	427
Recovering the Admin Account Password	428
HSM Roles	430
HSM Security Officer (SO)	430
Auditor (AU)	430
Logging In as HSM Security Officer	431
Changing the HSM SO Credential	431
Logging In as Auditor	432
Changing the Auditor Credential	432
Partition Roles	433
Initializing the Crypto Officer and Crypto User Roles	434
Logging In to the Application Partition	435
Changing a Partition Role Credential	437
Resetting the Crypto Officer or Crypto User Credential	437
Name, Label, and Password Requirements	438
Custom Appliance User Accounts	438
Custom Appliance Roles	439
Appliance User Passwords	439
HSM Labels	439
Cloning Domains	439
Partition Names	439
Partition Labels	440

HSM/Partition Role Passwords or Challenge Secrets440

PREFACE: About the Administration Guide

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

- > ["Application Partitions" on page 17](#)
- > ["Audit Logging" on page 29](#)
- > ["Backup and Restore Using a G5-Based Backup HSM" on page 53](#)
- > ["Backup and Restore Using a G7-Based Backup HSM" on page 76](#)
- > ["Capabilities and Policies" on page 95](#)
- > ["Client-Partition Connections" on page 122](#)
- > ["Configuration File Summary" on page 153](#)
- > ["Decommissioning, Zeroizing, Re-imaging, or Resetting an HSM to Factory Conditions" on page 165](#)
- > ["High-Availability Groups" on page 190](#)
- > ["HSM Initialization" on page 224](#)
- > ["HSM Status Values" on page 235](#)
- > ["PED Authentication" on page 242](#)
- > ["Performance Monitoring" on page 320](#)
- > ["Security Effects of Administrative Actions" on page 322](#)
- > ["Secure Transport Mode" on page 328](#)
- > ["Slot Numbering and Behavior" on page 332](#)
- > ["SNMP Monitoring" on page 335](#)
- > ["Tamper Events" on page 348](#)
- > ["Troubleshooting" on page 351](#)
- > ["Updates and Upgrades" on page 393](#)
- > ["Users and Roles" on page 416](#)

The preface includes the following information about this document:

- > ["Customer Release Notes" on the next page](#)
- > ["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.gemalto.com>.

Audience

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

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

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

Document Conventions

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

Notes

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

NOTE Take note. Contains important or helpful information.

Cautions

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

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

Warnings

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

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

Command syntax and typeface conventions

Format	Convention
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 to this service is governed by the support plan arrangements made between Thales and your organization. Please consult this support plan for further information about your entitlements, including the hours when telephone support is available to you.

Customer Support Portal

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

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

Telephone

The support portal also lists telephone numbers for voice contact. ([KB0013367](#))

Email Support

You can also contact technical support by email at technical.support@gemalto.com.

CHAPTER 1: Application Partitions

The SafeNet Luna Network HSM has two types of partition:

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

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

Depending on your SafeNet Luna Network HSM model and the number of additional partition licenses you have purchased, you can create anywhere from 5 to 100 application partitions on the HSM. Each partition can store cryptographic objects according to the amount of memory you assign. The HSM SO can customize the size of individual partitions until all the memory on the HSM is allotted. To purchase additional partition licenses, see ["Upgrading HSM Capabilities and Partition Licenses" on page 401](#).

This chapter contains the following procedures for managing application partitions:

- > ["Creating or Deleting an Application Partition" below](#)
- > ["Customizing Partition Sizes" on the next page](#)
- > ["Initializing an Application Partition" on page 21](#)
- > ["Activation and Auto-activation on Multi-factor- \(PED-\) Authenticated Partitions" on page 23](#)
- > ["Partition Utilization Metrics" on page 26](#)

Creating or Deleting an Application Partition

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

Prerequisites

- > The HSM must be initialized (see ["HSM Initialization" on page 224](#)).
- > You require the HSM SO credential (blue PED key).

To create an application partition

1. Connect to the appliance via SSH or a serial connection, and log in to LunaSH as **admin** or **operator**, or a custom user with an **admin** or **operator** role (see ["Logging In to LunaSH" on page 421](#)).
2. Log in as HSM SO (see ["Logging In as HSM Security Officer" on page 431](#)).
3. Create the application partition, specifying a partition name. This name is distinct from the partition label assigned during initialization and can be changed later. You can also specify the desired partition size in bytes (see also ["Customizing Partition Sizes" below](#)).

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

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

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

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

No two partitions can have the same name.

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

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

```
lunash:> partition list
```

To delete an application partition

1. Connect to the appliance via SSH or a serial connection, and log in to LunaSH as **admin** or **operator**, or a custom user with an **admin** or **operator** role (see ["Logging In to LunaSH" on page 421](#)).
2. Log in as HSM SO (see ["Logging In as HSM Security Officer" on page 431](#)).
3. Delete the application partition by specifying its name.

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

Customizing Partition Sizes

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

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

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

- > ["Creating a Custom-Sized Partition" on the next page](#)
- > ["Re-sizing an Existing Partition" on the next page](#)
- > ["Creating Multiple Equal Large Partitions" on page 20](#)

Prerequisites

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

- > Total HSM storage
- > Current memory usage
- > Current number of partitions
- > Maximum number of partitions allowed

Use lunash:> **partition list** to see:

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

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

Creating a Custom-Sized Partition

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

To create a custom-sized partition

1. Connect to the appliance via SSH or a serial connection, and log in to LunaSH as **admin** or **operator**, or a custom user with an **admin** or **operator** role (see "Logging In to LunaSH" on page 421).
2. Log in to the HSM as HSM SO (see "Logging In as HSM Security Officer" on page 431).
3. Create the application partition, specifying the desired size in bytes. To use all remaining space on the HSM, specify **-allfreestorage** instead of **-size**.

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

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

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

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

No two partitions can have the same name.

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

Re-sizing an Existing Partition

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

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

To re-size an existing partition

1. Connect to the appliance via SSH or a serial connection, and log in to LunaSH as **admin** or **operator**, or a custom user with an **admin** or **operator** role (see "Logging In to LunaSH" on page 421).
2. Log in to the HSM as HSM SO (see "Logging In as HSM Security Officer" on page 431).
3. Re-size the desired partition by specifying the partition name and the desired size in bytes. To use all remaining space on the HSM, specify **-allfreestorage** instead of **-size**.

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

Creating Multiple Equal Large Partitions

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

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

1. Start by creating 20 partitions (the maximum allowed) – each will have X bytes available to it.
2. Delete 4 of them (leaving 16).
3. Re-size one partition to use **-allfreestorage**, which makes that partition as large as five small partitions – the four partitions you just deleted, freeing their allotment, plus the one you are currently resizing – and leaves the HSM with 15 partitions having X bytes each, plus the large one.
4. Delete another four small partitions.
5. Re-size one small partition to use **-allfreestorage**, which makes that partition large (there are now two equally-sized large partitions) and leaves the HSM with 10 partitions having X bytes each, plus the two large ones.
6. Delete another four small partitions.
7. Re-size one small partition to use **-allfreestorage**, which makes that partition large (there are now three equally-sized large partitions) and leaves the HSM with 5 partitions having X bytes each, plus the three large ones.
8. Delete another four small partitions.
9. Re-size the single remaining small partition to use **-allfreestorage**, which makes that partition large and leaves 0 (zero) of the original partitions with X bytes each, and the four large partitions of equal size, with no unallocated space on the HSM.

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

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 the next page](#)).

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 is performed using LunaCM.

Prerequisites

- > The new partition must be assigned to the client and visible in LunaCM (see ["Client-Partition Connections" on page 122](#)).
- > If you want to configure the partition's policies with a policy template, the template file must be available on the client (see ["Setting Partition Policies Using a Template" on page 114](#)).
- > PED authentication: A local or remote PED connection must be established (see ["Local PED Setup" on page 251](#) or ["Remote PED Setup" on page 257](#)). Ensure that you have enough blue (Partition SO) and red (Domain) PED keys for your planned authentication scheme (see ["Creating PED Keys" on page 276](#)).

To initialize a new application partition

1. Launch LunaCM on the client workstation.
2. Set the active slot to the partition you want to initialize.

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

3. 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 challenge secrets must be 7-255 characters in length. The following characters are allowed:

```
abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789 !@#$%^&*()_-+[]
```

```
{ } \ | / ; : ' , . < > ? ` ~
```

Double quotation marks (") are problematic and should not be used in passwords.

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

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 276](#)).

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 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 251](#) or ["Remote PED Setup" on page 257](#)).

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>
```

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, 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 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" on page 348](#) and ["Partition Capabilities and Policies" on page 106](#) for more information.

This section contains instructions for the following procedures:

- > ["Enabling Activation on a Partition" below](#)
- > ["Activating a Role" on the next page](#)
- > ["Enabling Auto-activation" on page 25](#)
- > ["Deactivating a Role" on page 25](#)

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 both the 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 21](#)).

To enable activation on a partition

1. Log in to the partition as Partition SO (see ["Logging In to the Application Partition" on page 435](#)).
`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 and/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 Crypto User. The role will become 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" on the previous page](#)).
- > The role you wish to activate must be initialized on the partition (see ["Initializing the Crypto Officer and Crypto User Roles" on page 434](#)).

To activate a role

1. Log in to the partition using the appropriate role (see ["Logging In to the Application Partition" on page 435](#)):
 - If you are activating the Crypto Officer role, log in as Partition SO.
 - If you are activating the Crypto User role, log in as Crypto Officer.

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

2. 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 106](#)).

In LunaCM, passwords and challenge secrets must be 7-255 characters in length. The following characters are allowed:

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

Double quotation marks (") are problematic and should not be used in passwords.

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

```
lunacm:> role 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 will be prompted for the PED key, regardless of the policy setting.

3. Log out of the partition.

```
lunacm:> role logout
```

4. Provide the initial challenge secret to the designated CO or CU by secure means. The PED secret will be 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 437](#).

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 23](#)).

To enable auto-activation on a partition

1. Log in to the partition as Partition SO (see ["Logging In to the Application Partition" on page 435](#)).
lunacm:> **role login -name po**
2. Enable partition policy 23.
lunacm:> **partition changepolicy -policy 23 -value 1**
Auto-activation will take effect for each affected role (CO and/or CU) the next time the role is authenticated.
3. [Optional] For optimal reliability, the SafeNet 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 ["Logging In to the Application Partition" on page 435](#)).
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**

Partition Utilization Metrics

In order to ensure the quality of service (QoS) that you provide to applications that make use of HSM partitions, it is first necessary to know how the users and applications are making use of the HSM resources - that is, the distribution of demand.

For an HSM with a single application partition, it can be helpful to know what type of load is being imposed on the HSM and the enumeration and categorization of operations that are being performed. Application developers might have a good idea of the expected ratio of operations, but the operations team managing the application servers would like to know the real-world utilization, for their planning and management purposes.

For a Network HSM with multiple partitions that are sharing the space and the processing resources of the HSM, it is useful to know which partitions are presenting the greatest load, and the kinds of operations that are most common or frequent. That knowledge aids in resource planning and possible relocation or reallocation of partitions to ensure reliable service for all users.

NOTE Utilization metrics are based on *utilization counters* that track operations by category. This is not to be confused with *usage counters*, that track and limit the number of times a key or certificate is allowed to be used.

This feature has software and/or firmware dependencies. See "[Version Dependencies by Feature](#)" on page 393 for more information.

Rules of acquisition

Utilization Metrics count these operations within category "bins" per partition:

- > Sign
- > Verify
- > Encrypt
- > Decrypt
- > Key generate
- > Key derive

Operations not in that list do not increment any counter. That is, an operation request to the HSM increments counters in 0 or more bins. The list might expand in future releases. Each bin has a single counter that counts how many requests have been received from the host, since the last counter-reset order or power cycle. Counters for a partition can be read and reset as a single operation, or as two separate operations.

The utilization counters count *requests* to the HSM, because, while successful requests are expected and are counted, unsuccessful requests also consume resources and therefore need to be counted as well. Any request that fails on the host - meaning it does not reach the HSM - is not counted, because it did not use any HSM resources.

Utilization counters are volatile, and therefore are lost in the event of a power failure. If they are valued, they should be polled regularly and the results kept in non-volatile storage on the host.

Availability of Partition Utilization Metrics

Utilization metrics are supported by firmware 7.3 (and newer) which implements HSM-level policy **49: Allow Partition Utilization Metrics**. That policy is off (value 0) by default, as it is not required in all use-cases, and is most useful where multiple applications use the HSM.

NOTE The Utilization Metrics feature allows the HSM SO to know which operations are being performed on the HSM. This information is normally available only to the Auditor when audit logging is turned on. However, while the SO can see a record of cryptographic operations, there is no visibility as to which keys are being used.

Setting the policy on (value 1) enables utilization metrics for all partitions including the Admin partition. Changing the policy is not destructive in either direction (off-to-on or on-to-off).

The **hsm qos metrics show** command allows you to view the current utilization counter values for all partitions, and overall counts for the entire HSM, or to export the current counts to a file, without resetting the counters.

The **hsm qos metrics reset** command allows you to reset to zero the current utilization counter values for all partitions; additionally, you have the option to view the current counts or to export the current counts to a file, without losing any counts between the view/export action and the reset action.

To access the Partition Utilization Metrics feature

1. Ensure that your HSM is at firmware version 7.3 or newer (if needed, upgrade to a suitable version; see ["Updating the SafeNet Luna HSM Firmware" on page 398](#)).
2. Set HSM policy 49 (Allow Partition Utilization Metrics) to "On".

```
lunash:>hsm changepolicy -policy 49 -value 1

'hsm changePolicy' successful.

Policy Allow Partition Utilization Metrics is now set to value: 1

Command Result : 0 (Success)
```

To view or save Partition Utilization Metrics without resetting

Run the **hsm qos metrics show** command.

```
lunash:>hsm qos metrics show
```

To reset the Partition Utilization Metrics counters to zero

Metrics are reset whenever power is lost to the HSM or the HSM is reset, or the HSM is initialized. These events do not save the metrics.

To reset the metrics without exporting:

Run the **hsm qos metrics reset** command without option.

```
lunash:>hsm qos metrics reset
```

To reset the Partition Utilization Metrics counters to zero while also viewing or exporting the information

Run the **hsm qos metrics reset -export** command (which saves the current counter values to a named file before they are zeroed).

```
lunash:>hsm qos metrics reset -export somefilename
```

Or run the **hsm qos metrics reset -display** command (which shows, but does not save the counter data).

```
lunash:>hsm qos metrics reset -display
```

CHAPTER 2: Audit Logging

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

- > ["Audit Logging Overview" below](#)
- > ["Configuring and Using Audit Logging" on page 38](#)
- > ["Audit Logging General Advice and Recommendations" on page 43](#)
- > ["Audit Log Categories and HSM Events" on page 45](#)
- > ["Remote Audit Logging" on page 51](#)
- > ["Audit log troubleshooting" on page 52](#)

Audit Logging Overview

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

Types of events included in the logs

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

- > log access attempts (logins)
- > log HSM management (init/reset/etc)
- > key management events (key create/delete)
- > asymmetric key usage (sig/ver)
- > first asymmetric key usage only (sig/ver)
- > symmetric key usage (enc/dec)
- > first symmetric key usage only (enc/dec)
- > log messages from CA_LogExternal
- > log events relating to log configuration

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

Event log storage

When the HSM logs an event, the log is stored on the HSM. The audit user cannot view these log entries. Before a log can be viewed, it must be rotated. Log rotation saves the log entries on the HSM to the HSM

appliance, where they can be viewed. Log records are HMACed using an audit log secret to ensure their authenticity. The audit log secret is unique to the HSM where the log was created, and is required to view the HSM event logs. The secret can be exported, allowing you to view and verify the logs on another HSM.

Event logging impacts HSM performance

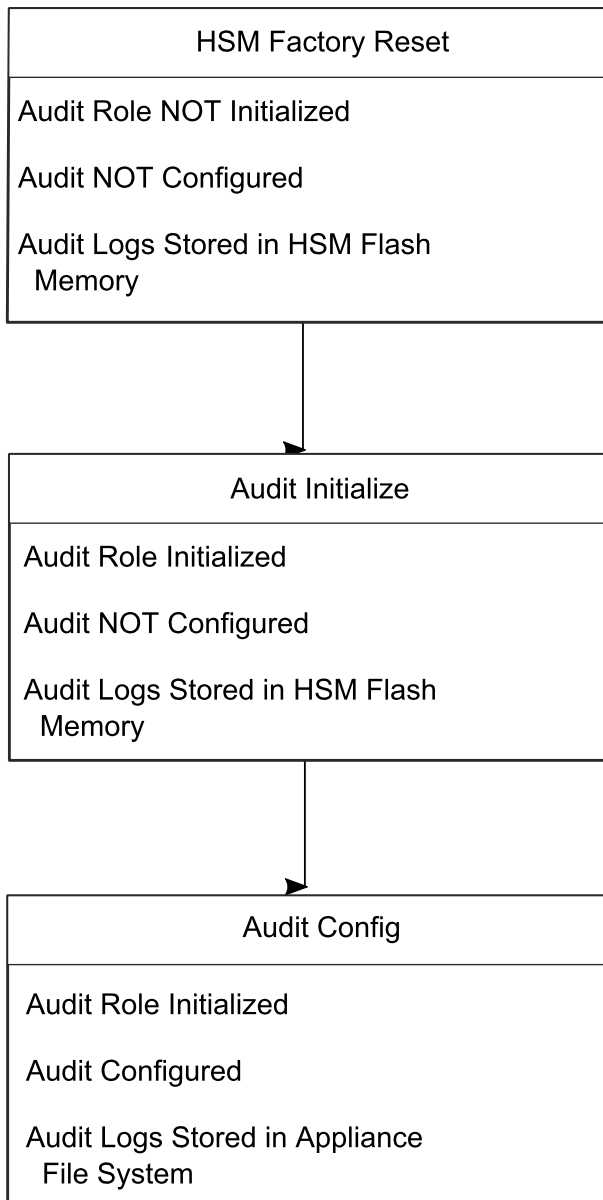
Each audit log record generated requires HSM resources. Configuring event logging to record most, or all, events may have an impact on HSM performance. You may need to adjust your logging configuration to provide adequate logging without significantly affecting performance. By default, only critical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

Audit Logging Features

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

- > Log entries originate from the SafeNet Luna Network HSM - the feature is implemented via HSM firmware (rather than in the library) for maximum security.
- > Log origin is assured.
- > Logs and individual records can be validated by any SafeNet Luna Network HSM that is a member of the same domain.
- > Audit Logging can be performed on password-authenticated (FIPS 140-2 level 2) and PED-authenticated (FIPS 140-2 level 3) configurations, but these configurations may not validate each other's logs - see the "same domain" requirement, above.
- > Each entry includes the following:
 - When the event occurred
 - Who initiated the event (the authenticated entity)
 - What the event was
 - The result of the logging event (success, error, etc.)
- > Multiple categories of audit logging are supported, configured by the audit role.
- > Audit management is a separate role - the role creation does not require the presence or co-operation of the SafeNet Luna Network HSM SO.
- > The category of audit logging is configurable by (and only by) the audit role.
- > Audit log integrity is ensured against the following:
 - Truncation - erasing part of a log record
 - Modification - modifying a log record
 - Deletion - erasing of the entire log record
 - Addition - writing of a fake log record
- > Log origin is assured.
- > The following critical events are logged unconditionally, regardless of the state of the audit role (initialized or not):
 - Tamper
 - Decommission

- Zeroization
- SO creation
- Audit role creation

**Note:**

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

Note:

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

Audit limitations and Controlled tamper recovery state

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

- > Auditor (the Audit role) cannot verify the integrity of audit logs until after recovery from tamper.

- > Auditor cannot be initialized when the HSM is in controlled tamper recovery state.
- > Existing Audit role can login when in controlled tamper recovery state.
- > Existing Audit role cannot make audit config changes when in controlled tamper recovery state.
- > Existing Audit role cannot export the audit secret when in controlled tamper recovery state.

The Audit Role

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

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

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

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

To simplify configuration,

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

Audit User on the Appliance

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

Audit Role on the HSM

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

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

Password-authenticated HSMs

For SafeNet Luna Network HSMs with Password Authentication, the auditor role logs into the HSM to perform their activities using a password. After initializing the Audit role on a password-authenticated HSM, log in as the Auditor and set the domain (see ["role setdomain" on page 1](#) for the command syntax). This step is required before setting logging parameters or the log filepath, or importing/exporting audit logs.

PED-authenticated HSMs

For SafeNet Luna Network HSMs with PED Authentication, the auditor role logs into the HSM to perform their activities using the Audit (white) PED key.

Role Initialization

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

Appliance Audit User Available Commands

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

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

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

```
lunash:>help
```

The following top-level commands are available:

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

Audit Log Secret

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

Log Secret and Log Verification

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

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

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

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

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

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

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

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

Audit Log Records

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

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

MSG 1	HMAC 0
	...
MSG n-1	HMAC n-2
MSG n	HMAC n-1
...	
MSG n+m	HMAC n+m-1

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

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

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

Audit Log Message Format

Each message is a fixed-length, comma delimited, and newline-terminated string. The table below shows the width and meaning of the fields in a message.

Offset	Length (Chars)	Description
0	10	Sequence number
10	1	Comma
11	17	Timestamp
28	1	Comma
29	256	Message text, interpreted from raw data
285	1	Comma
286	64	HMAC of previous record as ASCII-HEX
350	1	Comma
351	96	Data for this record as ASCII-HEX (raw data)
447	1	Newline '\n'

Log Capacity

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

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

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

LOG FULL condition

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

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

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

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

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

Configuration Persists Unless Factory Reset is Performed

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

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

Audit Logging Stops Working if the Current Log File is Deleted

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

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

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

Example

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

Configuring and Using Audit Logging

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

- > ["Configuring Audit Logging" below](#)
- > ["Copying Log Files Off the Appliance" on page 41](#)
- > ["Exporting the Audit Logging Secret and Importing to a Verifying HSM" on page 41](#)
- > ["Reading the Audit Log Records" on page 42](#)
- > ["Audit Role Authentication Considerations" on page 43](#)

Configuring Audit Logging

Configure audit logging using the LunaSH **audit** commands. See ["audit" on page 1](#) in the *LunaSH Command Reference Guide*.

Prerequisites (HSM SO):

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

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

To configure audit logging (Auditor):

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

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

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

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

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

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

```
lunash:> audit init
```

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

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

```
lunash:> audit login
```

- On password-authenticated HSMs, you are prompted to enter the password for the audit role.

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

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

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

```
lunash:> audit sync
```

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

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

NOTE The first time you configure audit logging, we suggest using only the **?** option, to see all the available options in the configuration process. See also "[audit config](#)" on page 1 in the *LunaSH Command Reference Guide*.

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

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

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

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

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

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

Log Entries

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

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

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

Copying Log Files Off the Appliance

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

To copy files off the appliance

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

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

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

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

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

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

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

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

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

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

Exporting the Audit Logging Secret and Importing to a Verifying HSM

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

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

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

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

The filename is displayed when the secret is exported. You can check the filename with **my file list**.

2. On a computer connected to both HSMs, use **scp** or **pscp** to transfer the logging secret from the appliance.

- If you are planning to verify logs with a SafeNet Luna PCIe HSM, you can use the PCIe HSM's host computer.
- If you are planning to verify logs with a second SafeNet Luna Network HSM, you must transfer the logging secret to a client computer, and then to the second appliance.

Linux	<pre><client_install_dir>:> scp audit@<hostname_or_IP>:<log_secret_file> . Then, if transferring to a second SafeNet Luna Network HSM: <client_install_dir>:> scp <log_secret_file> audit@<hostname_or_IP>:</pre>
Windows	<pre><client_install_dir>:> pscp audit@ <hostname_or_IP>:<log_secret_file> . Then, if transferring to a second SafeNet Luna Network HSM: <client_install_dir>:> pscp <log_secret_file> audit@<hostname_or_IP>:</pre>

This copies the identified file from the remote SafeNet Luna Network HSM's file system (in the "audit" account) and stores the copy on your local computer file system in the directory from which you issued the command. Provide the audit user's credentials when prompted.

3. Login to the verifying HSM as the audit user. For this example, we will assume that you have already initialized the HSM audit user role, using the same domain/secret as is associated with the source HSM.
 - If you are using a SafeNet Luna Network HSM, connect via SSH and login to LunaSH as the audit user:

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

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

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

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

```
lunash:>audit log verify -file <audit_log_filename>.log
```
 - SafeNet Luna PCIe HSM (LunaCM):

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

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

Reading the Audit Log Records

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

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

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

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

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

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

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

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

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

```
150718020
```

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

Audit Role Authentication Considerations

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

Audit Logging General Advice and Recommendations

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

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

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

- > Use a shell script to execute the **audit sync** command at least once every 24 hours, provided the host has maintained its connection(s) to its configured NTP server(s).
- > Do not allow synchronization with the host's clock if the host has lost connectivity to NTP. This ensures that the HSM's internal clock is not set to a less accurate time than it has maintained internally. In general, the HSM's RTC will drift much less than the host's RTC and will, therefore, be significantly more accurate than the host in the absence of NTP.
- > Review logs at least daily and adjust configuration settings if necessary. It is important that any anomalies be identified as soon as possible and that the logging configuration that has been set is effective. If possible, use the remote logging feature to transmit log data to a Security Information and Event Management (SIEM) system to automatically analyze log data and identify anomalous events.
- > Execute the **audit log tarlogs** LunaSH command regularly to archive the audit logs and transfer them to a separate machine for long term storage. Also, execute the **audit log clear** LunaSH command regularly to free up the audit log disk space on SafeNet Luna Network HSM.
- > Consider installing and configuring a SafeNet Luna PCIe HSM in (or connected to) the remote log server to act as a "verification engine" for the remote log server. Ensure that the log secret for the operational HSM(s) has been shared with the log server verification HSM.

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

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

An important element of the security audit logging feature is the 'Log External' function. See the *SDK Reference Guide* for more information. For applications that cannot add this function call, it is possible to use the LunaCM command-line function **audit log external** within a startup script to insert a text record at the time the application is started.

Disk Full

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

To resolve that situation, the audit user must:

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

4. Restart the callback service (**service restart cbs**).

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

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

Audit Log Categories and HSM Events

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

HSM Access

HSM Event	Description
LUNA_LOGIN	C_Login. This event must be allowed to proceed even if the result should be logged but cannot (for example, due to a log full condition).
LUNA_LOGOUT	C_Logout. This event must be allowed to proceed even if the result should be logged but cannot (for example, due to a log full condition).
LUNA_MODIFY_OBJECT	C_SetAttributeValue
LUNA_OPEN_SESSION	C_OpenSession. This event must be allowed to proceed even if the result should be logged but cannot (for example, due to a log full condition).
LUNA_CLOSE_ALL_SESSIONS	C_CloseAllSessions
LUNA_CLOSE_SESSION	C_CloseSession This event must be allowed to proceed even if the result should be logged but cannot (for example, due to a log full condition).
LUNA_OPEN_ACCESS	CA_OpenApplicationID
LUNA_CLEAN_ACCESS	CA_Restart, CA_RestartForContainer
LUNA_CLOSE_ACCESS	CA_CloseApplicationID
LUNA_LOAD_CUSTOM_MODULE	CA_LoadModule

HSM Event	Description
LUNA_LOAD_ENCRYPTED_CUSTOM_MODULE	CA_LoadEncryptedModule
LUNA_UNLOAD_CUSTOM_MODULE	CA_UnloadModule
LUNA_EXECUTE_CUSTOM_COMMAND	CA_PerformModuleCall
LUNA_HA_LOGIN	CA_HAGetLoginChallenge, CA_HAAnswerLoginChallenge, CA_HALogin, CA_HAAnswerMofNChallenge, HAActivateMofN

Log External

HSM Event	Description
LUNA_LOG_EXTERNAL	CA_LogExternal

HSM Management

HSM Event	Description
LUNA_ZEROIZE	CA_FactoryReset This event is logged unconditionally.
LUNA_INIT_TOKEN	C_InitToken This event is logged unconditionally.
LUNA_SET_PIN	C_SetPIN
LUNA_INIT_PIN	C_InitPIN
LUNA_CREATE_CONTAINER	CA_CreateContainer
LUNA_DELETE_CONTAINER	CA_DeleteContainer, CA_DeleteContainerWithHandle
LUNA_SEED_RANDOM	C_SeedRandom
LUNA_EXTRACT_CONTEXTS	C_GetOperationState

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

HSM Event	Description
LUNA_SET_CONTAINER_SIZE	CA_SetContainerSize

Key Management

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

HSM Event	Description
LUNA_M_OF_N_ACTIVATE	CA_ActivateMofN
LUNA_M_OF_N_MODIFY	CA_ActivateMofN
LUNA_EXTRACT	CA_Extract
LUNA_INSERT	CA_Insert
LUNA_LKM_COMMAND	CA_LKMInitiatorChallenge, CA_LKMReceiverResponse, CA_LKMInitiatorComplete, CA_LKMReceiverComplete.
LUNA_MODIFY_USAGE_COUNT	CA_ModifyUsageCount

Key Usage and Key First Usage

HSM Event	Description
LUNA_ENCRYPT_INIT	C_EncryptInit
LUNA_ENCRYPT	C_Encrypt
LUNA_ENCRYPT_END	C_EncryptFinal
LUNA_DECRYPT_INIT	C_DecryptInit
LUNA_DECRYPT	C_Decrypt
LUNA_DECRYPT_END	C_DecryptFinal
LUNA_DIGEST_INIT	C_DigestInit
LUNA_DIGEST	C_Digest
LUNA_DIGEST_KEY	C_DigestKey
LUNA_DIGEST_END	C_DigestFinal
LUNA_SIGN_INIT	C_SignInit
LUNA_SIGN	C_Sign
LUNA_SIGN_END	C_SignFinal

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

Audit Log Management

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

Remote Audit Logging

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

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

UDP Considerations

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

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

Possible approaches include the following:

> With templates:

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

> Without templates:

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

> Dynamic filename:

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

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

Example using TCP

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

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

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

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

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

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

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

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

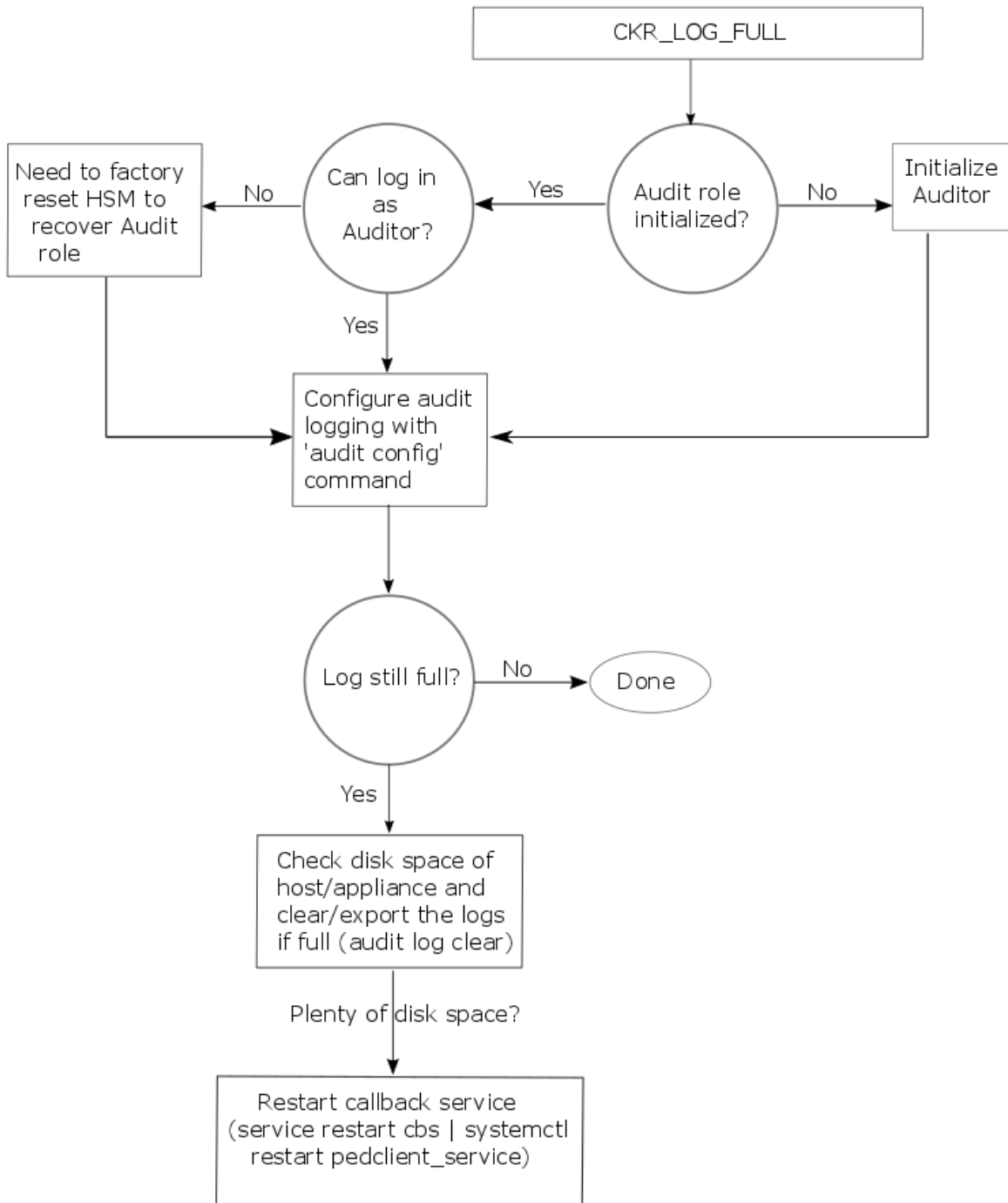
```
# service rsyslog restart
```

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

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

Audit log troubleshooting

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



CHAPTER 3: Backup and Restore Using a G5-Based Backup HSM

SafeNet 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 SafeNet Luna G5 Backup HSM" on page 57](#)
 - ["Installing the Backup HSM" on page 60](#)
 - ["Installing or Replacing the Backup HSM Battery" on page 60](#)
 - ["Backup HSM Secure Transport and Tamper Recovery" on page 63](#)
 - ["Resetting the Backup HSM to Factory Conditions" on page 68](#)
- > [Backing Up and Restoring the Appliance Configuration](#)
- > ["Backup/Restore Using an Appliance-Connected Backup HSM" on page 68](#)
- > ["Backup/Restore Using a Client-Connected Backup HSM" on page 71](#)
- > ["Configuring a Remote Backup HSM Server" on page 74](#)

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 SafeNet Luna Backup HSM or an application partition on any other Luna HSM for backup/restore operations.

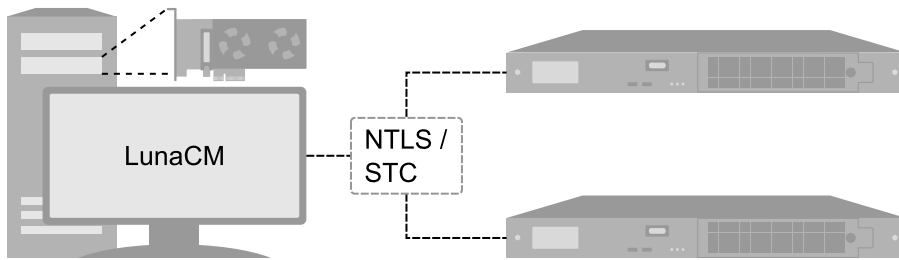
Backup and restore operations require that cloning be enabled on the HSM/partition.

- > ["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 56](#)

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 237](#).

Backup HSM Connected to the Appliance

In this configuration, the SafeNet Luna Backup HSM is connected directly to one of the USB ports on the SafeNet 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

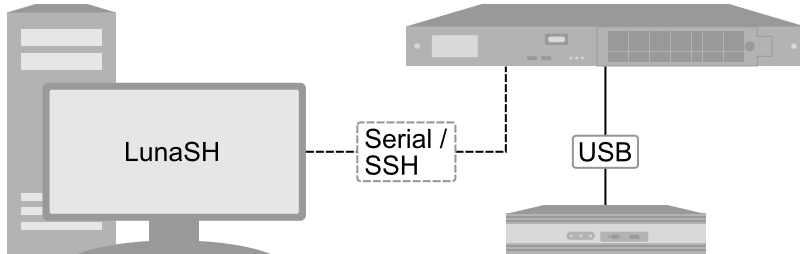
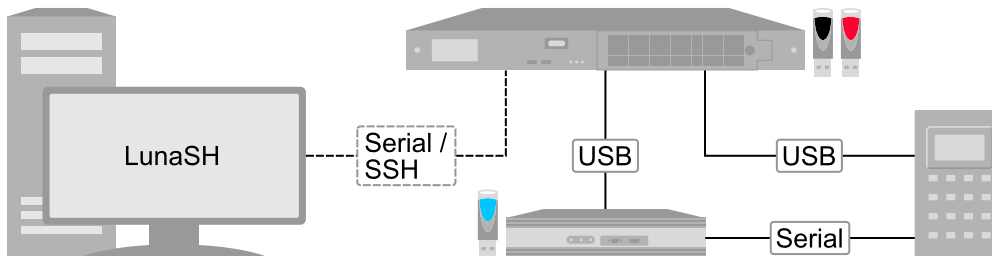


Figure 2: Locally-connected Backup HSM using local PED authentication



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 Backup HSM" on page 68](#).

Backup HSM Connected to the Client Workstation

In this configuration, the SafeNet 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

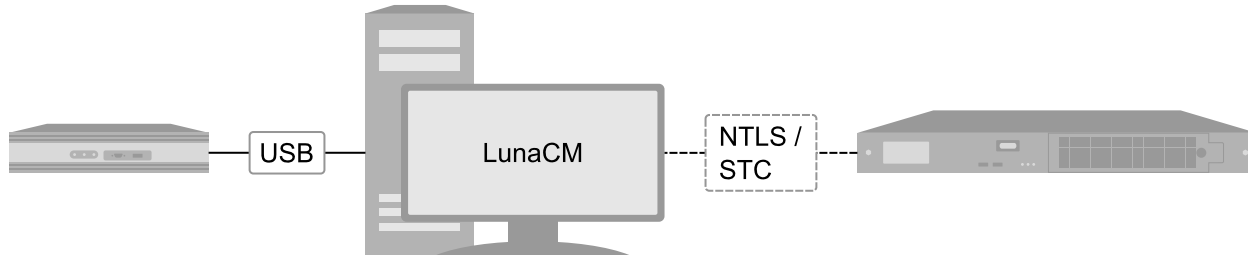
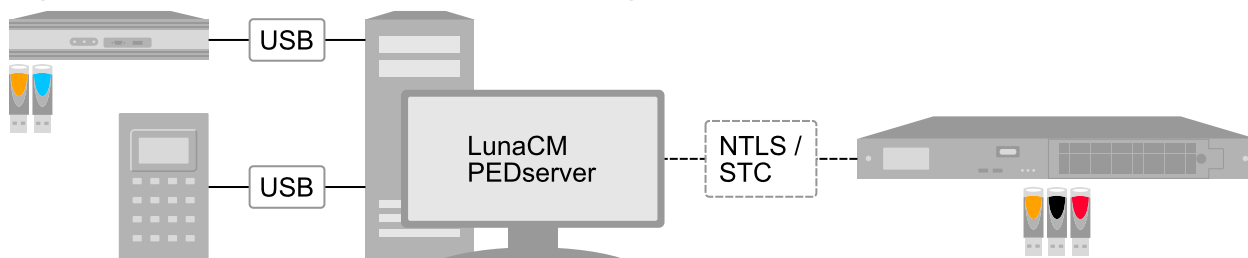


Figure 4: Client-connected backup HSM using remote PED authentication



See "[Backup/Restore Using a Client-Connected Backup HSM](#)" on page 71.

Backup HSM Installed Using Remote Backup Service (RBS)

In this configuration, the SafeNet 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 SafeNet Luna Network HSM, to mitigate the consequences of catastrophic loss (fire, flood, etc).

Figure 5: Remote backup (RBS) using password authentication

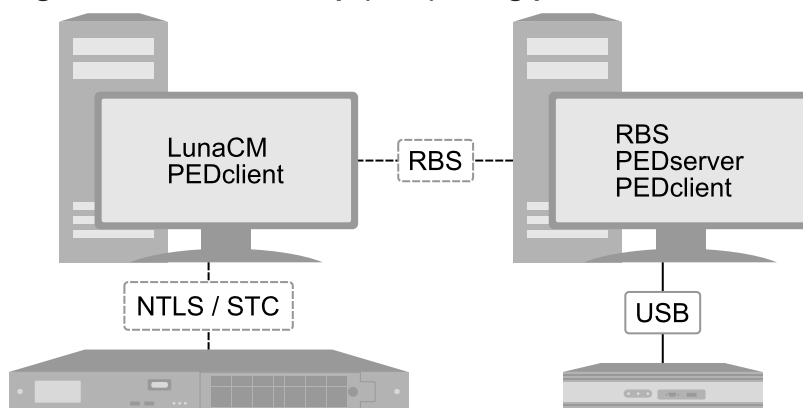
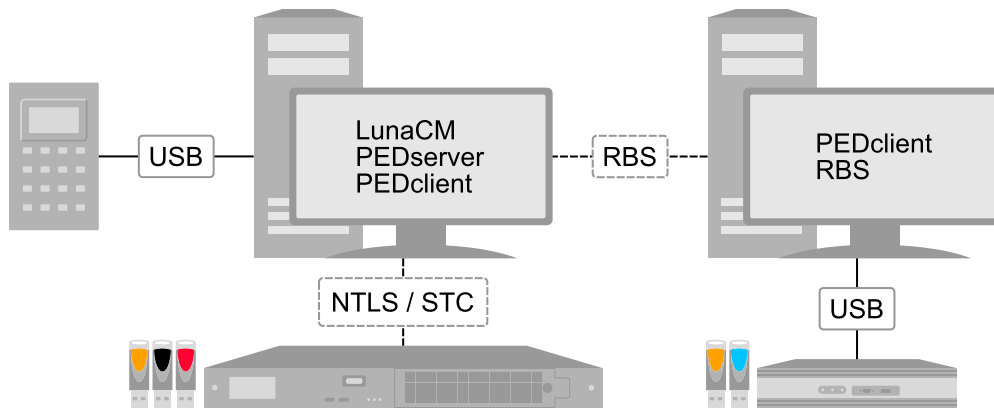
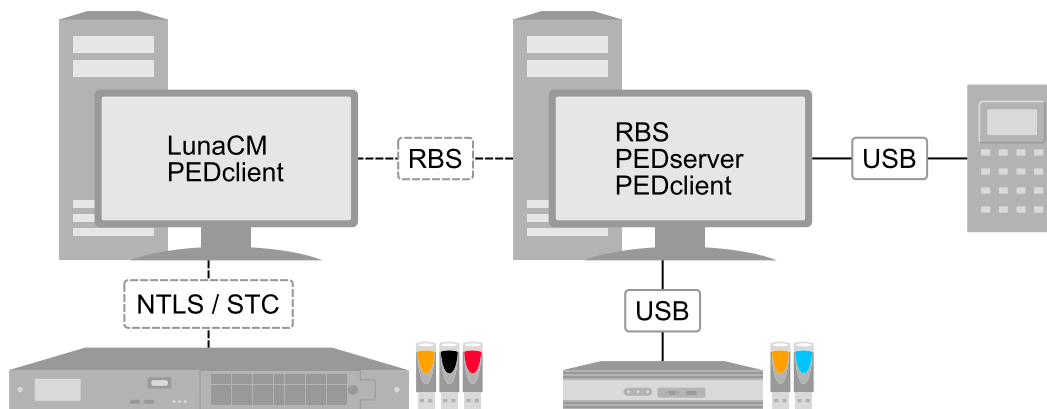


Figure 6: Remote backup (RBS) using remote PED authentication at the client**Figure 7: Remote backup (RBS) using remote PED authentication at the RBS server**

See ["Configuring a Remote Backup HSM Server" on page 74](#).

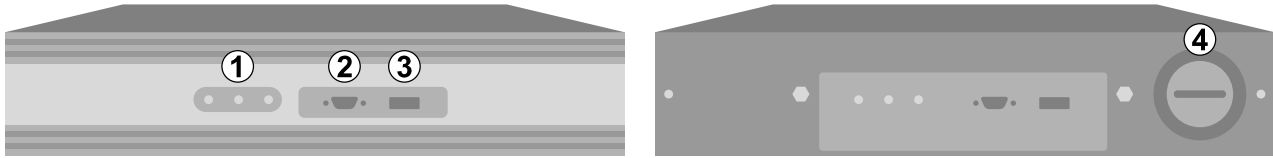
About the SafeNet Luna G5 Backup HSM

The SafeNet Luna Backup HSM 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 SafeNet Luna Backup HSM:

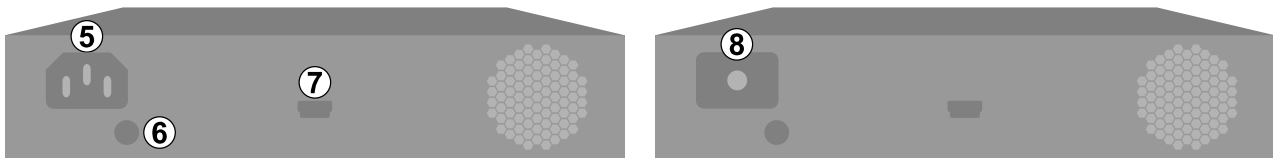
- > ["Physical Features" on the next page](#)
- > ["Backup HSM Functionality" on the next page](#)
- > ["Storage and Maintenance" on page 59](#)
- > ["Installing the Backup HSM" on page 60](#)
- > ["Installing or Replacing the Backup HSM Battery" on page 60](#)
- > ["Backup HSM Secure Transport and Tamper Recovery" on page 63](#)
- > ["Initializing the Backup HSM Remote PED Vector" on page 66](#)
- > ["Resetting the Backup HSM to Factory Conditions" on page 68](#)

Physical Features

The front panel of the SafeNet Luna Backup HSM (G5 model) 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 SafeNet Luna Backup HSM (G5 model) 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"> > Active: The Backup HSM is performing a procedure. Do not disconnect or unplug the device when this light is illuminated. > Tamper: The Backup HSM is in a tamper state. You must clear the tamper state before backing up or restoring partitions. > Error: HSM device driver error. Contact Thales Group Customer Support (see "Support Contacts" on page 16).
2	Serial port for attaching a local SafeNet 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 "Installing or Replacing the Backup HSM Battery" on page 60.
5	Power connector for a SafeNet Luna Backup HSM with an internal power supply. See "Storage and Maintenance" on the next page for more information.
6	Index hole. Engages with the index post on a SafeNet Luna Backup HSM rack shelf.
7	Mini-USB port for connecting the SafeNet Luna Backup HSM to a SafeNet HSM or client workstation. See "Installing the Backup HSM" on page 60.
8	Power source connector for a SafeNet Luna Backup HSM with an external power supply (included).

Backup HSM Functionality

The SafeNet Luna Backup HSM allows you to back up application partitions from one or more Luna HSMs. Backup operations are performed on a per-partition basis.

Password or PED Authentication

The SafeNet Luna Backup HSM can be configured to back up either password- or PED-authenticated partitions. You must specify the authentication method when you initialize the 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 SafeNet Luna Backup HSM Firmware" on page 399](#).

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 SafeNet 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 SafeNet 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 Group 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 63](#)). 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.

Installing the Backup HSM

You can connect the SafeNet Luna Backup HSM to a SafeNet Luna Network HSM, a SafeNet Luna HSM Client workstation, or a host machine containing a SafeNet Luna PCIe HSM. Refer to ["Planning Your Backup HSM Deployment" on page 54](#) for detailed descriptions of the configuration options.

To install the Safenet Luna Backup HSM

1. Connect the SafeNet 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 SafeNet Luna HSM Client installer (see ["SafeNet Luna HSM Client Software Installation" on page 1](#) for details).
3. [Local PED] If you plan to authenticate the SafeNet 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 58](#)).
To use the same local PED to authenticate both the Backup HSM and SafeNet Luna Network HSM, connect the PED to the SafeNet Luna Network HSM using a USB Mini-B to USB cable (see ["Physical Features" on page 248](#)). You can switch between the two using PED modes (see ["Modes of Operation" on page 250](#)).
4. Connect the SafeNet Luna Backup HSM using the included Mini-USB to USB cable. If you are connecting the Backup HSM to:
 - a. **SafeNet Luna Network HSM:** Connect to one of the USB ports on the front or rear panel of the appliance.
 - b. **SafeNet Luna HSM Client:** Connect to a USB port on the client workstation.
 - c. **SafeNet 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 63](#).

Installing or Replacing the Backup HSM Battery

The SafeNet Luna Backup HSM 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-SOCI₂)
- > 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 SafeNet Luna Backup HSM 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.



5. 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.



6. Replace the front bezel by aligning the clips with their posts and pushing it into place.
7. Removing the battery causes a tamper event on the Backup HSM. To clear the tamper, see ["Backup HSM Secure Transport and Tamper Recovery"](#) below.

Backup HSM Secure Transport and Tamper Recovery

The SafeNet Luna Backup HSM recognizes a similar list of tamper conditions to the SafeNet Luna Network HSM (see ["Tamper Events"](#) on page 348). 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 SafeNet 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 SafeNet Luna Network HSM (see ["Secure Transport Mode"](#) on page 328 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" on the next page](#)

- > ["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 66](#)

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 60](#)). This procedure is only available using LunaCM. If the Backup HSM is connected directly to a SafeNet Luna Network HSM, disconnect it and connect it to a workstation with SafeNet 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 276](#)).
 - [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 250](#)).
 - [Remote PED] Set up a Remote PED server to authenticate the Backup HSM (see ["Remote PED Setup" on page 257](#)).
 - [Remote PED] Initialize the Backup HSM RPV (see ["Initializing the Backup HSM Remote PED Vector" on page 66](#)). 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 SafeNet 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 SafeNet 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 SafeNet 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 SafeNet 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 SafeNet 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.

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

Prerequisites

- > SafeNet Luna PED with firmware 2.7.1 or newer

- > USB mini-B to USB-A connector cable
- > Luna PED DC power supply (if included with your Luna PED)
- > Blank or reusable orange PED key (or multiple keys, if you plan to make extra copies or use an M of N security scheme). See ["Creating PED Keys" on page 276](#) for more information.
- > Install the Backup HSM at the client and connect it to power (see ["Installing the Backup HSM" on page 60](#)).
- > 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 250](#)).

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 276](#) 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 261](#).

Resetting the Backup HSM to Factory Conditions

These instructions will allow you to restore your SafeNet 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 SafeNet 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 SafeNet 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 Backup HSM

You can connect the SafeNet Luna Backup HSM directly to one of the USB ports on the SafeNet 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 This deployment 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 (see ["Backup/Restore Using a Client-Connected Backup HSM" on page 71](#)).

This configuration cannot be used with Remote PED.

This section provides instructions for the following procedures using this kind of deployment:

- > ["Initializing the Backup HSM" on the next page](#)
- > ["Backing Up an Application Partition" on the next page](#)
- > ["Restoring an Application Partition from Backup" on page 70](#)

Initializing the Backup HSM

Before you can use the SafeNet 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 60](#)).
- > 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 63](#)).
- > [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 276](#)).
- > [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 250](#)).

To initialize a locally-connected Backup HSM using LunaSH on the SafeNet Luna Network HSM

1. Log in to LunaSH as **admin**, or an **admin**-level custom user.
2. [Optional] View the SafeNet 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 SafeNet 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" above](#)).
- > You must have **admin** or **admin**-level access to LunaSH on the SafeNet Luna Network HSM.
- > **Partition policy 0: Allow private 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 SafeNet Luna Network HSM using a Mini-B to USB-A cable (see ["Local PED Setup" on page 251](#)), 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 250](#)).

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. [Optional] View the SafeNet Luna Backup HSMs currently connected to the appliance and find the correct serial number.

```
lunash:> token backup list
```

3. 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, include the **-add** option to add 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.

```
lunash:> partition backup -partition <source_label> -tokenpar <target_label> -serial <Backup_HSM_serialnum> [-add]
```

You are prompted for the source partition's Crypto Officer credential (black PED key or challenge secret).

4. [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 250](#)). 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 SafeNet Luna Network HSM.
- > **Partition policy 0: Allow private 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 SafeNet Luna Network HSM using a Mini-B to USB-A cable (see ["Local PED Setup" on page 251](#)), 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 250](#)).

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. [Optional] View the SafeNet Luna Backup HSMs currently connected to the appliance and find the correct serial number.

```
lunash:> token backup list
```
3. [Optional] View the backups currently available on the Backup HSM.

```
lunash:> token backup partition list -serial <Backup_HSM_serialnum>
```
4. 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

```
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).

5. [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 250](#)). 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 Backup HSM

You can connect the SafeNet 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 73](#)

Initializing the Backup HSM

Before you can use the SafeNet 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 60](#)).
- > 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 63](#)).
- > [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 276](#)).
 - [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 250](#)).
 - [Remote PED] Initialize the Backup HSM RPV (see ["Initializing the Backup HSM Remote PED Vector" on page 66](#)). 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 257](#)).

To initialize a client-connected Backup HSM

1. Launch LunaCM on the client workstation.
2. Set the active slot to the SafeNet 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. 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 SafeNet 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](#)).
- > **Partition policy 0: Allow private 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.
- > 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 23](#)), 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 66](#)). If the source partition is not activated, you may need the orange PED key for the SafeNet 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 257](#)). 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

1. Launch LunaCM on the client workstation.
2. 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 250](#)).
- [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**]

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.
- > **Partition policy 0: Allow private key cloning** must be 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 23](#)), 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 257](#)). 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.

- Set the active slot to the target partition and log in as Crypto Officer.

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

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

- [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 250](#)).

- [Remote PED] Connect the Backup HSM slot to PEDserver.

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

- [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>
```

- [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>
```

- 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.

```
lunacm:> partition archive restore -slot <Backup_HSM_slotnum> -partition <backup_label> [-replace]
```

You are prompted for the backup's Crypto Officer credential.

The backup contents are cloned to the application partition.

Configuring a Remote Backup HSM Server

In this configuration, The SafeNet 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 SafeNet Luna Network HSM, to protect against catastrophic loss (fire, flood, etc).

RBS is a utility, included with the SafeNet 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/Configuring the Remote Backup Service

RBS is installed using the SafeNet 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 SafeNet Luna Network HSM client workstation, install the following SafeNet Luna HSM Client components (see ["SafeNet Luna HSM Client Software Installation" on page 1](#)):

- **Network**
 - **Remote PED:** if you are backing up PED-authenticated partitions
- > Install the SafeNet Luna Backup HSM(s) at the workstation that will host RBS (see ["Installing the Backup HSM" on page 60](#)).
- > [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 66](#)).

To install and configure RBS

1. On the workstation hosting the Backup HSM(s), install the **Backup** component of the SafeNet Luna HSM Client (see ["SafeNet Luna HSM Client Software Installation" on page 1](#)). If this workstation will also host a Remote PED, install the **Remote PED** component as well (Windows only).
2. Navigate to the SafeNet 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**

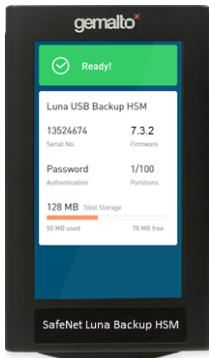
RBS displays a list of Backup HSMs currently connected to the workstation. Select the ones you want to provide remote backup services. When you have specified your selection, enter **X** to exit the configuration tool.
4. Launch the RBS daemon (Linux/UNIX) or console application (Windows).
 - Linux/UNIX: # **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 SafeNet Luna HSM Client workstation (["SCP and PSCP" on page 1](#)).
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 Backup HSM" on page 71](#) for procedures.

CHAPTER 4: Backup and Restore Using a G7-Based Backup HSM



The following topics describe how to configure and use the G7-based SafeNet Luna Backup HSM to backup and restore the cryptographic objects in your user partitions. You can perform backup and restore operations by connecting the G7-based SafeNet Luna Backup HSM to a SafeNet Luna HSM Client workstation or SafeNet Luna Network HSM appliance:

About Backup/Restore Using the G7-based SafeNet Luna Backup HSM

> ["Overview and Key Concepts" below](#)

Backup/Restore from a SafeNet Luna HSM Client Workstation Using LunaCM

> ["Initializing a Client-Connected G7-Based Backup HSM" on page 79](#)

> ["Backing Up to a Client-Connected G7-Based Backup HSM" on page 83](#)

> ["Restoring From a Client-Connected G7-Based Backup HSM" on page 89](#)

Backup/Restore from a SafeNet Luna HSM Client Workstation Using the Remote Backup Service (RBS)

> ["Backup and Restore to a Remote Backup Service \(RBS\)-Connected G7-Based Backup HSM" on page 93](#)

NOTE This feature has software and/or firmware dependencies. See ["Version Dependencies by Feature" on page 393](#) for more information.

Overview and Key Concepts

This topic provides the following background information you need to perform backup and restore operations using a G7-based backup HSM:

> ["Overview" below](#)

> ["Credentials Required to Perform Backup and Restore Operations" on the next page](#)

> ["Client Software Required to Perform Backup and Restore Operations From a Client Workstation" on page 78](#)

> ["PED Authentication with the G7-Based Backup HSM" on page 78](#)

> ["Backup and Restore Best Practices" on page 78](#)

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 SafeNet Luna HSM Client workstation, or to a SafeNet Luna Network HSM appliance:

- > When you connect the backup HSM to a SafeNet 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 SafeNet 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.

NOTE You can connect the backup HSM to any USB port on the client workstation or SafeNet Luna Network HSM appliance. Do not attempt to connect the backup HSM to the USB port on the HSM card.

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:

<source> User HSM	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.
<source> User Partition	<p>Crypto Officer (CO). Required to access the objects in the <source> user partition that will be backed up.</p> <p>Domain. Required to allow objects to be cloned between the <source> user partition and <target> backup partition. The domains for the <source> user partition and <target> backup partition must match, otherwise the backup will fail.</p>
<target> Backup HSM	<p>HSM Security Officer (SO). Required to create or access the <target> 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 <target> backup partition.</p> <p>Note: You create new credentials for both roles on HSM initialization, and use them for subsequent backups to the <target> backup HSM.</p>
<target> Backup Partition	<p>Partition owner (PSO). Required to access the <target> backup partition.</p> <p>Crypto Officer (CO). Required to access the objects in the <target> backup partition.</p> <p>Note: You create new credentials for both roles on the initial backup, and use them for subsequent backups to the <target> backup partition.</p>

Client Software Required to Perform Backup and Restore Operations From a Client Workstation

You must install the SafeNet Luna HSM Client software and USB driver for the backup HSM on the workstation you intend to use to perform backup and restore operations. See the release notes for supported versions and operating systems, and refer to [SafeNet Luna HSM Client Software Installation](#) for detailed installation instructions.

NOTE Ensure that the backup HSM is not connected to the SafeNet 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 G7-Based Backup HSM

The G7-based backup HSM is equipped with a single USB port that is used to connect the backup HSM to a SafeNet Luna HSM Client workstation or SafeNet Luna Network HSM appliance. As such, any PED connections to the backup HSM must use a remote PED and the **pedserver** service:

- > When the G7-based backup HSM is connected to a client workstation, you authenticate to it with a remote PED that is connected to the same client workstation used to host the backup HSM, or to a separate workstation used to host the remote PED. 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.

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.

Initializing a Client-Connected G7-Based Backup HSM

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" on page 430](#)). 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 82](#)

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 SafeNet 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.

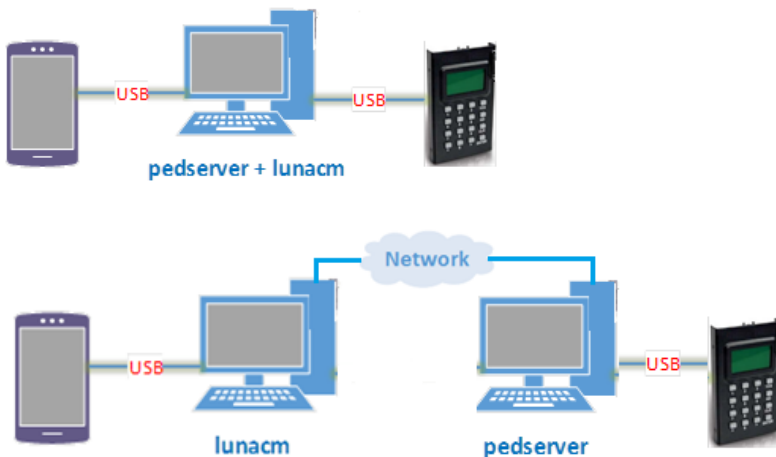
Prerequisites

Before beginning, ensure that you are familiar with the concepts in ["PED Authentication" on page 242](#). 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 SafeNet Luna HSM Client workstation using one of the following configurations:



- a. Install the required client software on the SafeNet Luna HSM Client workstation. See ["Initializing a Client-Connected G7-Based Backup HSM" on the previous page](#) for details.
- b. Connect the backup HSM directly to the SafeNet 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 SafeNet 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:

Windows	C:\Program Files\Safenet\LunaClient> "pedserver mode start" on page 315
Linux	/usr/safenet/lunaclient> "pedserver mode start" on page 315

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" on page 328** for more information:

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

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

6. Connect to the SafeNet 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 -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
```

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.

9. 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
```

10. 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 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.

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

```
lunacm:> hsm init -iped -label USB_BACKUP_HSM_G7
```

11. 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 286](#) for details.
12. 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 SafeNet 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.

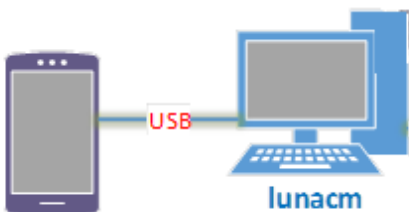
### Prerequisites

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

1. Configure your SafeNet Luna HSM Client workstation as illustrated below:



- a. Install the required client software on the SafeNet Luna HSM Client workstation. See ["Initializing a Client-Connected G7-Based Backup HSM" on page 79](#) for details.
- b. Connect the backup HSM directly to the SafeNet 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](#)" on page 328 for more information:

```
lunacm:> stm recover
```

**NOTE** Recovering a G7-based HSM 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 G7-Based Backup HSM

To perform a backup, you connect the backup HSM to the SafeNet 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 87](#)

### 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 SafeNet 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.

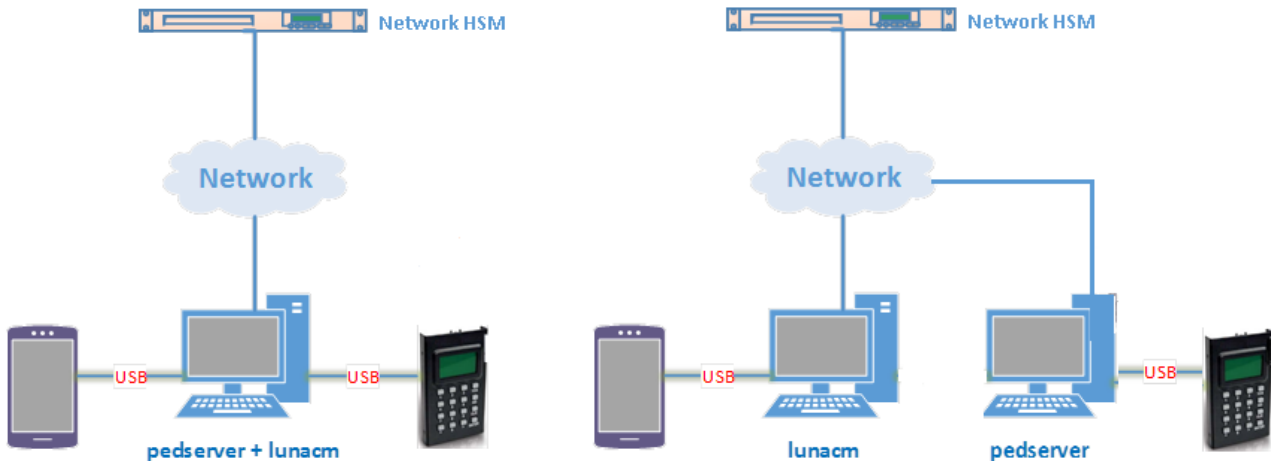
### Prerequisites

Before beginning, ensure that you are familiar with the concepts in ["PED Authentication" on page 242](#). You require the credentials listed in ["Backing Up to a Client-Connected G7-Based Backup HSM" on the previous page](#).

**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 23](#) for more information.

### To backup a PED-authenticated partition

1. Configure your SafeNet Luna HSM Client workstation using one of the following configurations:



- a. Install the required client software on the SafeNet Luna HSM Client workstation. See ["Backing Up to a Client-Connected G7-Based Backup HSM" on the previous page](#) for details.
- b. Connect the backup HSM directly to the SafeNet 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 SafeNet 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 315 |
| <b>Linux</b>   | /usr/safenet/lunaclient> <b>pedserver mode start</b> on page 315             |

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 SafeNet 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 SafeNet 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 &lt;source&gt; 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>]
```

If you omit the **-partition** option when creating a new backup, the partition is assigned a default name (<source\_partition\_name>\_<YYYYMMDD>).

## 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.

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. |

**-append  
and -  
replace**

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).

**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 286](#) 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 SafeNet Luna HSM Client workstation that hosts the slot for the partition you want to backup, and perform the following tasks:

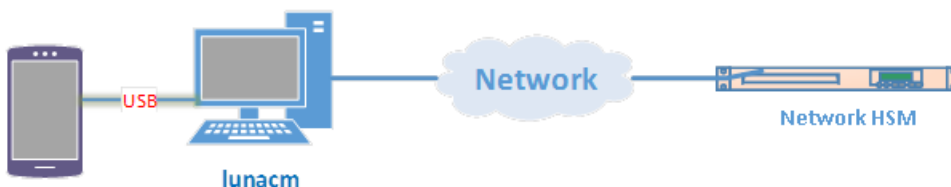
1. Log in to the <source> user partition as the Crypto Officer (CO).
2. Perform the backup operation and respond to the prompts for the HSM SO, partition SO (PO), crypto officer (CO), and domain passwords for the backup HSM/partition. The backup HSM and the partition you want to restore to must be members of the same domain.

### Prerequisites

You require the credentials listed in ["Backing Up to a Client-Connected G7-Based Backup HSM" on page 83](#).

### To backup a password-authenticated partition

**1.** Configure your SafeNet Luna HSM Client workstation as illustrated below:



- a.** Install the required client software on the SafeNet Luna HSM Client workstation and start LunaCM. See ["Backing Up to a Client-Connected G7-Based Backup HSM" on page 83](#) for more information.
- b.** Connect the backup HSM directly to the SafeNet 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>]

If you omit the **-partition** option when creating a new backup, the partition is assigned a default name (<source\_partition\_name>\_<YYYYMMDD>).

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.

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 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). |



## Restoring From a Client-Connected G7-Based Backup HSM

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, as detailed in ["Restoring From a Client-Connected G7-Based Backup HSM" above](#).

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 91](#)

### 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 SafeNet 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.

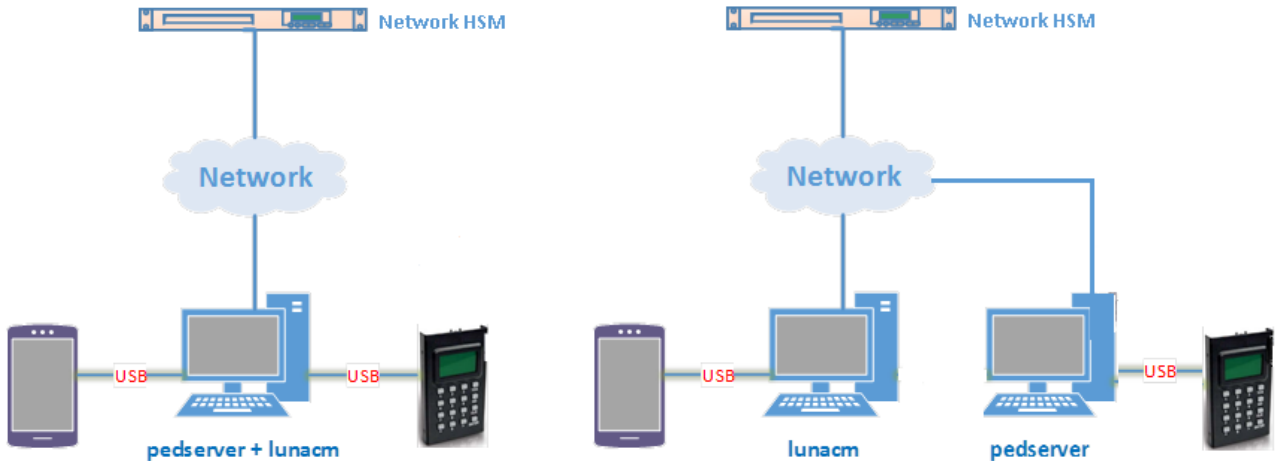
#### Prerequisites

Before beginning, ensure that you are familiar with the concepts in ["PED Authentication" on page 242](#). You require the credentials listed in ["Restoring From a Client-Connected G7-Based Backup HSM" 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 23](#) for more information.

#### To restore a PED-authenticated partition

1. Configure your SafeNet Luna HSM Client workstation using one of the following configurations:



- a. Install the required client software on the SafeNet Luna HSM Client workstation. See ["Restoring From a Client-Connected G7-Based Backup HSM"](#) on the previous page for details.
- b. Connect the backup HSM directly to the SafeNet 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 SafeNet 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"](#) on page 95 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> <b>"pedserver mode start" on page 315</b> |
| <b>Linux</b>   | /usr/safenet/lunaclient> <b>"pedserver mode start" on page 315</b>             |

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 SafeNet 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, as detailed in ["Restoring From a Client-Connected G7-Based Backup HSM" on page 89](#).

```
lunacm:> partition archive restore -slot <backup_HSM_admin_slot> -partition <target_partition_label>
```

The restore operation begins once you have completed the authentication process. Objects are restored one at a time.

## 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 SafeNet 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):

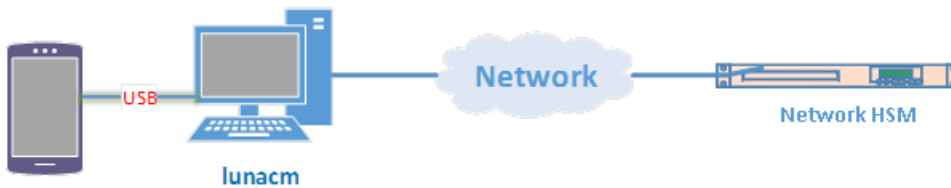
- Perform the restore operation. You are prompted for the HSM SO, partition SO (PO), crypto officer (CO), and domain passwords for the backup partition. The backup HSM and the partition you want to restore to must be members of the same domain.

### Prerequisites

You require the credentials listed in ["Restoring From a Client-Connected G7-Based Backup HSM" on page 89](#).

### To restore a password-authenticated partition

- Configure your SafeNet Luna HSM Client workstation as illustrated below:



- Install the required client software on the SafeNet Luna HSM Client workstation and start LunaCM. See ["Restoring From a Client-Connected G7-Based Backup HSM" on page 89](#) for more information.
- Connect the backup HSM directly to the SafeNet 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.

- 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" on page 95](#) for more information.
- 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.

- Select the user partition you want to restore to:

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

- Log in to the user partition as the Crypto Officer (CO):

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

- Initiate the restore operation. Respond to the prompts to provide the required passwords, as detailed in ["Restoring From a Client-Connected G7-Based Backup HSM" on page 89](#)

```
lunacm:> partition archive restore -slot <backup_HSM_admin_slot> -partition <target_partition_label>
```

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 G7-Based Backup HSM

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 SafeNet 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 SafeNet Luna Network HSM, to protect against catastrophic loss (fire, flood, etc).

RBS is a utility, included with the SafeNet 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 SafeNet 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

- > Install the following SafeNet Luna HSM Client components on any SafeNet Luna Network HSM client workstation that hosts slots for the partitions you want to backup using RBS (see [SafeNet Luna HSM Client Software Installation](#)):
  - **Network**
  - **Remote PED:** if you are backing up PED-authenticated partitions.
- > Connect the backup HSM(s) directly to the SafeNet 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 G7-Based Backup HSM](#)" on [page 79](#).
- > 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 SafeNet Luna HSM Client (see ["SafeNet Luna HSM Client Software Installation" on page 1](#)). If this workstation will also host a Remote PED, install the **Remote PED** component as well (Windows only).
2. Navigate to the SafeNet 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 SafeNet Luna HSM Client workstation (see [SCP and PSCP](#)).
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 G7-Based Backup HSM" on page 83](#) and ["Restoring From a Client-Connected G7-Based Backup HSM" on page 89](#) for detailed procedures.

# CHAPTER 5: Capabilities and Policies

The SafeNet Luna Network HSM's configuration is based on HSM capabilities, displayed using the LunaSH command **hsm showpolicies**. They are set at manufacture according to the model you selected at time of purchase. Capabilities can only be modified by purchase and application of capability updates.

A subset of HSM capabilities have corresponding HSM policies that allow you to customize the HSM configuration. Policies can be modified based on your specific needs. For example, you can restrict the HSM to use only FIPS-approved algorithms (FIPS mode) by setting HSM policy **12** to 1 (on).

Partitions inherit the capabilities and policy settings of the HSM. Partitions also have policies that can be set to customize the partition functions. Partition policies can never be modified to be less secure than the corresponding HSM capability/policy. For example, if HSM policy **7** is set to disallow cloning, partition policies **0** and **4**, which allow cloning of private or secret keys, cannot be set to 1 (on).

The HSM or Partition SO can create and apply Policy Templates to initialize multiple HSMs/partitions with the same preferred policy settings.

The following sections describe individual HSM/partition capabilities and policies:

- > ["HSM Capabilities and Policies" below](#)
  - ["Setting HSM Policies Manually" on page 103](#)
  - ["Setting HSM Policies Using a Template" on page 104](#)
- > ["Partition Capabilities and Policies" on page 106](#)
  - ["Setting Partition Policies Manually" on page 113](#)
  - ["Setting Partition Policies Using a Template" on page 114](#)
  - ["Configuring the Partition for Cloning or Export of Private Keys" on page 118](#)

## HSM Capabilities and Policies

---

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

- > **HSM Capabilities** are features of HSM functionality, set at manufacture based on the HSM model you selected at time of purchase. You can add new capabilities to the HSM by purchasing and applying capability licenses from Thales Group (see ["Upgrading HSM Capabilities and Partition Licenses" on page 401](#)). Some capabilities have corresponding modifiable HSM policies.
- > **HSM Policies** are configurable settings that allow the HSM Security Officer to modify the function of their corresponding capabilities. Some policies affect HSM-wide functionality, and others allow further customization of individual partitions by the Partition Security Officer.

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

- > ["Setting HSM Policies Manually" on page 103](#)

> ["Setting HSM Policies Using a Template" on page 104](#)

To zeroize the HSM and revert policies to their default values, see ["Resetting to Factory Condition" on page 167](#).

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

## Destructive Policies

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

| # | HSM Capability                                                                                                                                                                                                                                                                                                                                                                                           | HSM Policy |
|---|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|
| 0 | <p><b>Enable PIN-based authentication</b></p> <ul style="list-style-type: none"> <li>&gt; <b>Allowed:</b> The HSM authenticates all users with keyboard-entered passwords.</li> <li>&gt; <b>Disallowed:</b> See HSM capability 1 below.</li> </ul>                                                                                                                                                       | N/A        |
| 1 | <p><b>Enable PED-based authentication</b></p> <ul style="list-style-type: none"> <li>&gt; <b>Allowed:</b> The HSM authenticates users with secrets stored on physical PED keys, read by a SafeNet Luna PED. The Crypto Officer and Crypto User roles may also be configured with a secondary, keyboard-entered challenge secret.</li> <li>&gt; <b>Disallowed:</b> See HSM capability 0 above.</li> </ul> | N/A        |
| 2 | <p><b>Performance level</b></p> <p>Numerical value indicates the HSM's performance level, determined by the model you selected at time of purchase:</p> <ul style="list-style-type: none"> <li>&gt; <b>4: Standard</b> performance</li> <li>&gt; <b>8: Enterprise</b> performance</li> <li>&gt; <b>15: Maximum</b> performance</li> </ul>                                                                | N/A        |
| 4 | <p><b>Enable domestic mechanisms &amp; key sizes</b></p> <p>Always <b>allowed</b>. All SafeNet Luna Network HSMs are capable of full-strength cryptography with no US export restrictions.</p>                                                                                                                                                                                                           | N/A        |



| #  | HSM Capability                                                                                                                                                                                                                                                                                                                    | HSM Policy                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|----|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 6  | <p><b>Enable masking</b></p> <p>Always <b>disallowed</b>. SIM has been deprecated on all current SafeNet Luna Network HSMs.</p>                                                                                                                                                                                                   | N/A                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| 7  | <p><b>Enable cloning</b></p> <p>Always <b>allowed</b>. All current SafeNet Luna Network HSMs can clone cryptographic objects from one partition to another.</p>                                                                                                                                                                   | <p><b>Allow cloning (Destructive)</b></p> <ul style="list-style-type: none"> <li>&gt; <b>ON</b> (default): The HSM may clone cryptographic objects from one partition to another. This is required to back up partitions or include them in HA groups. Partition SOs can enable/disable cloning on individual partitions.</li> <li>&gt; <b>OFF</b>: No partition on the HSM may clone cryptographic objects. Partition SOs cannot change this.</li> </ul>                                                                                                                |
| 9  | <p><b>Enable full (non-backup) functionality</b></p> <ul style="list-style-type: none"> <li>&gt; <b>Allowed</b>: The HSM is capable of full cryptographic functions.</li> <li>&gt; <b>Disallowed</b>: The HSM is capable of backup functions only (disallowed on SafeNet Luna Backup HSMs only).</li> </ul>                       | N/A                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| 12 | <p><b>Enable non-FIPS algorithms</b></p> <p>Always <b>allowed</b>. The HSM can use all cryptographic algorithms described in <a href="#">Supported Mechanisms</a>.</p>                                                                                                                                                            | <p><b>Allow non-FIPS algorithms (Destructive)</b></p> <ul style="list-style-type: none"> <li>&gt; <b>ON</b> (default): The HSM may use all available cryptographic algorithms.</li> <li>&gt; <b>OFF</b>: Only algorithms sanctioned by the FIPS 140-2 standard are permitted. The following is displayed in the output from lunash:&gt; <b>hsm show</b>:</li> </ul> <pre>FIPS 140-2 Operation: ===== The HSM is in FIPS 140-2 approved operation mode.</pre>                                                                                                             |
| 15 | <p><b>Enable SO reset of partition PIN</b></p> <p>Always <b>allowed</b>. This capability enables:</p> <ul style="list-style-type: none"> <li>&gt; the Partition SO to reset the password or PED secret of the Crypto Officer.</li> <li>&gt; the Crypto Officer to reset the password or PED secret of the Crypto User.</li> </ul> | <p><b>SO can reset partition PIN (Destructive)</b></p> <ul style="list-style-type: none"> <li>&gt; <b>ON</b>: Partition SO may reset the password or PED secret of a Crypto Officer who has been locked out after too many failed login attempts.</li> <li>&gt; <b>OFF</b> (default): The CO lockout is permanent and the partition contents are no longer accessible. The partition must be re-initialized, and key material restored from a backup device.</li> </ul> <p>See "<a href="#">Resetting the Crypto Officer or Crypto User Credential</a>" on page 437.</p> |

| #  | HSM Capability                                                                                                                                                                                                                                                                                                                                                                         | HSM Policy                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|----|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 16 | <p><b>Enable network replication</b></p> <p>Always <b>allowed</b>. This capability enables cloning of cryptographic objects over a network. This is required for HA groups, and for partition backup to a remote or client-connected SafeNet Luna Backup HSM.</p>                                                                                                                      | <p><b>Allow network replication</b></p> <ul style="list-style-type: none"> <li>&gt; <b>ON</b> (default): Cloning of cryptographic objects is permitted over a network. Remote and client-connected backup is allowed, and the partition may be used in an HA group.</li> <li>&gt; <b>OFF</b>: Cloning over a network is not permitted. Partition backup is possible to a locally-connected SafeNet Luna Backup HSM only.</li> </ul>                                                                                                                                                                                           |
| 17 | <p><b>Enable Korean Algorithms</b></p> <ul style="list-style-type: none"> <li>&gt; <b>Allowed</b>: if you have purchased and applied a license for the Korea-specific algorithm set. See "<a href="#">Upgrading HSM Capabilities and Partition Licenses</a>" on page 401 to purchase this capability.</li> <li>&gt; <b>Disallowed</b> if you have not applied this license.</li> </ul> | N/A                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| 18 | <p><b>FIPS evaluated</b></p> <p>Always <b>disallowed</b> - deprecated capability. All SafeNet Luna Network HSMs are capable of operating in FIPS Mode.</p>                                                                                                                                                                                                                             | N/A                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| 19 | <p><b>Manufacturing Token</b></p> <p>Always <b>disallowed</b>. For Thales Group internal use only.</p>                                                                                                                                                                                                                                                                                 | N/A                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| 21 | <p><b>Enable forcing user PIN change</b></p> <p>Always <b>allowed</b>. This capability forces the Crypto Officer or Crypto User to change the initial role credential created by the Partition SO.</p>                                                                                                                                                                                 | <p><b>Force user PIN change after set/reset</b></p> <ul style="list-style-type: none"> <li>&gt; <b>ON</b> (default): After the Partition SO initializes or resets the Crypto Officer credential, the CO must change the credential before any other actions are permitted. This also applies when the CO initializes/resets the Crypto User role. This policy is intended to enforce the separation of roles on the partition.</li> <li>&gt; <b>OFF</b>: The CO/CU may continue to use the credential assigned by the Partition SO.</li> </ul> <p>See "<a href="#">Changing a Partition Role Credential</a>" on page 437.</p> |
| 22 | <p><b>Enable portable masking key</b></p> <p>Always <b>allowed</b>, but SIM is not supported on this version of SafeNet Luna Network HSM.</p>                                                                                                                                                                                                                                          | <p><b>Allow offboard storage (Destructive)</b></p> <p>Deprecated policy. On previous HSMs, this policy allowed or disallowed the use of the portable SIM key.</p> <p>Default: <b>ON</b></p>                                                                                                                                                                                                                                                                                                                                                                                                                                   |

| #  | HSM Capability                                                                                                                                                                                                                                                                                                                                                                                                                                          | HSM Policy                                                                                                                                                                                                                                                                                                |
|----|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 23 | <p><b>Enable partition groups</b></p> <p>Always <b>disallowed</b> - deprecated capability.</p>                                                                                                                                                                                                                                                                                                                                                          | N/A                                                                                                                                                                                                                                                                                                       |
| 25 | <p><b>Enable Remote PED usage</b></p> <p>Always <b>allowed</b> on PED-authenticated HSMs.</p> <p>Always <b>disallowed</b> on password-authenticated HSMs.</p>                                                                                                                                                                                                                                                                                           | <p><b>Allow Remote PED usage</b></p> <ul style="list-style-type: none"> <li>&gt; <b>ON</b> (default): The HSM may authenticate roles using a remotely-located PED server or a locally-installed PED.</li> <li>&gt; <b>OFF</b>: The HSM must use a locally-installed PED to authenticate roles.</li> </ul> |
| 27 | <p><b>HSM non-volatile storage space</b></p> <p>Displays the maximum non-volatile storage space (in bytes) on the HSM, determined by the SafeNet Luna Network HSM model you selected at time of purchase.</p>                                                                                                                                                                                                                                           | N/A                                                                                                                                                                                                                                                                                                       |
| 30 | <p><b>Enable Unmasking</b></p> <p>Always <b>allowed</b>. This capability enables migration from legacy SafeNet HSMs that used SIM.</p>                                                                                                                                                                                                                                                                                                                  | <p><b>Allow unmasking</b></p> <ul style="list-style-type: none"> <li>&gt; <b>ON</b> (default): Cryptographic objects may be migrated from legacy SafeNet HSMs that used SIM.</li> <li>&gt; <b>OFF</b>: Migration from legacy HSMs using SIM is not possible.</li> </ul>                                   |
| 33 | <p><b>Maximum number of partitions</b></p> <p>Displays the maximum number of application partitions that can be created on the HSM. The default maximum is determined by the SafeNet Luna Network HSM model you selected at time of purchase. On some models, you can upgrade the number of allowable partitions by purchasing additional partition licenses (see "<a href="#">Upgrading HSM Capabilities and Partition Licenses</a>" on page 401).</p> | <p><b>Current maximum number of partitions</b></p> <p>You can change HSM policy 33 to lower the effective maximum number of partitions below the actual licensed maximum. You cannot, however, lower the maximum below the number of partitions currently existing on the HSM.</p>                        |
| 35 | <p><b>Enable Single Domain</b></p> <p>Always <b>disallowed</b>. Not applicable to SafeNet Luna Network HSM.</p>                                                                                                                                                                                                                                                                                                                                         | N/A                                                                                                                                                                                                                                                                                                       |
| 36 | <p><b>Enable Unified PED Key</b></p> <p>Always <b>disallowed</b>. Not applicable to SafeNet Luna Network HSM.</p>                                                                                                                                                                                                                                                                                                                                       | N/A                                                                                                                                                                                                                                                                                                       |

| #  | HSM Capability                                                                                                                                                                                                                                                                                                              | HSM Policy                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|----|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 37 | <p><b>Enable MofN</b></p> <p>Always <b>allowed</b> on PED-authenticated HSMs. Always <b>disallowed</b> on password-authenticated HSMs.</p>                                                                                                                                                                                  | <p><b>Allow MofN</b></p> <ul style="list-style-type: none"> <li>&gt; <b>ON</b> (default): During PED key creation, you have the option to require a quorum to authenticate the role, by splitting the PED secret among multiple PED keys (see "<a href="#">M of N Split Secrets (Quorum)</a>" on page 247)</li> <li>&gt; <b>OFF</b>: Users do not have the option to split PED secrets (M and N are automatically set to 1).</li> </ul>                                                              |
| 38 | <p><b>Enable small form factor backup/restore</b></p> <p>Always <b>disallowed</b>. Not available in this release.</p>                                                                                                                                                                                                       | N/A                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| 39 | <p><b>Enable Secure Trusted Channel</b></p> <p>Always <b>allowed</b>. This capability enables Secure Trusted Channel (STC) to be used for partition-client connections, and/or to encrypt traffic between the HSM and appliance (see "<a href="#">Secure Trusted Channel</a>" on page 125).</p>                             | <p><b>Allow Secure Trusted Channel</b></p> <ul style="list-style-type: none"> <li>&gt; <b>ON</b>: Secure Trusted Channel is enabled for partition-client connections (see "<a href="#">Creating a Client-Partition STC Connection</a>" on page 135). STC can be used to encrypt traffic between the appliance and the HSM (see "<a href="#">Using the STC Admin Channel</a>" on page 145).</li> <li>&gt; <b>OFF</b> (default): All clients must access partitions using NTLS connections.</li> </ul> |
| 40 | <p><b>Enable decommission on tamper</b></p> <p>Always <b>allowed</b>. This enables the HSM to be automatically decommissioned if a tamper event occurs (see "<a href="#">Comparing Zeroize, Decommission, Re-image, and Factory Reset</a>" on page 171).</p>                                                                | <p><b>Decommission on tamper (Destructive)</b></p> <ul style="list-style-type: none"> <li>&gt; <b>ON</b>: The HSM is decommissioned if a tamper event occurs (see "<a href="#">Tamper Events</a>" on page 348).</li> <li>&gt; <b>OFF</b> (default): The contents of the HSM are not affected by a tamper event.</li> </ul>                                                                                                                                                                           |
| 42 | <p><b>Enable partition re-initialize</b></p> <p>Always <b>disallowed</b>. Not applicable to SafeNet Luna Network HSM. This capability and any associated feature and command(s) are applicable only to the Luna IS product, which shares some common code. No such feature has been tested on SafeNet Luna Network HSM.</p> | N/A                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| 43 | <p><b>Enable low level math acceleration</b></p> <p>Always <b>allowed</b>. This capability enables acceleration of cryptographic functionality for maximum HSM performance.</p>                                                                                                                                             | <p><b>Allow low-level math acceleration</b></p> <ul style="list-style-type: none"> <li>&gt; <b>ON</b> (default): Provides maximum HSM performance.</li> <li>&gt; <b>OFF</b>: Do not turn this policy off unless instructed by Thales Group Technical Support.</li> </ul>                                                                                                                                                                                                                             |

| #  | HSM Capability                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     | HSM Policy                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|----|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 45 | <p><b>Enable Fast-Path</b></p> <p>Always <b>disallowed</b>. Not available in this release.</p>                                                                                                                                                                                                                                                                                                                                                                                                                     | N/A                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| 46 | <p><b>Allow Disabling Decommission</b></p> <p>Always <b>allowed</b>. This capability enables the HSM SO to disable the decommission button on the HSM.</p>                                                                                                                                                                                                                                                                                                                                                         | <p><b>Disable Decommission (Destructive)</b></p> <ul style="list-style-type: none"> <li>&gt; <b>ON</b>: The decommission button is disabled, preventing decommissioning of the HSM.</li> <li>&gt; <b>OFF</b> (default): Decommission works as described in <a href="#">"Decommissioning the HSM Appliance" on page 166</a>.</li> </ul> <div style="border: 1px solid orange; padding: 5px; margin-top: 10px;"> <p><b>CAUTION!</b> Changing this policy will destroy partitions on the HSM, and they must be recreated. If HSM policy 40 is enabled, you cannot enable this policy (fails with error: CKR_CONFIG_FAILS_DEPENDENCIES). However, attempting to enable it will still destroy HSM partitions.</p> </div> |
| 47 | <p><b>Enable Tunnel Slot</b></p> <p>Always <b>disallowed</b>. Not available in this release.</p>                                                                                                                                                                                                                                                                                                                                                                                                                   | N/A                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| 48 | <p><b>Enable Controlled Tamper Recovery</b></p> <p>Always <b>allowed</b>. This capability enables the HSM SO to require tamper events to be explicitly cleared before normal operations can resume.</p>                                                                                                                                                                                                                                                                                                            | <p><b>Do Controlled Tamper Recovery</b></p> <ul style="list-style-type: none"> <li>&gt; <b>ON</b> (default): After a tamper event, the HSM SO must explicitly clear the tamper before the HSM can resume normal operations.</li> <li>&gt; <b>OFF</b>: The HSM must be restarted before it can resume normal operations.</li> </ul> <p>See <a href="#">"Tamper Events" on page 348</a> for more information.</p>                                                                                                                                                                                                                                                                                                     |
| 49 | <p><b>Enable Partition Utilization Metrics</b></p> <p>Always <b>allowed</b>. This capability enables the HSM SO to view (or export to a named file) counters that record how many times specific cryptographic operations have been performed in application partitions since the last counter-reset event. This provides a picture of operational utilization that can be used to guide the (re-)allocation and balancing of partitions and applications, for better service to all users of your partitions.</p> | <p><b>Allow Partition Utilization Metrics</b></p> <ul style="list-style-type: none"> <li>&gt; <b>ON</b>: The HSM SO can view Partition Utilization Metrics.</li> <li>&gt; <b>OFF</b> (default): Partition Utilization Metrics are not available.</li> </ul> <p>See <a href="#">"Partition Utilization Metrics" on page 26</a> for more information.</p>                                                                                                                                                                                                                                                                                                                                                             |

| #  | HSM Capability                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  | HSM Policy                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|----|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 50 | <p><b>Enable Functionality Modules</b></p> <p>This capability enables Functionality Modules (FMs) to be loaded to the HSM (see <a href="#">"Functionality Modules" on page 177</a>).</p> <ul style="list-style-type: none"> <li>&gt; <b>Allowed</b> on FM-ready HSMs running firmware 7.4 or higher, with the FM capability license installed (see <a href="#">"Preparing the SafeNet Luna Network HSM to Use FMs" on page 180</a>).</li> <li>&gt; <b>Disallowed</b> on FM-ready HSMs running firmware 7.4 or higher without the FM capability license.</li> </ul> <p>Does not appear on HSMs that are not FM-ready or are running firmware older than 7.4.</p> | <p><b>Allow Functionality Modules (Destructive)</b></p> <ul style="list-style-type: none"> <li>&gt; <b>ON:</b> With this policy enabled, Functionality Modules may be loaded to the HSM, permitting custom cryptographic operations. Allows use of the <b>ctfm</b> utility and FM-related commands, and the use of Functionality Modules in general with this HSM.</li> <li>&gt; <b>OFF</b> (default): FMs may not be loaded to the HSM.</li> </ul> <div style="border: 1px solid orange; padding: 5px; margin-top: 10px;"> <p><b>CAUTION!</b> Enabling FMs (<b>HSM policy 50</b>) introduces changes to Luna HSM functionality, some of which are permanent; they cannot be removed by disabling the policy. Refer to <a href="#">"FM Deployment Constraints" on page 177</a> for details before enabling.</p> <p>If you are using Crypto Command Center, ensure that your CCC version supports FM-enabled HSMs before you enable <b>HSM policy 50</b>. Refer to the CCC CRN for details.</p> </div> |
| 51 | <p><b>Enable SMFS Auto Activation</b></p> <p>This capability enables the Secure Memory File System (SMFS) to be activated automatically on startup.</p> <ul style="list-style-type: none"> <li>&gt; <b>Allowed</b> on FM-ready HSMs running firmware 7.4 or higher, with the FM capability license installed (see <a href="#">"Preparing the SafeNet Luna Network HSM to Use FMs" on page 180</a>).</li> <li>&gt; <b>Disallowed</b> on FM-ready HSMs running firmware 7.4 or higher without the FM capability license.</li> </ul> <p>Does not appear on HSMs that are not FM-ready or are running firmware older than 7.4.</p>                                  | <p><b>Allow SMFS Auto Activation (Destructive)</b></p> <ul style="list-style-type: none"> <li>&gt; <b>ON:</b> With this policy enabled, the Secure Memory File System (SMFS) is automatically activated on startup, providing a secure, tamper-enabled location in the HSM memory where Functionality Modules can load keys and parameters. Auto-activation for SMFS, like auto-activation for PED-authenticated partitions in general, persists through a power outage of up to 2 hours duration.</li> <li>&gt; <b>OFF</b> (default): If disabled, the HSM SO must manually activate the SMFS each time the HSM reboots or loses power.</li> </ul>                                                                                                                                                                                                                                                                                                                                                   |

| #  | HSM Capability                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         | HSM Policy                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|----|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 52 | <p><b>Allow Restricting FM Privilege Level</b></p> <p>This capability enables the HSM SO to restrict the sensitive key attributes of partition objects from FMs.</p> <ul style="list-style-type: none"> <li>&gt; <b>Allowed</b> on FM-ready HSMs running firmware 7.4 or higher, with the FM capability license installed (see <a href="#">"Preparing the SafeNet Luna Network HSM to Use FMs" on page 180</a>).</li> <li>&gt; <b>Disallowed</b> on FM-ready HSMs running firmware 7.4 or higher without the FM capability license.</li> </ul> <p>Does not appear on HSMs that are not FM-ready or are running firmware older than 7.4.</p>            | <p><b>Restrict FM Privilege Level (Destructive)</b></p> <ul style="list-style-type: none"> <li>&gt; <b>ON</b>: FM privilege is restricted.</li> <li>&gt; <b>OFF</b> (default): FM privilege permits FMs to see the sensitive key attributes (including key values) of cryptographic objects on application partitions. This privilege is necessary for most FMs, so that the Crypto Officer (CO) and Crypto User (CU) roles can use partition objects with the FM. However, some FMs might not require this privilege and it can be restricted to satisfy some certification requirements (such as Common Criteria).</li> </ul> |
| 53 | <p><b>Allow Encrypting of Keys from FM to HSM</b></p> <p>This capability enables key encryption between the FM and the Functionality Module Crypto Engine interface (FMCE).</p> <ul style="list-style-type: none"> <li>&gt; <b>Allowed</b> on FM-ready HSMs running firmware 7.4 or higher, with the FM capability license installed (see <a href="#">"Preparing the SafeNet Luna Network HSM to Use FMs" on page 180</a>).</li> <li>&gt; <b>Disallowed</b> on FM-ready HSMs running firmware 7.4 or higher without the FM capability license.</li> </ul> <p>Does not appear on HSMs that are not FM-ready or are running firmware older than 7.4.</p> | <p><b>Encrypt Keys Passing from FM to HSM (Destructive)</b></p> <ul style="list-style-type: none"> <li>&gt; <b>ON</b>: With this policy enabled, keys created by an FM are encrypted before crossing from the FM to the Functionality Module Crypto Engine interface (FMCE). This internal encryption may be required to satisfy some certification requirements (such as Common Criteria).</li> <li>&gt; <b>OFF</b> (default): Keys are not encrypted before crossing to the FMCE.</li> </ul>                                                                                                                                  |

## Setting HSM Policies Manually

The HSM SO can change available policies to customize HSM functionality. Some policies apply to all partitions on the HSM; others enable the Partition SO to customize functionality at the partition level. Refer to ["HSM Capabilities and Policies" on page 95](#) for a complete list of HSM policies and their effects.

In most cases, HSM policies are either enabled (**1**) or disabled (**0**), but some allow a range of values.

To change multiple policy settings during HSM initialization, see ["Setting HSM Policies Using a Template" on the next page](#).

### Prerequisites

- > The HSM must be initialized (see ["HSM Initialization" on page 224](#)).

- > If you are changing a destructive policy and you have partitions existing on the HSM, back up any important cryptographic objects (see ["Backup and Restore Using a G5-Based Backup HSM" on page 53](#) or ["Backup and Restore Using a G7-Based Backup HSM" on page 76](#)).

### To manually set or change an HSM policy

1. Log in to LunaSH as **admin**, or an **admin**-level custom user.
2. [Optional] Display the existing HSM policy settings.  
lunash:> **hsm showpolicies**
3. Log in as HSM SO (see ["Logging In as HSM Security Officer" on page 431](#)).  
lunash:> **hsm login**
4. Change the policy setting by specifying the policy number and the desired value (**0**, **1**, or a number in the accepted range for that policy).  
lunash:> **hsm changepolicy -policy <policy\_ID> -value <value>**

## Setting HSM Policies Using a Template

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

See also ["Setting Partition Policies Using a Template" on page 114](#).

**NOTE** This feature has software and/or firmware dependencies. See ["Version Dependencies by Feature" on page 393](#) for more information.

You can create a policy template file from an initialized or uninitialized HSM, and edit it using a standard text editor.

HSM policy templates cannot be used to alter settings for an initialized HSM. Once an HSM has been initialized, the SO must change individual policy values manually (see ["Setting HSM Policies Manually" on the previous page](#)).

To zeroize the HSM and revert policies to their default values, see ["Resetting to Factory Condition" on page 167](#).

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

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

- > ["Creating an HSM Policy Template" on the next page](#)
- > ["Editing an HSM Policy Template" on the next page](#)
- > ["Applying an HSM Policy Template" on page 106](#)



## Creating an HSM Policy Template

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

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

### To create an HSM policy template

1. Login to LunaSH as **admin**. If you are creating a template from an initialized HSM, you must log in as HSM SO.  
 lunash:> **hsm login**
2. Create the HSM policy template file with an original filename. No file extension is required. If a template file with the same name exists, it is overwritten.  
 lunash:> **hsm showpolicies -exporttemplate <filename>**
3. On a client workstation, use **scp/pscp** to transfer the template file from the source appliance (see [SCP and PSCP](#)).
4. Customize the template file with a standard text editor (see ["Editing an HSM Policy Template" below](#)).

## Editing an HSM Policy Template

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

### HSM Policy Template Example

This example shows the contents of an HSM policy template created using the factory default policy settings. Use a standard text editor to change the policy values (0=OFF, 1=ON, or the desired value 0-255). You cannot edit the destructiveness of HSM policies. See ["HSM Capabilities and Policies" on page 95](#) for more information.

If you export a policy template from an uninitialized HSM, the **Sourced from HSM** header field remains blank. This field is informational and you can still apply the template.

The **Policy Description** field is included in the template for user readability only. Policies are verified by the number in the **Policy ID** field.

```
Policy template FW Version 7.1.0
Field format - Policy ID:Policy Description:Policy Value
Sourced from HSM: myLunaHSM, SN: 66331

6:"Allow masking":0
7:"Allow cloning":1
12:"Allow non-FIPS algorithms":1
15:"SO can reset partition PIN":0
16:"Allow network replication":1
21:"Force user PIN change after set/reset":1
```

```

22:"Allow offboard storage":1
23:"Allow partition groups":0
25:"Allow remote PED usage":0
30:"Allow unmasking":1
33:"Current maximum number of partitions":100
35:"Force Single Domain":0
36:"Allow Unified PED Key":0
37:"Allow MofN":0
38:"Allow small form factor backup/restore":0
39:"Allow Secure Trusted Channel":0
40:"Decommission on tamper":0
42:"Allow partition re-initialize":0
43:"Allow low level math acceleration":0
46:"Disable Decommission":1
47:"Allow Tunnel Slot":0
48:"Do Controlled Tamper Recovery":1

```

### Editing Guidelines and Restrictions

When creating or editing policy templates:

- > You can remove a policy from the template by adding **#** at the beginning of the line or deleting the line entirely. When you apply the template, the HSM will use the default value for that policy.
- > You may not use invalid policy values (outside the acceptable range), or values that conflict with your HSM's capabilities. For example, **HSM capability 6: Enable Masking** is always **Disallowed**, so you cannot set the corresponding HSM policy to **1**. If you attempt to initialize an HSM with a template containing invalid policy values, an error is returned and initialization fails.

### Applying an HSM Policy Template

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

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

1. From a client workstation, use **scp/pscp** to transfer the template file to the **admin** user on the destination appliance (see [SCP and PSCP](#)).
2. Login to LunaSH as **admin** on the destination appliance, and initialize the HSM using the policy template file.

```
lunash:> hsm init -label <label> -applytemplate <filename>
```

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

```
lunash:> hsm showpolicies
```

## Partition Capabilities and Policies

An application partition can be configured to provide a range of different functions. 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" on page 95](#)). 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 113](#)
- > ["Setting HSM Policies Using a Template" on page 104](#)

## 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 SafeNet 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" on page 95</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> |
| 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>                                                   |
| 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>                                                                                                                                                                                                                                                                                                            |

| # | Partition Capability                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               | Partition Policy                                                                                                                                                                                                                                                                                                                                                           |
|---|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 3 | <p><b>Enable private key masking</b></p> <p>Always <b>0</b>. SIM has been deprecated on SafeNet Luna Network HSM.</p>                                                                                                                                                                                                                                                                                                                                                                                                                              | <p><b>Allow private key masking</b></p> <p>Always <b>0</b>.</p>                                                                                                                                                                                                                                                                                                            |
| 4 | <p><b>Enable secret key cloning</b></p> <p>Always <b>1</b>. This capability allows secret keys to be cloned to another SafeNet 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>" on page 95). 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>Always <b>0</b>. SIM has been discontinued on SafeNet Luna Network HSM.</p>                                                                                                                                                                                                                                                                                                                                                                                                                             | <p><b>Allow secret key masking</b></p> <p>Always <b>0</b>.</p>                                                                                                                                                                                                                                                                                                             |

| #  | 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 Group 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>                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| 15 | <p><b>Allow failed challenge responses</b></p> <p>Always <b>1</b>. This capability/policy applies to PED-authenticated SafeNet 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 23 and <a href="#">"Logging In to the Application Partition"</a> on page 435 for more information.</p>                                                                                    |

| #  | Partition Capability                                                                                                                                                                                                                                                                                                                                                                              | Partition Policy                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|----|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 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="#">Logging In to the Application Partition</a>" on page 435).</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.<br/>Default: <b>10</b></p>                                                                                                                                                                                                                                                                                                                                                                                                             |
| 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 23.</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>" on page 348 for more information.</p> |

| #  | Partition Capability                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       | Partition Policy                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|----|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 23 | <p><b>Enable auto-activation</b></p> <p>This capability allows the partition to remain activated for up to two hours if the SafeNet Luna Network HSM loses power. See "<a href="#">Activation and Auto-activation on Multi-factor- (PED-) Authenticated Partitions</a>" on page 23.</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</b> (7 characters).</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</b> (7 characters)</p> |
| 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>                                                                                                                                                                                                      |

| #  | Partition Capability                                                                                                                                                                                                                                                         | Partition Policy                                                                                                                                                                                                                                                                                                                                                                   |
|----|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 29 | <p><b>Enable RSA signing without confirmation</b><br/>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><br/>Always <b>1</b>. While SIM is discontinued on SafeNet Luna Network HSM, this capability allows keys to be migrated from legacy SafeNet HSMs.</p>                                                                                  | <p><b>Allow private key unmasking</b></p> <ul style="list-style-type: none"> <li>&gt; <b>1</b> (default): Private keys can be migrated from legacy SafeNet HSMs that used SIM.</li> <li>&gt; <b>0</b>: Migration of private keys from legacy HSMs using SIM is not possible.</li> </ul>                                                                                            |
| 32 | <p><b>Enable secret key unmasking</b><br/>Always <b>1</b>. While SIM is discontinued on SafeNet Luna Network HSM, this capability allows keys to be migrated from legacy SafeNet HSMs.</p>                                                                                   | <p><b>Allow secret key unmasking</b></p> <ul style="list-style-type: none"> <li>&gt; <b>1</b> (default): Secret keys can be migrated from legacy SafeNet HSMs that used SIM.</li> <li>&gt; <b>0</b>: Migration of secret keys from legacy HSMs using SIM is not possible.</li> </ul>                                                                                               |
| 33 | <p><b>Enable RSA PKCS mechanism</b><br/>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>                                                                                             |



| #  | Partition Capability                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    | Partition Policy                                                                                                                                                                                                                                                                                                                                                                                                       |
|----|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 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; CKM_AES_CBC_PAD</li> <li>&gt; CKM_AES_CBC_PAD_IPSEC</li> <li>&gt; CKM_ARIA_CBC_PAD</li> <li>&gt; CKM_ARIA_L_CBC_PAD</li> <li>&gt; CKM_CAST3_CBC_PAD</li> <li>&gt; CKM_CAST5_CBC_PAD</li> <li>&gt; CKM_DES_CBC_PAD</li> <li>&gt; CKM_DES3_CBC_PAD</li> <li>&gt; CKM_DES3_CBC_PAD_IPSEC</li> <li>&gt; CKM_RC2_CBC_PAD</li> <li>&gt; CKM_RC5_CBC_PAD</li> <li>&gt; CKM_SEED_CBC_PAD</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>: STC is used for all client access to this partition. You must first set up and register the STC identities (see "<a href="#">Creating a Client-Partition STC Connection</a>" on page 135).</li> <li>&gt; <b>0</b> (default): NTLS is used for all client access to this partition.</li> </ul> |
| 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>                                                                           |

## 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 106 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" below](#).

See also ["Configuring the Partition for Cloning or Export of Private Keys" on page 118](#).

### Prerequisites

- > The partition must be initialized (see ["Initializing an Application Partition" on page 21](#)).
- > If you are changing a destructive policy, back up any important cryptographic objects (see ["Backup and Restore Using a G5-Based Backup HSM" on page 53](#) or ["Backup and Restore Using a G7-Based Backup HSM" on page 76](#)).

**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 ["Logging In to the Application Partition" on page 435](#)).  
lunacm:> **role login -name po**
  4. Change the policy setting by specifying the policy number and the desired value (**0**, **1**, or a number in the accepted range for that policy).  
lunacm:> **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 Template" on page 104](#).

**NOTE** This feature has software and/or firmware dependencies. See ["Version Dependencies by Feature" on page 393](#) 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 page 113](#)).

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" below](#)
- > ["Applying a Partition Policy Template" on page 117](#)

## 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

1. 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 106](#) 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
```

## 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 Keys](#)" on page 118 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.

## 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]
```

# CHAPTER 6: Configuring the Partition for Cloning or Export of Private Keys

By default, the SafeNet Luna Network HSM stores all keys in hardware, allowing private keys to be copied only to another SafeNet 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 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 has software and/or firmware dependencies. See ["Version Dependencies by Feature" on page 393](#) for more information.

The Partition SO can set the mode by changing the following policies (see ["Partition Capabilities and Policies" on page 106](#) 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).

The policies can be set at the time of initialization, using a policy template (see ["Setting Partition Policies Using a Template" on page 114](#)) or by following the procedures described below:

- > ["Cloning Mode" below](#)
- > ["Key Export Mode" on the next page](#)
- > ["No Backup Mode" on page 120](#)

**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 SafeNet Luna Backup HSM in the same cloning domain.
- > All keys/objects are replicated within the partition's HA group.
- > Private keys cannot be wrapped off the HSM (cannot be exported to a file encrypted with a wrapping key).

In this mode, private keys are never allowed to exist outside of a trusted SafeNet 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 115).

### 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 115):

```
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 keys cannot be cloned to other partitions nor to a SafeNet 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 116).

### 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 115):

```
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 keys cannot be cloned to other partitions or to a SafeNet Luna Backup HSM. All other objects can still be cloned.
- > Private 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 115](#)):

```
0:"Allow private key cloning":0:1:0
1:"Allow private key wrapping":0:1:0
```

# CHAPTER 7: 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 127](#)
- > ["Creating an NTLS Connection Using a Client Certificate Signed by a Trusted Certificate Authority" on page 131](#)
- > ["Assigning or Revoking NTLS Client Access to a Partition" on page 134](#)
- > ["Creating a Client-Partition STC Connection" on page 135](#)
- > ["Connecting an Initialized STC Partition to Multiple Clients" on page 139](#)
- > ["Converting Initialized NTLS Partitions to STC" on page 143](#)
- > ["Using the STC Admin Channel" on page 145](#)
- > ["Configuring STC Identities and Settings" on page 146](#)
- > ["Restoring Broken NTLS or STC Connections" on page 150](#)

## Comparing NTLS and STC

---

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

- > ["Network Trust Link Service" on the next page](#)
- > ["Secure Trusted Channel" on page 125](#)

| NTLS                                                                                                                                                                                                                                                                                                                                                                                                                                 | STC                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <ul style="list-style-type: none"> <li>&gt; Does not encrypt data between network interface and HSM</li> <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; Encrypts data between network interface and HSM</li> <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 SafeNet 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 SafeNet 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 NTLS architecture consists of:

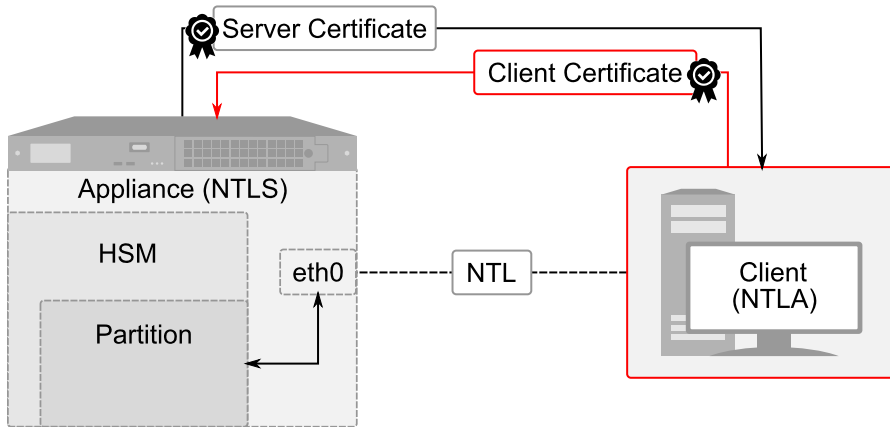
- > Network Trust Link Server (NTLS), which runs on the appliance and manages the NTLS connections to the appliance. NTLS uses port 1792 on the SafeNet Luna Network HSM appliance.
- > Network Trust Link Agent (NTLA), which runs on the client and manages NTLS connections to the client. The NTLA is included in the SafeNet Luna HSM Client software.

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

The certificate that identifies the appliance is always self-signed; the client certificate 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.

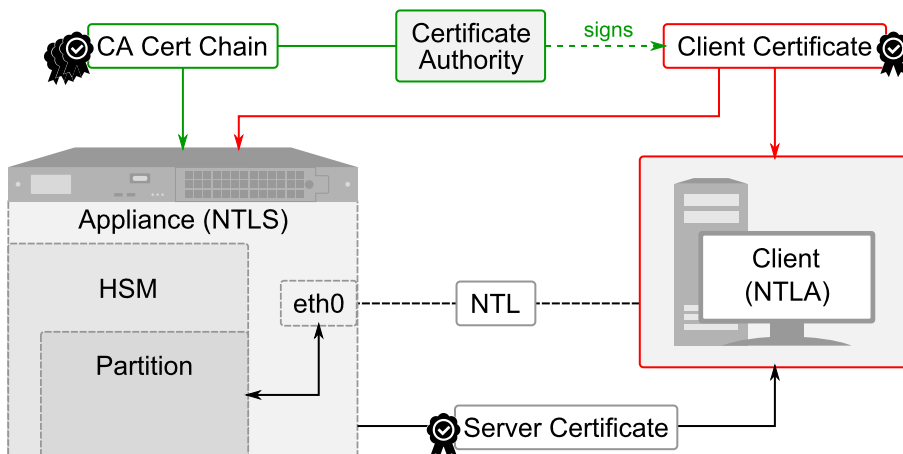
There are two methods of assigning partitions to a client via a self-signed NTL connection:

- > 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](#)" on page 425).

See "[Creating an NTLs Connection Using Self-Signed Certificates](#)" on page 127.

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

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.



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.

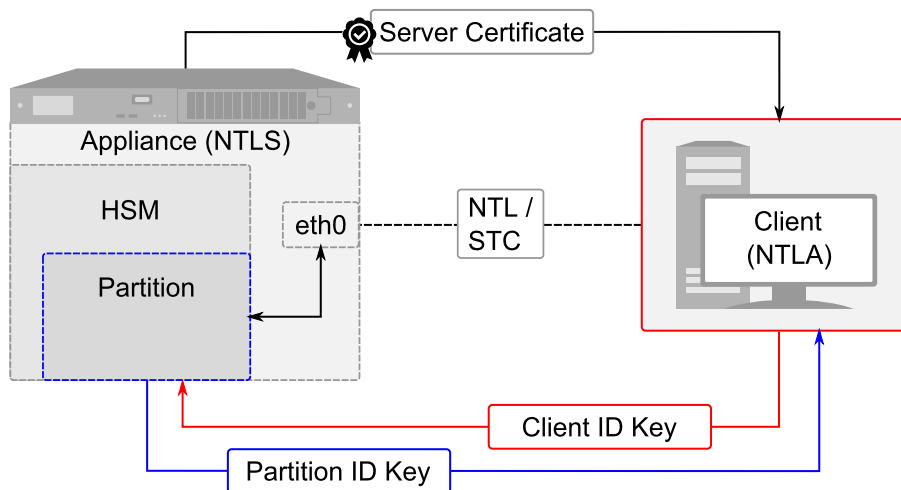
See ["Creating an NTLS Connection Using a Client Certificate Signed by a Trusted Certificate Authority"](#) on page 131.

## 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 a Client-Partition STC Connection"](#) on page 135
- > ["Connecting an Initialized STC Partition to Multiple Clients"](#) on page 139
- > ["Converting Initialized NTLS Partitions to STC"](#) on page 143

## 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 146](#) 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 146](#) 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 SafeNet 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 145](#).

## 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.

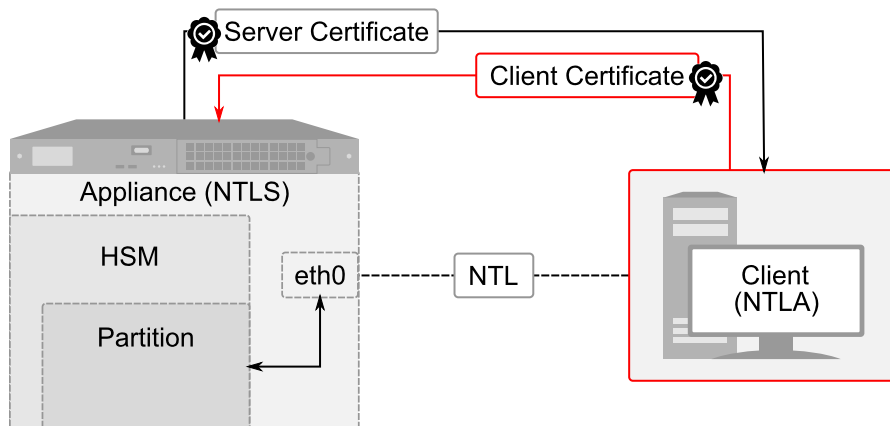
## Creating an NTLS Connection Using Self-Signed Certificates

To create an NTLS connection, the SafeNet 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 Client Certificate Signed by a Trusted Certificate Authority" on page 131](#).

**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 a Client-Partition STC Connection" on page 135](#). For more on the differences between NTLS and STC connections, see ["Comparing NTLS and STC" on page 122](#).

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 130](#): 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](#)" on page 425).
- > 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**.
- > SafeNet Luna HSM Client software must be installed on the client workstation (see [SafeNet Luna HSM Client Software Installation](#) in the *Installation Guide*)
- > The client workstation must have an SSH client installed to provide secure shell access to the SafeNet Luna Network HSM appliance. The PuTTY SSH client (**putty.exe**) is included in the Windows client installation.
- > Read/write access to the SafeNet Luna HSM Client installation directory is required for the certificate exchange.
- > The client workstation must have network access to the SafeNet 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 SafeNet 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** (Windows) or **scp** (Linux/UNIX) to import the HSM Appliance Server Certificate (**server.pem**) from the appliance to the client workstation ([SCP and PSCP](#)). 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.

- Windows: **pscp <user>@<host/IP>:server.pem <target\_filename>**
- Linux/UNIX: **scp <user>@<host/IP>:server.pem <target\_filename>**

**NOTE** When using **scp** or **pscp** 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
```

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 Group 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 SafeNet 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** (Windows) or **scp** (Linux/UNIX) to export the client certificate to the **admin** account (or an **admin**-level custom account) on the Network HSM appliance (**SCP and PSCP**). The file arriving at the appliance is automatically placed in the appropriate directory. Do not specify a target directory.
  - Windows: **pscp** <cert\_path/filename> **admin@<host/IP>:[<target\_filename>]**
  - Linux/UNIX: **scp** <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](#)" on page 421).
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. Restart the NTLS service. After registering a client with a hostname certificate, this ensures that the new client is included.

```
lunash:> service restart ntls
```

9. [Optional] Verify the client registration.

```
lunash:> client list
```

Now that the NTLS connection is established, the SafeNet 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 134).

## One-Step NTLS Connection Procedure

The SafeNet 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 SafeNet 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 **scp/pscp** 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.

### SafeNet 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" on page 17](#)).
- > The client must not have a certificate already registered on the appliance.

### SafeNet Luna HSM Client Prerequisites

- > Client software must be installed (see [SafeNet Luna HSM Client Software Installation](#)).
- > 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" on page 425](#)).
- > 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 127](#) 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.

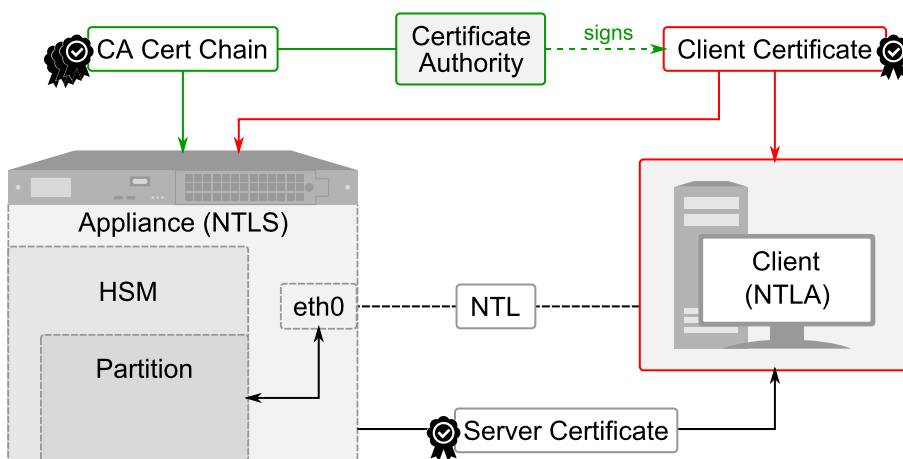
The NTLS connection is now active, and the specified partition has been assigned to the client. If you want this client to have access to more partitions on this HSM, see ["Assigning or Revoking NTLS Client Access to a Partition" on page 134](#).

To initialize the application partition, see ["Initializing an Application Partition" on page 21](#).

## Creating an NTLS Connection Using 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" below](#)
2. ["Authenticating a Client Using a 3rd-Party CA" on the next page](#)
3. ["Registering the Client Certificate and CA Certificate Chain on the Appliance" on page 133](#)



**NOTE** This feature has software and/or firmware dependencies. See ["Version Dependencies by Feature" on page 393](#) 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 (**SCP and PSCP**). 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.

- Windows: **pscp** <user>@<host/IP>:**server.pem** <target\_filename>
- Linux/UNIX: **scp** <user>@<host/IP>:**server.pem** <target\_filename>

**NOTE** When using **scp** or **pscp** 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
```

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 3rd-Party 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 3rd-party CA

1. On the client workstation, open a command prompt and navigate to the SafeNet 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-encoded client certificate
  - The CA's base64-encoded certificate chain, including the root certificate
4. Copy the signed client certificate to the following location in the SafeNet 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 SafeNet Luna Network HSM appliance.
- > You require the signed base64-encoded client certificate and the CA's base64-encoded certificate chain, including the root certificate.

**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 **scp** or **pscp** (see [SCP and PSCP](#)). 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](#)" below).

## 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 122)
- > The HSM SO must create the application partition on the HSM (see "[Creating or Deleting an Application Partition](#)" on page 17)

### 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](#)" on page 421).
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 21).

### 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 421](#)).

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

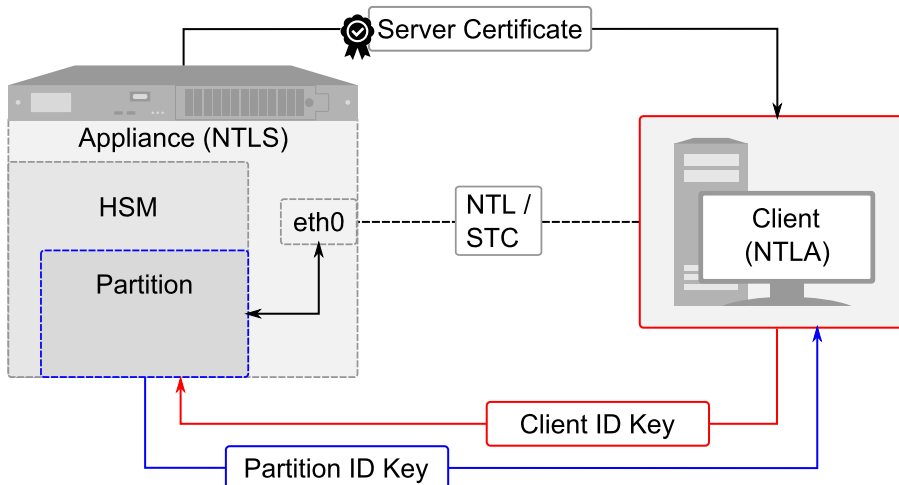
```
lunash:> client show -client <client_name>
```

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

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

## Creating a Client-Partition 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 SafeNet 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 SafeNet 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.

If you plan to use Functionality Modules (FMs) on your HSM, you cannot use STC client connections. Use NTLS connections instead (see ["FM Deployment Constraints" on page 177](#)).

1. ["Preparing the HSM/Partition to Use STC" on the next page](#)
2. ["Preparing the Client to Use STC" on page 137](#)
3. ["Creating a Client-Partition STC Connection" on page 137](#)

## Preparing the HSM/Partition to Use STC

To establish an STC connection between partition and client, you must first enable STC on the HSM, 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, 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 146](#) 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" on page 421](#)).
2. Log in as HSM SO (see ["Logging In as HSM Security Officer" on page 431](#)).

```
lunash:> hsm login
```

3. Enable HSM Policy 39: Allow Secure Trusted Channel.

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

4. Create one or more new partitions for the client (see ["Creating or Deleting an Application Partition" on page 17](#)).

```
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 SafeNet Luna Network HSM file system. The file will be named with the partition's serial number.

```
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](#).

```
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 **scp** or **pscp**, 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 SafeNet 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 SafeNet 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:

```
<Lunaclient_install_directory>/data/client_identities/
```

## Creating a Client-Partition STC Connection

To access STC partitions on the SafeNet 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 SafeNet 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 **scp** or **pscp** to import the HSM Appliance Server Certificate (**server.pem**) from the appliance (**SCP and PSCP**). 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.

- Windows: **pscp admin@<host/IP>:server.pem <target\_filename>**
  - Linux/UNIX: **scp 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 Group 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 **scp** or **pscp** 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 SafeNet 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 SafeNet 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 21](#)). 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](#)).

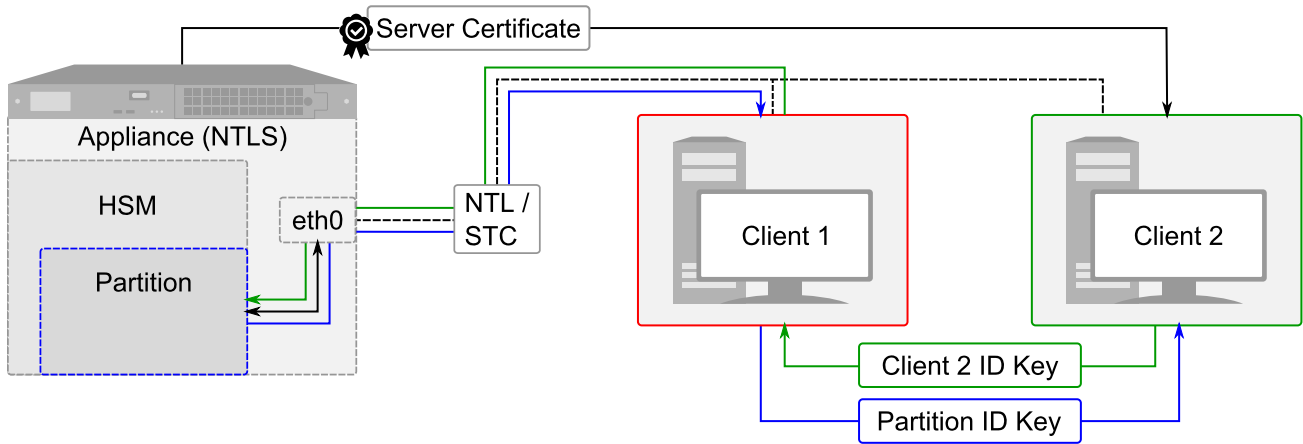
STC provides several configurable options that define the network settings for an STC link, and the security settings for the messages transmitted over the link. Although default values are provided that provide the optimal balance between security and performance, you can override the defaults, if desired. See ["Configuring STC Identities and Settings" on page 146](#) 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, he/she 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 141](#)



## 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 SafeNet 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:  
<Lunaclient\_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 **scp**, **pscp**, or other secure means (see [SCP and PSCP](#)):
  - 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 SafeNet 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 SafeNet 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 **scp** or **pscp** (see [SCP and PSCP](#)).

2. Open a command prompt or terminal window and navigate to the SafeNet 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 SafeNet 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 SafeNet 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>
```

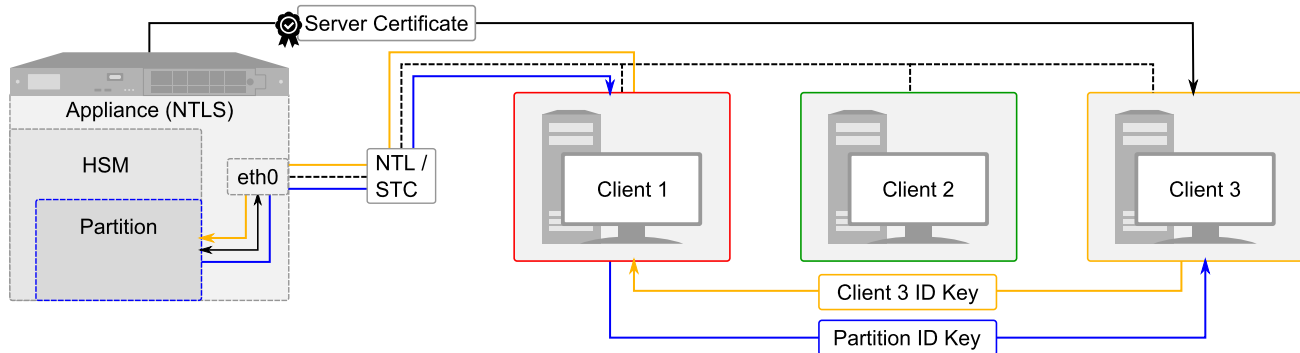
LunaCM restarts. If successful, the partition appears in the list of available slots.

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" on page 18](#)).

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 146](#) 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 SafeNet Luna Network HSM must be converted. It is not possible for a client to connect to multiple partitions on a single SafeNet Luna Network HSM using a combination of NTLS and STC.

The Partition SO must complete this procedure on the client workstation.

### Prerequisites

- > 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:

```
<Lunaclient_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:> stconfig partitionidexport
```

The partition identity public key is named for the partition serial number (<partitionSN>.**pid**) and automatically exported to:

```
<Lunaclient_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:> stconfig clientregister -label <client_label> -file <path/client_identity>
```

5. Enable partition policy 37: Force STM Connection.

```
lunacm:> partition changepolicy -slot <slotnum> -policy 37 -value 1
```

**NOTE** If this command returns an error, ensure that the HSM SO has enabled HSM Policy 39.

6. Repeat steps 2-5 for each NTLS partition on the same SafeNet Luna Network HSM you want to register to this client.
7. Find the server ID for the SafeNet 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 the next page](#) for more information.

## Using the STC Admin Channel

Secure Trusted Channel (STC) can protect all communications to the HSM, including those originating on the SafeNet 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.

Unique STC identities, each defined by a 2048-bit RSA asymmetric public/private key pair, exist on the HSM and the SafeNet 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, 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. SafeNet Luna Network HSM provides configurable options for customizing your STC connections.

- > "[Configuring STC Settings](#)" below
- > "[Configuring STC Tokens and Identities](#)" on page 149

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

- > ["Message Integrity Verification" on the next page](#)
- > ["Rekey Threshold" on the next page](#)

For client-partition STC links, these options are set individually for each partition. 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.

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.

### 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)

```
lunash:> hsm stc activationtimeout show
lunash:> hsm stc activationtimeout set -time <seconds>
```

#### Uninitialized STC Partition (HSM SO)

```
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)

```
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)

```
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)**

```

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)**

```

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 hmaccisable -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 SafeNet 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 identity 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** 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.                            |
| <code>hsm stc identity show</code>                 | 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 or regenerated, those connections must be re-established before crypto operations can resume. This can be the result of HSM or partition zeroization, or regeneration of the HSM server certificate (**server.pem**) on the SafeNet Luna Network HSM appliance. The procedures on this page will allow you to restore your broken connections, wherever possible.

- > ["Restoring NTLS/STC Connections after Regenerating the HSM Server Certificate" 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 HSM Server Certificate

If you regenerate the HSM server certificate (**server.pem**) using `lunash:> sysconf regencert`, you must restore all NTLS and STC connections using the new 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 ntl
```

```
lunash:> service restart stc
```
2. Provide the new HSM Server Certificate (**server.pem**) to each client by **scp**, **pscp**, or other secure means.

##### Client administrators:

1. If you have access to LunaSH on the SafeNet Luna Network HSM appliance, you can retrieve the new HSM server certificate (**server.pem**) using **scp** or **pscp** (see [SCP and PSCP](#)). 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 134](#)). 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 a Client-Partition STC Connection" on page 135](#). 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 **scp**, **pscp**, or other secure means.

**Client administrator:**

1. If you have access to LunaSH on the SafeNet Luna Network HSM appliance, you can retrieve the new partition identity key (<partitionSN>.pem) using **scp** or **pscp** (see [SCP and PSCP](#)). 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.



# CHAPTER 8: Configuration File Summary

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

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

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

If you update the SafeNet 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.

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

**NOTE** Some of the sections/entries listed do not appear in the configuration file by default; you must add these sections/entries to change the behavior described below.  
Some of the entries listed include a default setting that is observed even if the entry is not included in the configuration file by default; you must add the entry to change the default behavior.

| Section/Setting   | Description                                                                                                                                                                                                                                                                                                                   |
|-------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Chrystoki2</b> |                                                                                                                                                                                                                                                                                                                               |
| LibNT             | Path to the Chrystoki2 library on Windows operating systems.<br><b>Default:</b> <code>C:\Program Files\SafeNet\LunaClient\cryptoki.dll</code>                                                                                                                                                                                 |
| LibUNIX64         | Path to the Chrystoki2 library on 64-bit Linux/UNIX operating systems.<br><b>Default:</b> <ul style="list-style-type: none"><li>&gt; <b>Linux/AIX:</b> <code>/usr/safenet/lunaclient/libs/64/libCryptoki2_64.so</code></li><li>&gt; <b>Solaris:</b> <code>/opt/safenet/lunaclient/libs/64/libCryptoki2_64.so</code></li></ul> |
| <b>Luna</b>       |                                                                                                                                                                                                                                                                                                                               |

| Section/Setting       | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|-----------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| CloningCommandTimeout | <p>The amount of time (in milliseconds) the library allows for the HSM to respond to a cloning command.</p> <p><b>Default: 300000</b></p>                                                                                                                                                                                                                                                                                                                                                                                                 |
| CommandTimeoutPedSet  | <p>This is an exception to DefaultTimeout (below). It defines the time (in milliseconds) allowed for all PED-related HSM commands. PED-related commands can take longer than ordinary commands governed by DefaultTimeOut.</p> <p>Generally, the following formula applies:<br/> <math display="block">\text{CommandTimeOutPedSet} = \text{DefaultTimeOut} + \text{PEDTimeout1} + \text{PEDTimeout2} + \text{PEDTimeout3}</math></p> <p><b>Default: 720000</b></p>                                                                        |
| DefaultTimeOut        | <p>Defines the time (in milliseconds) the HSM driver in the host system waits for HSM commands to return a result. If a result is not returned in that time, the driver halts the HSM and returns DEVICE_ERROR to all applications using the HSM. The only exceptions are when a command's timeout is hard-coded in the Cryptoki library, or the command falls into a class governed by one of the other timeout intervals described elsewhere in this section.</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 PEDTimeout2, the HSM returns an appropriate result code (such as PED_TIMEOUT). This is the timeout you might increase from the Default value if you were initializing larger MofN PED Key sets - the HSM allows M and N to each be up to 16 splits - maybe applying PED PINS, and making a duplicate set as well.</p> <p><b>Default: 200000</b></p> |

| Section/Setting   | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|-------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| PEDTimeout3       | <p>Defines the additional time (in milliseconds) the HSM waits for a remote PED to respond to a PED operation request. Therefore, the actual time the firmware waits for a remote PED response is PEDTimeout2 + PEDTimeout3.</p> <p><b>Default: 20000</b></p>                                                                                                                                                                                                                                                   |
| <b>CardReader</b> |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| LunaG5Slots       | <p>Number of SafeNet Luna USB HSM slots reserved so that the library will check for connected devices.</p> <p><b>Valid Values:</b></p> <ul style="list-style-type: none"> <li>&gt; <b>0:</b> If you have no SafeNet Luna USB HSMs and wish to eliminate the reserved spaces in your slot list, use this setting.</li> <li>&gt; <b>1-N:</b> Can be set to any number, but is effectively limited by the number of external USB devices supported by your client workstation.</li> </ul> <p><b>Default: 3</b></p> |
| RemoteCommand     | <p>This setting was used when debugging older SafeNet products. For modern products it is ignored.</p> <p><b>Valid Values:</b></p> <ul style="list-style-type: none"> <li>&gt; <b>0:</b> false</li> <li>&gt; <b>1 (default):</b> true</li> </ul>                                                                                                                                                                                                                                                                |
| <b>RBS</b>        |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| CmdProcessor      | <p>The location of the RBS library.</p> <p><b>Default:</b></p> <ul style="list-style-type: none"> <li>&gt; <b>Windows:</b> C:\Program Files\SafeNet\LunaClient\rbs_processor2.dll</li> <li>&gt; <b>Linux/AIX:</b> /usr/safenet/lunaclient/rbs/lib/librbs_processor2.dll</li> <li>&gt; <b>Solaris:</b> /opt/safenet/lunaclient/rbs/lib/librbs_processor2.dll</li> </ul>                                                                                                                                          |
| HostPort          | <p>The port number used by the RBS server.</p> <p><b>Valid Values:</b> any unassigned port</p> <p><b>Default: 1792</b></p>                                                                                                                                                                                                                                                                                                                                                                                      |
| ClientAuthFile    | <p>The location of the RBS Client authentication file.</p> <p><b>Default:</b></p> <ul style="list-style-type: none"> <li>&gt; <b>Windows:</b> C:\Program Files\SafeNet\LunaClient\config\clientauth.dat</li> <li>&gt; <b>Linux/AIX:</b> /usr/safenet/lunaclient/rbs/clientauth.dat</li> <li>&gt; <b>Solaris:</b> /opt/safenet/lunaclient/rbs/clientauth.dat</li> </ul>                                                                                                                                          |

| Section/Setting      | Description                                                                                                                                                                                                                                                                                                      |
|----------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 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 SafeNet 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                                                                                                                                                                                                                                          |
| SSLConfigFile        | Location of the OpenSSL configuration file.<br><b>Default:</b><br>> <b>Windows:</b> C:\Program Files\SafeNet\LunaClient\openssl.cnf<br>> <b>Linux/AIX:</b> /usr/safenet/lunaclient/bin/openssl.cnf<br>> <b>Solaris:</b> /opt/safenet/lunaclient/bin/openssl.cnf                                                  |

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

| Section/Setting        | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ServerName##           | These entries identify NTLS-linked SafeNet Luna Network HSM servers/ports, and determines the order in which they are polled to create a slot list. These values are set by <code>vti</code> or <code>lunacm:&gt; clientconfig deploy</code> .                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| ServerPort##           |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| <b>Presentation</b>    | <b>NOTE</b> This section is not created automatically. To change any of the following values, you must first create this section in the configuration file.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| OneBaseSlotId          | Determines whether slot listing begins at <b>0</b> or <b>1</b> .<br><b>Default: 0</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| ShowAdminTokens        | Determines whether the Admin partitions of locally-installed SafeNet Luna PCIe HSMs are visible in the slot list.<br><b>Valid Values:</b> <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> <div style="border: 1px solid orange; padding: 5px; margin-top: 10px;"><b>CAUTION!</b> Setting this option to <b>0</b> will also hide the Admin slot on any attached Backup HSMs, making them inaccessible for performing backup operations.</div>                                                                                                                                                                                                                                                                       |
| ShowEmptySlots         | Determines whether slot numbers are reserved for partitions that have not yet been created on the HSM. When this setting is enabled, slot numbers remain consistent over time, even when new partitions are created.<br><b>Valid Values:</b> <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 blue; padding: 5px; margin-top: 10px;"><b>NOTE</b> This does not apply to SafeNet Luna Network HSM partitions assigned to the client, which will always appear in the lowest-numbered slots, causing locally-connected and DPoD slots to increment higher.</div> |
| ShowUserSlots          | Allows you to set permanent slot numbers for specific partitions or HA virtual partitions. If you use this setting, you must specify a slot for all partitions on a specific HSM, or the partitions not listed here will not be visible to the client.<br><b>Valid Values:</b> Comma-delimited list in the format <slotnum>(<serialnum>)<br><b>Example:</b><br><b>ShowUserSlots=1(351970018022),2(351970018021),3(351970018020),...</b>                                                                                                                                                                                                                                                                                                                                                                                   |
| <b>HAConfiguration</b> |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |

| Section/Setting       | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|-----------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| AutoReconnectInterval | <p>Specifies the interval (in seconds) at which the library will attempt to reconnect with a missing HA member, until the set number of attempts is reached. This value is set using lunacm:&gt; <a href="#">hagroup interval</a>.</p> <p><b>Valid Values:</b></p> <ul style="list-style-type: none"> <li>&gt; <b>60-1200:</b> Wait the specified number of seconds between reconnection attempts.</li> </ul> <p><b>Default:</b> 60 seconds</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| HAOnly                | <p>Determines whether individual HA member slots are visible to client applications. Hiding individual members helps prevent synchronization errors by preventing applications from directing calls to individual member partitions. If a member partition fails, the other slots in the system change, which can cause applications to send calls to the wrong slot number. This setting prevents this by hiding all physical slots from applications.</p> <p><b>Valid Values:</b></p> <ul style="list-style-type: none"> <li>&gt; <b>0</b> (default): All partitions are visible to applications as slots.</li> <li>&gt; <b>1:</b> Only HA virtual slots are visible to applications.</li> </ul> <div style="border: 1px solid black; padding: 5px; margin-top: 10px;"> <p><b>NOTE</b> This setting does not affect how slots are numbered in LunaCM; you can still configure individual member partitions with HAOnly mode enabled.</p> </div> |
| reconnAtt             | <p>Specifies the number of reconnection attempts the client makes to a missing HA member. Once this number is reached, you must manually reconnect the member when it becomes available (see "<a href="#">Manually Recovering a Failed HA Group Member</a>" on page 219).</p> <p>This value is set using lunacm:&gt; <a href="#">hagroup retry</a>.</p> <p><b>Valid Values:</b></p> <ul style="list-style-type: none"> <li>&gt; <b>-1:</b> Perform infinite reconnection attempts.</li> <li>&gt; <b>0:</b> Disable HA auto-recovery.</li> <li>&gt; <b>1-500:</b> Perform the specified number of reconnection attempts.</li> </ul>                                                                                                                                                                                                                                                                                                                |
| <b>Misc</b>           |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |

| Section/Setting                        | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|----------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| CopyRSAPublicValuesFromPrivateTemplate | <p>Controls whether the public exponent of an RSA key can be copied from the private key template, if the public key template does not already have a public exponent attribute set.</p> <p><b>Valid Values:</b></p> <ul style="list-style-type: none"> <li>&gt; <b>0</b>: if no public exponent is provided in the public template, an error is returned (expected behavior).</li> <li>&gt; <b>1</b>(default): if no public exponent is provided in the public template, the private exponent is copied from the private template to populate the public template.</li> </ul> <p>For PKCS#11 compliance, this should be set to <b>0</b>.</p>                                               |
| 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>                                                                                                                                                                                                                                                                    |
| LoginAllowedOnFMEabledHSMs             | <p>Determines whether the client can log in to a partition on an HSM that uses Functionality Modules (FMs). FMs consist of custom-designed code that introduces new functionality, which can be more or less secure than standard HSM functions.</p> <p>Possible values include:</p> <ul style="list-style-type: none"> <li>&gt; <b>0</b>: the client does not allow login to an FM-enabled partition</li> <li>&gt; <b>1</b>: the client allows login to an FM-enabled partition</li> </ul> <p>This entry is added to the configuration file the first time you initialize or log in to an FM-enabled partition using LunaCM. You are prompted to confirm that you want to allow login.</p> |
| PE1746Enabled                          | <p>Enables the SafeXcel 1746 security co-processor on Luna 6 HSMs, which is used to offload packet processing and cryptographic computations from the host processor. Does not apply to Luna 7 HSMs or HSM on Demand services. 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 HSM on Demand" on page 238</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>                                          |



| Section/Setting                                | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| PluginModuleDir                                | <p>Specifies the location of client plugins. This setting is required to use the DPoD plugin to access DPoD HSM on Demand services.</p> <p><b>Default:</b></p> <ul style="list-style-type: none"> <li>&gt; <b>Windows:</b> C:\Program Files\SafeNet\LunaClient\plugins</li> <li>&gt; <b>Linux:</b> /usr/safenet/lunaclient/libs/64/plugins</li> </ul>                                                                                                                          |
| ProtectedAuthenticationPathFlagStatus          | <p>Specifies which role to check for challenge request status.</p> <p><b>Valid Values:</b></p> <ul style="list-style-type: none"> <li>&gt; <b>0</b> (default): no challenge request</li> <li>&gt; <b>1:</b> check for Crypto Officer challenge request</li> <li>&gt; <b>2:</b> check for Crypto User challenge request</li> </ul>                                                                                                                                              |
| ToolsDir                                       | <p>The location of the SafeNet Luna HSM Client tools.</p> <p><b>Default:</b></p> <ul style="list-style-type: none"> <li>&gt; <b>Windows:</b> C:\Program Files\SafeNet\LunaClient\</li> <li>&gt; <b>Linux/AIX:</b> /usr/safenet/lunaclient/bin/</li> <li>&gt; <b>Solaris:</b> /opt/safenet/lunaclient/bin/</li> </ul>                                                                                                                                                           |
| <b>Secure Trusted Channel</b>                  |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| 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>                                                                                     |
| 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:</b> C:\Program Files\SafeNet\LunaClient\softtoken.dll</p>                                          |
| PartitionIdentitiesDir                         | <p>Specifies the directory used to store the STC partition identities exported using lunacm:&gt; <a href="#">stconfig partitionidexport</a>.</p> <p><b>Default:</b></p> <ul style="list-style-type: none"> <li>&gt; <b>Windows:</b> C:\Program Files\SafeNet\LunaClient\data\partition_identities</li> <li>&gt; <b>Linux/AIX:</b> /usr/safenet/lunaclient/data/partition_identities</li> <li>&gt; <b>Solaris:</b> /opt/safenet/lunaclient/data/partition_identities</li> </ul> |

| Section/Setting     | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|---------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 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:</b> C:\Program Files\SafeNet\LunaClient\softtoken\001\</li> <li>&gt; <b>Linux/AIX:</b> /usr/safenet/lunaclient/softtoken/001/</li> <li>&gt; <b>Solaris:</b> /opt/safenet/lunaclient/softtoken/001/</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>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| AutoCleanUpDisabled | <p>Determines whether AutoCleanUp closes orphaned sessions in the event that an application leaves sessions open. Useful for SafeNet Luna PCIe HSM hosts. AutoCleanUp runs during C_Finalize on the client. SafeNet Luna Network HSM sessions are tracked and closed by the NTLS service.</p> <p><b>Valid Values:</b></p> <ul style="list-style-type: none"> <li>&gt; <b>0</b> (default): Run AutoCleanUp if your application leaks sessions and you cannot rewrite the application.</li> <li>&gt; <b>1:</b> Disable AutoCleanUp if you have a SafeNet Luna PCIe HSM and your client application does proper housekeeping, or if your application is connecting via NTLS to a SafeNet Luna Network HSM.</li> </ul>                 |
| <b>Toggles</b>      | <p><b>NOTE</b> This section is not created automatically. To change any of the following values, you must first create this section in the configuration file.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| 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> |
| lunacm_cv_ha_ui =   | <p>Controls whether SafeNet Data Protection on Demand's HSM on Demand (HSMoD) services can be active members of an HA group.</p> <p><b>Valid Values:</b></p> <ul style="list-style-type: none"> <li>&gt; <b>0:</b> HSMoD services can be added as active HA members.</li> <li>&gt; <b>1:</b> (default): HSMoD services can be added to HA groups as standby members only. This is the default behavior to maximize HA performance, which may suffer due to network latency.</li> </ul>                                                                                                                                                                                                                                             |

| Section/Setting         | Description                                                                                                                                                                                                                                                                                                                                                       |
|-------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>REST</b>             | <b>NOTE</b> This section is not created automatically. It must be copied from a DPoD HSM on Demand client configuration file (see <a href="#">Adding a DPoD HSM on Demand Service</a> ). This section governs DPoD functionality only and is not related to the Luna REST API.                                                                                    |
| ClientConnectIntervalMs | Interval in milliseconds between client connection attempts.<br><b>Default: 1000</b>                                                                                                                                                                                                                                                                              |
| ClientConnectRetryCount | Maximum connection attempts between the client and an HSMoD 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.<br><b>Default: 32</b>                                                                                                                                                                                                                                                                       |
| ClientTimeoutSec        | Time (in seconds) that the client waits for a response from an HSMoD service. This timeout applies to each retry attempt individually.<br><br><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.<br><br><b>Default: 120</b> |
| CVAppSpecificData       | String containing identifying information about your HSMoD service.                                                                                                                                                                                                                                                                                               |
| RestClient              | Indicates that SafeNet Luna HSM Client and associated tools are acting as REST clients.                                                                                                                                                                                                                                                                           |
| ServerName              | The name of the DPoD server providing HSMoD services.                                                                                                                                                                                                                                                                                                             |
| ServerPort              | The port used for DPoD server traffic.                                                                                                                                                                                                                                                                                                                            |
| SSLClientSideVerifyFile | Location of the DPoD server certificate chain file ( <b>server-certificate.pem</b> ).                                                                                                                                                                                                                                                                             |
| <b>XTC</b>              | <b>NOTE</b> This section is not created automatically. It must be copied from a DPoD HSM on Demand client configuration file (see <a href="#">Adding a DPoD HSM on Demand Service</a> ).                                                                                                                                                                          |
| Enabled                 | Indicates that XTC (Transferable Token Channel) is enabled. This channel must be enabled for the client to communicate with a DPoD service.<br><b>Valid Values:</b><br>> <b>0</b> : XTC is disabled.<br>> <b>1</b> (default): XTC is enabled.                                                                                                                     |

| Section/Setting     | Description                                                                                                                                                                      |
|---------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| PartitionCAPath     | Location of the HSMoD partition origin certificate ( <b>partition-ca-certificate.pem</b> ).                                                                                      |
| PartitionCertPath00 | Location of the HSMoD partition messaging certificate ( <b>partition-certificate.pem</b> ).                                                                                      |
| 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> |

# CHAPTER 9: Decommissioning, Zeroizing, Re-imaging, or Resetting an HSM to Factory Conditions

During the lifetime of a SafeNet Luna HSM, you might have cause to take the HSM out of service, and wish to perform actions to ensure that no trace of your sensitive material remains. Those events might include:

- > Placing the unit into storage, perhaps as a spare
- > Shipping to another location or business unit in your organization
- > Shipping the unit back to Gemalto for repair/re-manufacture
- > Removing the HSM permanently from operational use, for disposal at end-of-life

This chapter describes the available options in the following sections:

- > ["Zeroization" below](#)
- > ["Decommissioning the HSM Appliance" on the next page](#)
- > ["Resetting to Factory Condition" on page 167](#)
- > ["Re-Imaging the Appliance to Factory Baseline" on page 168](#)
- > ["Comparing Zeroize, Decommission, Re-image, and Factory Reset" on page 171](#)
- > ["End of Service and Disposal" on page 172](#)
- > ["Comparison of Destruction/Denial Actions" on page 174](#)
- > ["Effects of Administrative Actions on Functionality Modules" on page 176](#)
- > ["RMA and Shipping Back to Thales Group" on page 176](#)

## Zeroization

---

In the context of HSMs in general, the term "zeroize" means to erase all plaintext keys. Some HSMs keep all keys in plaintext within the HSM boundary. SafeNet Luna HSMs do not.

In the context of SafeNet Luna HSMs, keys at rest (keys or objects that are stored in the HSM) are encrypted. Keys are decrypted into a volatile working memory space inside the HSM only while they are being used. Items in volatile memory disappear when power is removed. The action that we loosely call "zeroizing", or clearing, erases volatile memory as well as destroying the key that encrypts stored objects.

Any temporarily decrypted keys are destroyed, and all customer keys on the HSM are immediately rendered inaccessible and unrecoverable whenever you:

- > perform **hsm factoryreset**
- > make too many bad login attempts on the SO account
- > press the Decommission button on the SafeNet Luna Network HSM back panel

- > set a "destructive" HSM policy
- > perform HSM firmware rollback

The KEK (key encryption key that encrypts all user objects, partition structure, cloning vectors, masking vectors, etc.) is destroyed by a zeroization (erasure) or decommission event. At that point, any objects or identities in the HSM become effectively random blobs of bits that can never be decoded.

**NOTE** The next HSM power-up following a KEK zeroization automatically erases the contents of user storage, which were already an indecipherable blob without the original KEK. That is, any zeroizing event instantly makes encrypted objects unusable, and as soon as power is re-applied, the HSM immediately erases even the encrypted remains before it allows further use of the HSM.

The HSM must now be re-initialized in order to use it again, and initialization overwrites the HSM with new user parameters. Everything is further encrypted with a new KEK unique to that HSM.

Keys not encrypted by the KEK are those that require exemption and are not involved in user identities or user objects:

- > The Master Tamper Key, which enables tamper handling
- > The Remote PED Vector, to allow Remote PED-mediated recovery from tamper or from Secure Transport Mode
- > The hardware origin key that certifies the HSM hardware as having been built by Thales Group

## Decommissioning the HSM Appliance

This section describes how to decommission the appliance to remove all current key material and configurations, so that it can be safely redeployed.

### To decommission the SafeNet Luna Network HSM:

For full decommission (removing the unit from service, clearing the HSM of all your material, clearing the appliance of all identifying information) of a SafeNet Luna Network HSM appliance, and assuming that you can power the appliance and gain admin access, follow these steps in LunaSH, using a serial connection:

1. Rotate all logs:
 

```
lunash:> syslog rotate
```
2. Delete all files in the SCP directory:
 

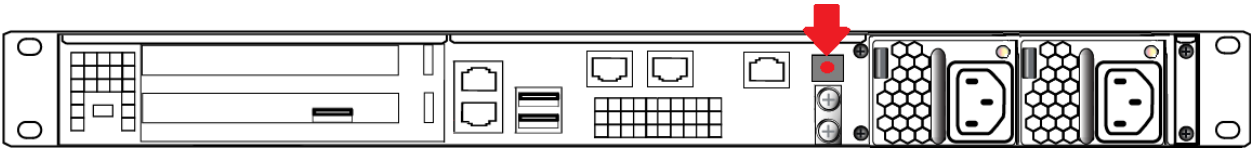
```
lunash:> my file clear
```
3. Delete all logs:
 

```
lunash:> syslog cleanup
```
4. Return the appliance to factory-default settings:
 

```
lunash:> sysconf config factoryreset -service all
```
5. Delete any backups of settings:
 

```
lunash:> sysconf config clear
```

- Push the decommission button (small red button, inset in the SafeNet Luna Network HSM back panel).



- Power down the appliance.
- Power up the appliance. At this point, the HSM internally issues and executes a **zeroize** command to erase all partitions and objects. This step takes about five minutes. The KEK is already gone at that point – erased as soon as the button is pressed – so the step of erasing partitions and objects is for customers subject to especially rigid decommission protocols.

## Disabling Decommissioning

You can disable the decommissioning feature if you have the factory-installed **HSM Capability 46: Allow Disable Decommission** (see ["HSM Capabilities and Policies" on page 95](#)). The primary reason for disabling decommissioning is to prevent the HSM from being automatically decommissioned due to loss of battery (see ["Tamper Events" on page 348](#)). If decommissioning is disabled, the SafeNet Luna Network HSM has an indefinite shelf life, as far as the battery is concerned.

### To disable decommissioning:

Set **HSM Policy 46: Disable Decommission** to 1(ON).

```
lunash:> hsm changehsmpolicy -policy 46 -value 1
```

## Resetting to Factory Condition

These instructions will allow you to restore your SafeNet Luna Network HSM to its original factory configuration. The HSM is zeroized, all partitions erased, and HSM policies are returned to their default settings. If you have performed firmware and appliance software updates, those remain in place, and are not affected by this procedure.

To revert to a baseline appliance software/firmware, see ["Re-Imaging the Appliance to Factory Baseline" on the next page](#).

To roll back the HSM firmware to the previous version, see ["Rolling Back the SafeNet Luna HSM Firmware" on page 400](#).

### Prerequisites

- > Only the HSM SO can perform factory reset.
- > You must access LunaSH via a serial console to execute **hsm factoryreset**.

### To reset the HSM to factory condition

- Login as HSM SO.

```
lunash:> hsm login
```

- Reset the HSM to factory settings.

```
lunash:> hsm factoryreset
```

3. Reset the appliance configuration (network settings, ssh, ntlm, etc.) to factory settings.

```
lunash:> sysconf config factoryreset -service all
```

4. Reboot the appliance.

## Re-Imaging the Appliance to Factory Baseline

The SafeNet Luna Network HSM appliance software update includes two versions: the newest version, and a baseline version that is stored in reserve on the appliance. If you find that the latest software does not suit your organization's purposes, you can re-image the appliance to its factory baseline. This procedure formats the SafeNet Luna Network HSM file system, zeroizes the HSM, erases the appliance configuration, and resets the software/firmware to the baseline version.

This capability is useful if you are re-purposing an HSM for a project that has standardized on an earlier software/firmware configuration, or if you need to format the appliance completely and remove all traces of its prior configuration (to securely return control of the appliance to a cloud provider, for example).

Appliance re-image also allows you to roll back the appliance software, which was not possible in previous Luna releases.

**NOTE** This feature has software and/or firmware dependencies. See "[Version Dependencies by Feature](#)" on page 393 for more information.

The baseline consists of:

- > SafeNet Luna Network HSM appliance software version **7.2**
- > SafeNet Luna Network HSM firmware version **7.0.3**

After you re-image the appliance, you can update to whichever software/firmware version you wish. For valid update paths, refer to the Customer Release Notes for the version you wish to install. Download your preferred software/firmware version from the Thales Group Support Portal (see "[Support Contacts](#)" on page 16).

**CAUTION!** Appliance re-image formats the SafeNet Luna Network HSM appliance file system and zeroizes the HSM. All files and settings on the appliance will be destroyed, including:

- > All roles, partitions, and cryptographic objects on the HSM (except for partition licenses); the HSM must be re-initialized
- > All existing client and remote PED server registrations, as well as the Remote PED Vector (RPV)
- > All appliance roles, including the **admin** role and any custom roles
- > All appliance configuration settings (except for the network configuration)
- > All files stored on the appliance, including upgrade packages and audit logs (see "[my file list](#)" on page 1)

After the appliance re-image procedure, only the following information is preserved:



- > Network configuration; if you are accessing the appliance remotely via SSH connection, you will not permanently lose contact with the appliance
- > Partition licenses purchased via the Thales Group License Portal, unless you included the **-base** option (see ["sysconf reimage start" on page 1](#))

### To re-image the appliance to factory baseline

1. Ensure that you have backed up all important cryptographic objects, appliance files, and appliance logs. Each user of the appliance (**admin**, **operator**, **monitor**, **audit**, and any custom users) must back up any important files by using **scp/pscp** to transfer them off the appliance file system (see ["SCP and PSCP" on page 1](#)). Ensure that application partitions are not being used by any client before proceeding.
2. Ensure that you have previously initialized the Auditor role and configured audit logging on the HSM. By default, audit logs for critical events are stored in the HSM's on-board memory. These logs are only accessible to the Auditor, and therefore cannot be erased by the re-image procedure. If you have never configured audit logging on the HSM, these logs remain in the HSM memory. If you are re-imaging the appliance for another party (or returning control of the appliance to a cloud provider), the next Auditor could access these logs.

To prevent this, configure audit logging on the HSM before re-imaging the appliance (see ["Configuring Audit Logging" on page 38](#)). This procedure will transfer the existing audit logs to the appliance file system, where they can be retrieved and then erased by the re-image process.

If you have not previously configured audit logging, you are prompted with a warning about this when you initiate the re-image process.

3. Ensure that the SafeNet Luna Network HSM is connected to an uninterruptible power supply.

**CAUTION!** Loss of power during the re-image operation may leave the appliance in an unrecoverable state.

4. Log in to LunaSH as **admin**, and then log in to the HSM as HSM SO.

```
lunash:>hsm login
```

5. Re-image the appliance to the baseline version (["sysconf reimage start" on page 1](#)).

```
lunash:>sysconf reimage start
```

**CAUTION!** The operation takes 15-20 minutes, and the appliance reboots twice. Do not manually reboot the appliance, tamper/decommission the HSM, or otherwise interrupt the operation during this time.

```
lunash:>sysconf reimage start
```

```
The HSM Administrator is logged in. Proceeding...
```

```
To remove audit logs from the HSM, you must configure the Audit Logs feature.
```

```
If you do not configure Audit Logs before re-imaging, the existing audit log history will be retained in the HSM.
```

```
Type 'proceed' to continue the re-imaging process without configuring Audit Logs, or 'quit' to cancel.
```

```
> proceed
```

Proceeding...

WARNING: This operation will revert the Luna Network HSM to the baseline of software 7.2.0-220 with firmware 7.0.3 !!!

- (1) This is a destructive operation that erases all partitions and key material.
- (2) Ensure that you have a valid backup of all your partitions.
- (3) After completion, you must re-initialize the HSM.
- (4) After completion, remote PED must be re-connected.
- (5) This operation takes 15-20 minutes. Make sure you have power backup in place.
- (6) Access to the appliance will be unavailable. DO NOT restart the appliance during this time.
- (7) The operation erases all appliance logs.
- (8) The re-imaging operation will generate additional audit logs in the HSM.
- (9) The re-imaging procedure includes multiple appliance reboot.
- (10) This operation CANNOT be undone.

Type 'proceed' to continue, or 'quit' to quit now.

> proceed

Proceeding...

Step 1 of 7: Backing up the appliance support information

...

Done

Step 2 of 7: Setting up the environment for the Appliance Re-image.

...

Done

Step 3 of 7: Extracting the packages

...

This step may take a few minutes... \

Done

Step 4 of 7: Preparing the Luna Network HSM baseline installation scripts

...

Done

Step 5 of 7: Updating to the Luna Network HSM baseline firmware

...

Done

Step 6 of 7: Installing Luna Network HSM Base licenses

...

This step may take a few minutes... \

Done

Step 7 of 7: Factory reset Luna Network HSM

...

The Luna Network HSM with baseline firmware version has been factory reset.

Done

The Luna Network HSM will restart multiple times to complete the baseline installation.

This process could take 15-20 minutes.

Please wait for the operation to complete as interrupting the process could have adverse effects.

During the re-image operation, the following messages appear on the front-panel LCD display to help track the progress:

Re-imaging  
in progress...  
First reboot...

Re-imaging  
in progress...  
Second reboot...

- When the process is complete, log in as **admin** via SSH, using the default password **PASSWORD**, and set up the appliance as if it were new.
- [Optional] The **admin** user can view a summary file of the re-image operation and initial startup (see "[my file list](#)" on page 1). Use **scp/pscp** to transfer the file to a client workstation.

lunash:>**my file list**

lunash:>my file list

```
4134 Jun 19 13:27 firstboot.log
```

Command Result : 0 (Success)

## Troubleshooting

If the re-image operation fails before the appliance reboots, retrieve the re-image log ("[sysconf reimage tarlog](#)" on page 1).

lunash:>**sysconf reimage tarlog**

lunash:>sysconf reimage tarlog

```
'hsm reimage tarlogs' successful
```

Use 'scp' from a client machine to get file named:

```
Baseline_Re_image_logs.20180614_14.40.40.tar.gz
```

Command Result : 0 (Success)

The log file now appears in the **admin** user's files on the appliance (see "[my file list](#)" on page 1). Use **scp/pscp** to transfer it to a client workstation. Thales Group Customer Support may request this log to help assess the issue.

**NOTE** The Appliance Re-image feature is not supported on HSMs that use Functionality Modules. If you have ever enabled **HSM policy 50: Allow Functionality Modules**, even if the policy is currently disabled, you cannot re-image the HSM appliance. See "[FM Deployment Constraints](#)" on page 177 for details.

## Comparing Zeroize, Decommission, Re-image, and Factory Reset

You can clear the contents of your HSM on demand, or the HSM may be cleared in response to an event. How this affects the contents and configuration of your HSM depends on whether the user partitions were deleted or whether the HSM was zeroized, decommissioned, re-imaged, or factory reset as detailed below:

| Action                 | Command/Event                                                                                                                                                                                             | Description                                                                                                                                                                                                                                                                                                                                                                                                  |
|------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Erase User Partitions  | <ul style="list-style-type: none"> <li>&gt; Enable or disable a destructive HSM policy</li> </ul>                                                                                                         | <p>Destroy/erase all user partitions, but do not zeroize the HSM. Policy 46 "Disable Decommission" is the exception in that it zeroizes the HSM and erases all user partitions if the policy is changed. To bring the HSM back into service, you need to:</p> <ol style="list-style-type: none"> <li>1. Recreate the partitions</li> <li>2. Reinitialize the partition roles</li> </ol>                      |
| Zeroize                | <ul style="list-style-type: none"> <li>&gt; Too many bad login attempts on the HSM SO account</li> <li>&gt; Perform an HSM firmware rollback</li> <li>&gt; <code>lunash:&gt;hsm zeroize</code></li> </ul> | <p>Deletes all partitions and their contents, but retains the HSM configuration (audit role and configuration, policy settings). To bring the HSM back into service, you need to:</p> <ol style="list-style-type: none"> <li>1. Reinitialize the HSM</li> <li>2. Recreate the partitions</li> <li>3. Reinitialize the partition roles</li> </ol>                                                             |
| Decommission           | <ul style="list-style-type: none"> <li>&gt; Press the decommission button on the rear of the appliance.</li> <li>&gt; Enable <b>HSM Policy 40: Decommission on Tamper</b>, and tamper the HSM.</li> </ul> | <p>Deletes all partitions and their contents, the audit role, and the audit configuration. Retains the HSM policy settings. To bring the HSM back into service, you need to:</p> <ol style="list-style-type: none"> <li>1. Reinitialize the HSM</li> <li>2. Reinitialize the audit role and reconfigure auditing</li> <li>3. Recreate the partitions</li> <li>4. Reinitialize the partition roles</li> </ol> |
| Re-image the Appliance | <code>lunash:&gt;sysconf reimage start</code>                                                                                                                                                             | <p>Formats the SafeNet Luna Network HSM file system, zeroizes the HSM, erases the appliance configuration, and resets the software/firmware to the baseline version. You will need to reconfigure the appliance and the HSM as if it were new, including setting a password for the <b>admin</b> role.</p>                                                                                                   |
| Factory Reset          | <code>lunash:&gt;hsm factoryreset</code>                                                                                                                                                                  | <p>Deletes all partitions and their contents, and resets all roles and policy configurations to their factory default values. To bring the HSM back into service, you need to completely reconfigure the HSM as though it were new from the factory.</p>                                                                                                                                                     |

## End of Service and Disposal

SafeNet Luna HSMs and appliances are deployed into a wide variety of markets and environments. Arranging for the eventual disposal of a SafeNet Luna HSM or appliance that is no longer needed can be a simple accounting task and a call to your local computer recycling service, or it can be a complex and rigorous set of

procedures intended to protect very sensitive information.

## Needs Can Differ

Some users of SafeNet Luna HSMs employ cryptographic keys and material that have a very short "shelf life". A relatively short time after the HSM is taken out of service, any objects that it contains are no longer relevant. The HSM could be disposed of, with no concern about any material that might remain in it.

The majority of our customers are concerned with their keys and objects that are stored on the HSM. It is important to them that those items never be exposed. The fact is that they are never exposed, but see below for explanations and actions that address the concerns of auditors who might be more accustomed to other ways of safeguarding HSM contents.

## SafeNet Luna HSM Protects Your Keys and Objects

The design philosophy of our SafeNet Luna HSMs ensures that contents are safe from attackers. Unlike other HSM products on the market, SafeNet Luna HSMs never store sensitive objects, like cryptographic keys, unencrypted. Therefore, SafeNet Luna HSMs have no real need - other than perception or "optics" - to perform active erasure of HSM contents, in case of an attack or tamper event.

Instead, the basic state of a SafeNet Luna HSM is that any stored keys and objects are strongly encrypted. They are decrypted only for current use, and only into volatile memory within the HSM.

If power is removed from the HSM, or if the current session closes, the temporarily-decrypted objects instantly evaporate. The encrypted originals remain, but they are unusable by anyone who does not have the correct HSM keys to decrypt them.

### How the HSM encryption keys protect your sensitive objects

In addition to encryption with the user specific access keys or passwords, all objects on the HSM are encrypted by the HSM's global key encryption key (KEK) and the HSM's unique Master Tamper Key (MTK).

If the HSM experiences a Decommission event (pressing of the small red button on back of SafeNet Luna Network HSM, or shorting of the pins of the decommission header on the HSM card, or removal of the battery while main power is not connected to a SafeNet Luna USB HSM) then the KEK is deleted.

If the HSM experiences a tamper event (physical intrusion, environmental excursion), then the MTK is destroyed.

Destruction of either of those keys instantly renders any objects in the HSM unusable by anyone. In the case of a Decommission event, when the HSM is next powered on, it requires initialization, which wipes even the encrypted remains of your former keys and objects.

We recognize that some organizations build their protocols around assumptions that apply to other suppliers' HSMs - where keys are stored unencrypted and must be actively erased in the event of an attack or removal from service. If your policies include that assumption, then you can re-initialize after Decommission - which actively erases the encrypted objects for which no decrypting key existed. For purposes of security, such an action is not required, but it can satisfy pre-existing protocols that presume a weakness not present in SafeNet Luna HSMs.

Our customers are often very high-security establishments that have rigorous protocols for removing a device from service. In such circumstances, it is not sufficient to merely ensure that all material is gone from the HSM. It is also necessary to clear any possible evidence from the appliance that contains the HSM, such as IP configuration and addresses, log files, etc.

If you have any concern that simply pressing the Decommission button and running **sysconf config factoryreset** is not sufficient destruction of potentially-sensitive information, then please refer to ["Decommissioning the HSM Appliance" on page 166](#).

## Comparison of Destruction/Denial Actions

Various operations on the SafeNet Luna Network HSM are intended to make HSM contents unavailable to potential intruders. The effect of those actions are summarized and contrasted in the following table, along with notes on how to recognize and how to recover from each scenario.

**Scenario 1:** MTK is destroyed, HSM is unavailable, but use/access can be recovered after reboot (See Note 1)

**Scenario 2:** KEK is destroyed (Real-Time Clock and NVRAM), HSM contents cannot be recovered without restore from backup See Note 2)

**Scenario 3:** Appliance admin password reset

| Event                                                                                                                                                                                                                                                                           | Scen. 1 | Scen. 2 | Scen. 3 | How to discover<br>(See Note 3)                                                                                                                | How to recover                                                                                   |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------|---------|---------|------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------|
| <ul style="list-style-type: none"> <li>&gt; Three bad SO login attempts</li> <li>&gt; lunash:&gt; <b>hsm zeroize</b></li> <li>&gt; lunash:&gt; <b>hsm factoryreset</b></li> <li>&gt; Any change to a destructive policy</li> <li>&gt; Firmware rollback (See Note 4)</li> </ul> | NO      | YES     | NO      | <ul style="list-style-type: none"> <li>&gt; Log entry</li> <li>&gt; "HSM IS ZEROIZED" in HSM Details (from <b>hsm show</b> command)</li> </ul> | Restore HSM objects from Backup                                                                  |
| Log in to SafeNet Luna Network HSM "recover" account (local serial connection)                                                                                                                                                                                                  | NO      | NO      | YES     | Log entry shows login by "recover"                                                                                                             | Log into appliance as admin, using the reset password "PASSWORD" and change to a secure password |

| Event                                                                                                                                                                                                                                                                                                                                                                                   | Scen. 1 | Scen. 2 | Scen. 3 | How to discover<br>(See Note 3)                                                                                                                                                                                                                                                                                                                                                                                   | How to recover                  |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------|---------|---------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------|
| Hardware tamper <ul style="list-style-type: none"> <li>&gt; Undervoltage or overvoltage during operation</li> <li>&gt; Under-temperature or over-temperature during operation</li> <li>&gt; Chassis interference (such as cover, fans, etc.)</li> </ul> Software (command-initiated) tamper <ul style="list-style-type: none"> <li>&gt; lunash:&gt; <b>hsm stm transport</b></li> </ul> | YES     | NO      | NO      | Parse logs for text like "tamper", "TVK was corrupted", or "Generating new TVK", indicating that a tamper event was logged. Example:<br><pre>RTC: external tamper latched/ MTK: security function was zeroized on previous tamper event and has not been restored yet</pre> Also, keywords in logs like: "HSM internal error", "device error"<br>SafeNet Luna Network HSM appliance front panel flashes error 30. | Reboot<br>[See Note 1]          |
| Decommission <ul style="list-style-type: none"> <li>&gt; Pressing the Decommission button on the back of the appliance</li> </ul>                                                                                                                                                                                                                                                       | NO      | YES     | NO      | Look for log entry like:<br><pre>RTC: tamper 2 signal/Zeroizing HSM after decommission...LOG(INFO): POWER-UP LOG DUMP END</pre>                                                                                                                                                                                                                                                                                   | Restore HSM objects from Backup |

**Note 1:** MTK is an independent layer of encryption on HSM contents, to manage tamper and Secure Transport Mode. A destroyed MTK is recovered on next reboot. If MTK cannot be recovered, only restoring from backup onto a new or re-manufactured HSM can retrieve your keys and HSM data.

**Note 2:** KEK is an HSM-wide encryption layer that encrypts all HSM objects, excluding only MTK, RPK, a wrapping key, and a couple of keys used for legacy support. A destroyed KEK cannot be recovered. If the KEK is destroyed, only restoring from backup can retrieve your keys and HSM data.

**Note 3:** To check the health of a remote HSM, script a frequent login to the HSM host and execution of a subset of HSM commands. If a command fails, check the logs for an indication of the cause.

**Note 4:** These actions all create a situation where **hsm init** is required, or strongly recommended before the HSM is used again.

In addition, another event/action that has a destructive component is HSM initialization. See "[HSM Initialization](#)" on page 224.

## Effects of Administrative Actions on Functionality Modules

| Action                                   | Deletes FMs |
|------------------------------------------|-------------|
| Destructive HSM Policy                   | Yes         |
| Zeroize on 3 bad SO attempts             | No          |
| <b>hsm zeroize</b> command               | No          |
| <b>hsm factoryReset</b> command          | Yes         |
| Decommission                             | Yes         |
| <b>hsm init</b> when already initialized | No          |
| Destructive CUF application              | Yes         |

NOTE: In all the above cases, the Secure Memory File System is re-initialized, destroying all contents.

**NOTE** Ensure that all destructive policies are set before you load FMs into the HSM firmware. Any change of a destructive policy will erase all loaded FMs.

## RMA and Shipping Back to Thales Group

Although rare, it could happen that you need to ship a SafeNet appliance back to Thales Group.

Contact your Thales representative to obtain the Return Material Authorization (RMA) and instructions for packing and shipping.

You might wish (or your security policy might require you) to take maximum precaution with any contents in your HSM before it leaves your possession.

If so, there are two options available to secure the contents of the SafeNet Luna Network HSM before returning it to Thales Group:

- > Decommission the HSM, forcibly clearing all HSM contents (see ["Decommissioning the HSM Appliance" on page 166](#) for instructions).
- > Set Secure Transport Mode on the HSM (see ["Secure Transport Mode" on page 328](#) for instructions) and provide the verification string and random user string to your Thales Group representative by secure means. This will allow Thales Group to know if the HSM is tampered while in transit.



# CHAPTER 10: Functionality Modules

Functionality Modules (FMs) consist of your own custom-developed code, loaded and operating within the logical and physical security of a SafeNet Luna Network HSM as part of the HSM firmware. FMs allow you to customize your SafeNet Luna Network HSM's functionality to suit the needs of your organization. Custom functionality provided by your own FMs can include:

- > new cryptographic algorithms
- > security-sensitive code, isolated from the rest of the HSM environment
- > keys and critical parameters managed by the FM, independent from standard PKCS#11 objects, held in tamper-protected persistent storage

To create FMs, you will need the Functionality Module Software Development Kit (SDK), which is included with the SafeNet Luna HSM Client software. Applications that use FM functions are supported on Windows and Linux.

For detailed information on the FM architecture and how to use FMs with your applications, refer to ["About the FM SDK Programming Guide" on page 1](#).

**NOTE** This feature has software and/or firmware dependencies. See ["Version Dependencies by Feature" on page 393](#) for more information.

This feature has hardware dependencies described in ["Preparing the SafeNet Luna Network HSM to Use FMs" on page 180](#).

This chapter contains the following sections:

- > ["FM Deployment Constraints" below](#)
- > ["Preparing the SafeNet Luna Network HSM to Use FMs" on page 180](#)
- > ["Building and Signing an FM" on page 183](#)
- > ["Loading an FM Into the HSM Firmware" on page 186](#)
- > ["Deleting an FM From the HSM Firmware" on page 187](#)
- > ["Recovering the HSM After FM Failure" on page 188](#)

## FM Deployment Constraints

This section describes important considerations and constraints associated with deploying your Functionality Modules (FMs). Your SafeNet Luna Network HSM must meet all the criteria described in ["Preparing the SafeNet Luna Network HSM to Use FMs" on page 180](#).

Introducing FMs into your SafeNet Luna Network HSM deployment will change the functionality of certain HSM features. Please take the following constraints into consideration before using FMs:

- > ["FMs and High-Availability \(HA\)" on the next page](#)

- > ["FMs and Backup/Restore/Cloning" below](#)
- > ["FMs and Secure Trusted Channel \(STC\)" on the next page](#)
- > ["FMs and Appliance Re-imaging" on the next page](#)
- > ["FMs and HSM Firmware Rollback" on the next page](#)
- > ["FM Configuration and Remote PED" on the next page](#)
- > ["FM-Enabled HSM Cannot be Verified With CMU" on page 180](#)
- > ["Key Attributes" on page 180](#)
- > ["No EDDSA or EC\\_MONTGOMERY Private Keys with C\\_CreateObject" on page 180](#)
- > ["FM Sample Applications Dependent on General Cryptoki Samples" on page 180](#)

**CAUTION!** Enabling FMs (**HSM policy 50**) introduces changes to Luna HSM functionality, some of which are permanent; they cannot be removed by disabling the policy.

If you are using Crypto Command Center, ensure that your CCC version supports FM-enabled HSMs before you enable **HSM policy 50**. Refer to the CCC CRN for details.

## FMs and High-Availability (HA)

FM-specific functions must specify the exact HSM that will handle the operations. Therefore, the SafeNet Luna HSM Client's HA implementation currently cannot accommodate FM functionality. If you want your FM-specific operations to be load-balanced across multiple HSMs, you must program this functionality into your applications yourself.

HA will still work with standard Luna operations.

For HA to function, all HSMs with application partitions in the HA group must have the same algorithms and functionality available. If one member partition does not have a required algorithm available in HSM firmware, cryptographic objects using that algorithm cannot be cloned to that partition, and this will disrupt HA functions.

Therefore, all HSMs containing HA group members must have FMs enabled (as described in ["Preparing the SafeNet Luna Network HSM to Use FMs" on page 180](#)), and they must all have the same FM(s) loaded. HA login requires two FM-enabled HSMs.

For more information about HA, see ["High-Availability Groups" on page 190](#).

## FMs and Backup/Restore/Cloning

It is currently not possible to back up cryptographic material from an FM-enabled SafeNet Luna Network HSM to a SafeNet Luna Backup HSM, or to clone those objects to a partition on a non-FM-enabled Luna HSM. To back up your important keys, you must clone key material to another FM-ready or FM-enabled Luna HSM partition, either manually using `lunacm:> partition clone` or by setting up an HA group.

Similarly, material that has been backed-up from non-FM-enabled HSMs cannot be restored onto an FM-enabled HSM partition.

To back up keys stored in the SMFS, your application must provide all the functions to back up and restore these keys.

## FMs and Secure Trusted Channel (STC)

FMs are not currently compatible with clients that access application partitions via an STC connection. You must use NTLS connections instead.

## FMs and Appliance Re-imaging

The FM-ready configuration required to make FMs work makes it impossible to re-image the appliance to the baseline version. This restriction comes into effect once **HSM policy 50: Enable Functionality Modules** is set to **1**, and it continues to apply even if the policy is set back to **0**. Attempting to re-image the appliance software once **HSM policy 50** has been enabled will return the following:

```
lunash:>sysconf reimage start
```

```
The HSM Administrator is logged in. Proceeding...
```

```
The HSM Functionality Module policy (policy 50) has
previously been enabled.
```

```
Enabling this policy at any time causes the Appliance Re-image feature
to become unavailable.
```

```
ERROR, Not all required pre-conditions to re-image the appliance was satisfied
```

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

## FMs and HSM Firmware Rollback

Enabling **HSM Policy 50** permanently disables the ability to roll back the HSM firmware to a version lower than 7.4.0. Attempting to roll back the firmware once **HSM policy 50** has been enabled will return the following error:

```
ERROR, failed to roll back HSM F/W!!!
```

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

## FM Configuration and Remote PED

Various FM functions require HSM resets (for example, creating a partition or enabling an FM).

If you are configuring FMs while authenticating with Remote PED, the Remote PED connection is broken with each reset. LunaCM continues to show an active Remote PED connection until you restart LunaCM. You must close that apparent connection with `lunash:>hsm ped disconnect` and then open it again with `lunash:>hsm ped connect` before you can resume remote configuration.

This might be required several times during SafeNet Luna Network HSM setup for FMs. To prevent this, enable **HSM Policy 51: Allow SMFS Auto Activation**. If SMFS is not auto-activated, then the SMFS will require further individual PED prompts during the configuration process (SMFS is deactivated upon HSM reset if SMFS auto-activation is off).

**NOTE** Gemalto recommends that first time configuration of FM's be done locally, to minimize the issues mentioned above.

## FM-Enabled HSM Cannot be Verified With CMU

The FM-enabled SafeNet Luna Network HSM does not currently support confirming the HSM's authenticity using **cmu verifyhsm**, as described in ["Confirm the HSM's Authenticity" on page 1](#), or retrieving and confirming a Public Key Confirmation from the HSM using **cmu getpkc** and **cmu verifypkc**.

## Key Attributes

On an HSM with FMs enabled, keys that are derived or generated have the "always-sensitive" and the "never-extractable" attributes set to "false".

## No EDDSA or EC\_MONTGOMERY Private Keys with C\_CreateObject

This release of the SafeNet Luna Network HSM firmware does not allow FMs to use C\_CreateObject to create EDDSA or EC\_MONTGOMERY private keys. Use C\_GenerateKeyPair to create these types of key.

## FM Sample Applications Dependent on General Cryptoki Samples

When you install the FM SDK, the installation script ensures that the general Luna (PKCS) SDK and samples are also installed (first). This satisfies source dependencies for the FM samples. If you later delete or remove the Luna SDK, you might break those dependencies, and the FM samples will not build. You can manually correct this by performing a manual **rpm -i** of the cksample package.

## Space for FMs

Multiple FMs can be loaded into the FM space of the HSM, with a total memory limit of

- > 8 megabytes for FMs and
- > 4 megabytes of SMFS.

Unused FMs can be deleted, to free some memory space.

## Preparing the SafeNet Luna Network HSM to Use FMs

This section provides information on how to prepare your SafeNet Luna Network HSM to accept Functionality Modules (FMs). FMs require a specific factory configuration, the correct firmware version, a license upgrade, and the correct policy settings, as described below:

- > ["Step 1: Ensure You Have FM-Ready Hardware" on the next page](#)
- > ["Step 2: Update to Luna Appliance Software and HSM Firmware 7.4.0 or Higher" on the next page](#)
- > ["Step 3: Purchase and Apply the FM Capability License" on the next page](#)
- > ["Step 4: Apply HSM Policy Settings" on page 182](#)

**CAUTION!** Enabling FMs (**HSM policy 50**) introduces changes to Luna HSM functionality, some of which are permanent; they cannot be removed by disabling the policy. Refer to ["FM Deployment Constraints" on page 177](#) for details before enabling.

If you are using Crypto Command Center, ensure that your CCC version supports FM-enabled HSMs before you enable **HSM policy 50**. Refer to the CCC CRN for details.

## Step 1: Ensure You Have FM-Ready Hardware

The FM feature requires a specific SafeNet Luna Network HSM hardware configuration that must be created by Thales Group at the factory. SafeNet Luna Network HSMs that have this configuration are "FM-ready". If your SafeNet Luna Network HSM is not FM-ready, contact your Thales Group representative or Thales Group Customer Support for further guidance.

### Determining Whether the HSM is FM-Ready

Starting with release 7.4, all SafeNet Luna Network HSMs are FM-ready from the factory. HSMs shipped prior to 7.4 are not. To determine if your HSM is FM-ready, check the Product Part # on the appliance label:

Product Part #:  
908-XXXXXX-003-A  
Product Serial #:  
XXXXXXX



If the last 3-digit section of the Product Part # is **003** or higher, your HSM is FM-ready. If **002** or lower, contact your Thales Group representative or Thales Group Customer Support for guidance on how to obtain FM-ready hardware.

**NOTE Exception:** If your SafeNet Luna Network HSM includes 10GB optical Ethernet ports, your HSM is FM-Ready, even though the Product Part # ends in **001**.

## Step 2: Update to Luna Appliance Software and HSM Firmware 7.4.0 or Higher

To use FMs, you require appliance software 7.4 or higher, and HSM firmware version 7.4.0 or higher. You can download the latest software/firmware packages from the Thales Group Support Portal (see ["Updating the SafeNet Luna Network HSM Appliance Software" on page 397](#) and ["Updating the SafeNet Luna HSM Firmware" on page 398](#)).

When you have completed the upgrade, you can check the output from `lunash:>hsm show` to ensure that the HSM is FM-ready:

```
Functionality Module HW: FM Ready
=====
```

## Step 3: Purchase and Apply the FM Capability License

To use FMs, contact your Thales Group sales representative to purchase the FM capability license. You can validate the license on the Thales Group Licensing Portal (GLP) and install it with LunaSH. Refer to ["Upgrading HSM Capabilities and Partition Licenses" on page 401](#) for the procedure.

When you have activated your license on the HSM, you can use `lunash:>hsm displaylicenses` to check that it is installed:

```
HSM CAPABILITY LICENSES
License ID Description
=====
621000068-000 K7 Base
621010185-003 Key backup via cloning protocol
621000046-002 Maximum 100 partitions
621000134-002 Enable 32 megabytes of object storage
```

```

621000135-002 Enable allow decommissioning
621000021-002 Maximum performance
621000138-001 Controlled tamper recovery
621000154-001 Enable decommission on tamper with policy off
621000074-001 Enable Functionality Modules

```

## Step 4: Apply HSM Policy Settings

Applying the FM capability license allows you to set 4 new HSM policies that affect FMs on the SafeNet Luna Network HSM (see "[HSM Capabilities and Policies](#)" on page 95). Use `lunash:>hsm showpolicies` to list HSM policies.

| Description                         | Value | Code  | Destructive |
|-------------------------------------|-------|-------|-------------|
| =====                               | ===== | ===== | =====       |
| Allow Functionality Modules         | Off   | 50    | Yes         |
| Allow SMFS Auto Activation          | Off   | 51    | Yes         |
| Restrict FM Privilege Level         | Off   | 52    | Yes         |
| Encrypt keys passing from FM to HSM | Off   | 53    | Yes         |

### HSM Policy 50: Allow Functionality Modules

With this policy enabled, Functionality Modules may be loaded to the HSM, permitting custom cryptographic operations. Allows use of the `ctfm` utility and FM-related commands, and the use of Functionality Modules in general with this HSM.

The HSM SO must set HSM policy 50 to 1 (ON) to use FMs on the SafeNet Luna Network HSM. Changing this policy (OFF-to-ON or ON-to-OFF) will zeroize the HSM and it must be re-initialized.

**CAUTION!** Enabling FMs (**HSM policy 50**) introduces changes to Luna HSM functionality, some of which are permanent; they cannot be removed by disabling the policy. Refer to "[FM Deployment Constraints](#)" on page 177 for details before enabling.

If you are using Crypto Command Center, ensure that your CCC version supports FM-enabled HSMs before you enable **HSM policy 50**. Refer to the CCC CRN for details.

### HSM Policy 51: Allow SMFS Auto Activation

With this policy enabled, the Secure Memory File System (SMFS) is automatically activated on startup, providing a secure, tamper-enabled location in the HSM memory where Functionality Modules can load keys and parameters. Auto-activation for SMFS, like auto-activation for PED-authenticated partitions in general, persists through a power outage of up to 2 hours duration. If disabled, the HSM SO must manually activate the SMFS each time the HSM reboots or loses power.

Thales Group recommends setting HSM policy 51 to 1 (ON) to avoid having to manually re-activate the SMFS if you need to reboot the HSM. Changing this policy destroys all existing application partitions.

### HSM Policy 52: Restrict FM Privilege Level

With this policy enabled, FM privilege is restricted. By default, FM privilege permits FMs to see the sensitive key attributes (including key values) of cryptographic objects on application partitions. This privilege is necessary for most FMs, so that the Crypto Officer (CO) and Crypto User (CU) roles can use partition objects with the FM. However, some FMs might not require this privilege and it can be restricted to satisfy some certification requirements (such as Common Criteria).

FM privilege permits FMs to see the sensitive key attributes (including key values) of cryptographic objects on application partitions. This privilege is necessary for most FMs, so that the Crypto Officer (CO) and Crypto User (CU) roles can use partition objects with the FM. However, some FMs might not require this privilege and it can be restricted to satisfy some certification requirements (such as Common Criteria).

Unless you require CC certification, Thales Group does not recommend changing this policy from its default setting (OFF). Changing this policy destroys all existing application partitions.

### HSM Policy 53: Encrypt Keys Passing from FM to HSM

With this policy enabled, keys created by an FM are encrypted before crossing from the FM to the Functionality Module Crypto Engine interface (FMCE). This internal encryption may be required to satisfy some certification requirements (such as Common Criteria).

Unless you require CC certification, Thales Group does not recommend changing this policy from its default setting (OFF). Changing this policy (OFF-to-ON or ON-to-OFF) will destroy all existing application partitions.

## Building and Signing an FM

Once you have written your FM code, you must build the binary and then sign it using a private key on the HSM. A self-signed certificate is used to confirm the authenticity of the FM. This procedure will allow you to install the FM into your HSM firmware. Luna FMs must be built on a Linux system, so you can use the native **make** command. The following example uses the **skeleton** sample FM, included with the Luna FM SDK.

The FM binary must be signed with a private key, and loaded into the HSM firmware with a self-signed certificate from the same keypair to verify its authenticity. You can use **mkfm**, included with the SafeNet Luna HSM Client FM Tools, to sign your FM using a Luna application partition or your own Cryptoki signing station. The procedure below will show you how to use **mkfm**.

### Prerequisites

- > The FM binary must be built on a Linux client. You can use either a Windows or Linux client to perform the signing operation.
- > The FM Tools option in the SafeNet Luna HSM Client software must be installed on the client or signing station.
- > The client must have access to an application partition on the SafeNet Luna Network HSM. The Crypto Officer can create the keypair and certificate required.
- > **mkfm** requires access to a Cryptoki token (such as a Luna application partition) capable of using the CKM\_SHA512\_RSA\_PKCS mechanism.

### To build an FM binary

1. On your Linux client, navigate to the directory containing your FM code (<filename>.c). By default, FM samples provided with the Luna FM SDK are installed in **/usr/safenet/lunafmsdk/samples/**.

```
[user@myLunaClient ~]# cd /usr/safenet/lunafmsdk/samples/skeleton/fm/
[user@myLunaClient fm]# ls
hdr.c makefile skeleton.c
```

2. Use the Linux **make** command to build the FM binary.

```
make
```

The **make** process creates two new sub-directories, **bin-ppc** and **obj-ppc**. Your FM binary is located in **bin-ppc**, named **<filename>.bin**.

```
[user@myLunaClient ~]# cd /usr/safenet/lunafmsdk/samples/skeleton/fm/bin-ppc/
[user@myLunaClient bin-ppc]# ls
skeleton.bin
```

## To create an FM signing certificate on an application partition

1. If this is the first FM you are signing, you must first create a keypair and self-signed certificate on the application partition. If you already have a certificate for FM signing stored on the appliance, skip this procedure.

To sign an FM with **mkfm**, you must use an RSA private key at least 2048 bits long. The Crypto Officer can use the **cmu** utility to create the keypair. You will be prompted for the CO credential.

**NOTE** Always provide unique labels for your keys. If multiple private keys exist with the same label, **mkfm** will use the newest key (with the greatest object handle value).

**"cmu generatekeypair" on page 1 -labelpublic=<public\_key\_label> -labelprivate=<private\_key\_label> -keytype=rsa -sign=1 -verify=1**

```
[user@myLunaClient bin]# ./cmu generatekeypair -labelpublic=FMpub -labelprivate=FMpriv -
keytype=rsa -sign=1 -verify=1
Certificate Management Utility (64-bit) v7.4.0-208. Copyright (c) 2018 SafeNet. All rights
reserved.
```

```
Select token
[3] Token Label: myPartition
[4] Token Label: myPCIeHSM
Enter choice: 3
Please enter password for token in slot 3 : *****
```

```
Select RSA Mechanism Type -
[1] PKCS [2] FIPS 186-3 Only Primes [3] FIPS 186-3 Auxiliary Primes : 2
Enter modulus length (8 bit multiple) : 2048
```

2. Check the contents of the partition to find the key handles.

### cmu list

```
[user@myLunaClient bin]# ./cmu list
Certificate Management Utility (64-bit) v7.4.0-208. Copyright (c) 2018 SafeNet. All rights
reserved.
```

```
Select token
[3] Token Label: myPartition
[4] Token Label: pcie7pwd45
Enter choice: 3
Please enter password for token in slot 3 : *****
```

```
handle=48 label=FMpriv
handle=45 label=FMpub
```



3. Create a self-signed certificate on the partition by specifying a label, the public and private key handles, and any other attributes you wish to assign. You are prompted for required attributes (Common Name, serial number, start/end dates) that you do not specify.

**cmu selfsigncertificate** **-slot** <slot\_number> **-label** <cert\_label> **-publichandle=**<handle> **-privatehandle=**<handle>

```
[user@myLunaClient bin]# ./cmu selfsigncertificate -slot 3 -publichandle=45 -privatehandle=48 -label FMsign
Certificate Management Utility (64-bit) v7.4.0-208. Copyright (c) 2018 SafeNet. All rights reserved.
```

Please enter password for token in slot 3 : \*\*\*\*\*

```
Enter certificate serial number : 1
Enter Subject 2-letter Country Code (C) : CA
Enter Subject State or Province Name (S) : ON
Enter Subject Locality Name (L) : Ottawa
Enter Subject Organization Name (O) : Gemalto
Enter Subject Organization Unit Name (OU) :
Enter Subject Common Name (CN) : FMsign
Enter EMAIL Address (E) :
Enter validity start date
 Year : 2018
 Month : 12
 Day : 05
Enter validity end date
 Year : 2019
 Month : 12
 Day : 31
Using "CKM_SHA256_RSA_PKCS" Mechanism
```

4. Export the certificate to the client file system, specifying the desired filename with **.cert** extension.

**cmu export** **-slot** <slot\_number> **-label** <cert\_label> **-outputfile=**<filename.cert>

```
[user@myLunaClient bin]# ./cmu export -slot 3 -label FMsign -outputfile=FMsign.cert
Certificate Management Utility (64-bit) v7.4.0-208. Copyright (c) 2018 SafeNet. All rights reserved.
```

Please enter password for token in slot 3 : \*\*\*\*\*

## To sign an FM

1. Use the **mkfm** utility included with the SafeNet Luna HSM Client FM Tools to sign the FM, specifying the unsigned FM binary, the desired FM filepath/filename (with **.fm** extension), the slot number/name of the partition/token where the keypair is stored, and the private key label.

If you are specifying a slot number, include **-k SLOTID=<#>** instead of the partition name. If you are using a Cryptoki signing station other than a Luna 7.x application partition, include the **-c** option. You are prompted for the partition/token credential. By default, the Crypto Officer role is used; to use the Crypto User role instead, include the **-u** option.

**mkfm** **-f** <filepath/name>.bin **-o** <filepath/name>.fm **-k** <token\_or\_partition\_name/<private\_key\_label> [**-c**] [**-u**]

```
[root@k7tower bin-ppc]# ./mkfm -f /usr/safenet/lunafmsdk/samples/skeleton/fm/bin-ppc/skeleton.bin -o /usr/safenet/lunafmsdk/samples/skeleton/fm/bin-ppc/skeleton.fm -k myLunaPartition/FMpriv
```

Luna Functionality Module Signer Utility (64-bit) v7.4.0-208. Copyright (c) 2018 SafeNet. All rights reserved.

Please Enter the PIN: (for user 'co' on slot 3) \*\*\*\*\*

mkfm: Processing ELF file /usr/safenet/lunafmsdk/samples/skeleton/fm/bin-ppc/skeleton.bin

File successfully signed

The signed FM is now located in the directory you specified:

```
[user@myLunaClient ~]# cd /usr/safenet/lunafmsdk/samples/skeleton/fm/bin-ppc/
[user@myLunaClient bin-ppc]# ls
skeleton.bin skeleton.fm
```

Next, see ["Loading an FM Into the HSM Firmware" below](#).

## Loading an FM Into the HSM Firmware

A signed FM must be loaded into the HSM firmware to provide new functionality. The HSM SO can load FMs using LunaSH and the following procedure.

### Prerequisites

- > Your HSM must meet the criteria described in ["Preparing the SafeNet Luna Network HSM to Use FMs" on page 180](#).
- > **HSM policy 50: Allow Functionality Modules** must be enabled.
- > **HSM policy 51: Enable SMFS Auto Activation** must be enabled, if you intend to use auto-activation (recommended). Changing this policy later will erase all partitions and installed FMs.
- > Ensure that all destructive policies are set before you load FMs into the HSM firmware. Any change of a destructive policy will erase all loaded FMs.
- > The FM must be signed as described in ["Building and Signing an FM" on page 183](#), using the SafeNet Luna HSM Client 7.4 or higher. FMs built using the Luna 7.0.4 Tech Preview release are not compatible with this Luna version.
- > You require the FM signing certificate. If you have previously loaded an FM signed by the same key, the correct certificate is already present in the appliance **admin** files.

**NOTE** If you load an FM with the same FM ID as an already-loaded FM, it is considered an update, and replaces the existing FM.

### To load an FM into the HSM firmware

1. Use **scp** (Linux) or **pscp** (Windows) to transfer the signed FM to the appliance **admin** account (["SCP and PSCP" on page 1](#)).
  - Linux/UNIX: **scp** <signed\_FM> **admin@**<host/IP>:
  - Windows: **pscp** <signed\_FM> **admin@**<host/IP>:
2. Transfer the signing certificate to the appliance **admin** account (["SCP and PSCP" on page 1](#)). If you have previously loaded an FM signed by the same key, it should already be in the appliance **admin** files.

3. Connect to the appliance via SSH or a serial connection, and log in to LunaSH as **admin**.
4. Log in as HSM SO.  
lunash:> **hsm login**
5. [Optional] Confirm that the signed FM and the correct certificate are present in the **admin** files.  
lunash:> **my file list**
6. Load the FM to the HSM by specifying the FM and signing certificate files.  
lunash:> **hsm fm load -certFile <cert\_file> -fmFile <FM\_file>**
7. Restart the HSM. It is not necessary to reboot the appliance.  
lunash:> **hsm restart**

**NOTE** If you have FMs loaded, you must restart the HSM whenever you perform any of the following operations:

- > create a new partition and assign it to a client (even if it has the same slot number as a recently-deleted partition),
- > make a destructive change like re-initializing or zeroizing the HSM, or changing a destructive policy.

You will be unable to use the loaded FMs with new partitions until you restart the HSM. Use lunash:> **hsm restart**.

8. Log back in as HSM SO.  
lunash:> **hsm login**
9. Activate the Secure Memory File System.  
lunash:> **hsm fm smfs activate**
10. [Optional] Confirm that the FM was loaded and is now enabled.  
lunash:> **hsm fm status**

## Deleting an FM From the HSM Firmware

This procedure allows the HSM SO to delete a specified FM from the HSM firmware using LunaSH.

**NOTE** If you are replacing the currently-loaded FM with an updated version, you do not need to delete the old version. If the new version has the same FM ID, it will replace the original version in the HSM firmware (see "[Loading an FM Into the HSM Firmware](#)" on the [previous page](#)).

In addition to the procedure below, other actions can cause FMs to be deleted from the HSM and the SMFS to be erased. See "[Effects of Administrative Actions on Functionality Modules](#)" on page 176.

### Prerequisites

- > You require the FM ID of the FM you wish to delete.

## To delete an FM from the HSM firmware

1. [Optional] List the FMs currently loaded on the HSM to obtain the desired FM ID.

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

2. Log in as HSM SO.

```
lunash:> hsm login
```

3. Delete the FM by specifying its FM ID.

```
lunash:> hsm fm delete -id <FM_ID>
```

4. [Optional] Check the FM status again. The deleted FM's status is listed as "Zombie". At this point the FM is disabled, and its data will be fully deleted the next time you restart the HSM.

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

```
Getting status of the FM on all available devices
```

```
Current Functionality Module Configuration for device 0:
```

```
Serial # : 66331
```

```
Model : Luna K7
```

```
SMFS : Activated
```

```
FM Label : skeleton
```

```
FM ID : a000
```

```
Version : 1.01
```

```
Manufacturer : Safenet Inc.
```

```
Build Time : Wed Dec 5 14:44:47 2018 - EST
```

```
Fingerprint : 78 7C E3 C2 01 54 B3 99 08 59
```

```
ROM size : 7302
```

```
Status : Zombie (reboot HSM to cleanup)
```

```
Startup Status: OK
```

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

5. Restart the HSM. It is not necessary to reboot the appliance.

```
lunash:> hsm restart
```

## Recovering the HSM After FM Failure

In the event that an FM bug causes problems on the HSM, such as halting the HSM or other functionality issues, the HSM SO can take steps to recover the HSM. If you have important FM key objects stored in the Secure Memory File System (SMFS), you may be able to regain access to them. If you encounter issues with FM functionality, try the following before you proceed with recovery operations:

1. Debug your FM code. Build and sign the FM ("[Building and Signing an FM](#)" on page 183), and attempt to load it onto the HSM ("[Loading an FM Into the HSM Firmware](#)" on page 186). Loading an updated FM with the same FM ID will erase the old version and replace it.
2. If this does not fix the problem, or you are unable to load the patched FM, delete the old FM first ("[Deleting an FM From the HSM Firmware](#)" on the previous page).
3. If this does not work, continue to the recovery procedure below.

LunaSH includes the **hsm fm recover** command, which allows you to delete all FMs currently loaded on the HSM, erase the SMFS, or both. This provides a last resort for recovering HSM functionality when an FM causes a failure.

### Prerequisites

- > Try the methods above before continuing. If you are running multiple FMs, it may be simpler to delete and replace the one that is causing the issue.

### To recover the HSM after FM failure

1. Log in as HSM SO.

```
lunash:> hsm login
```

2. Erase all FMs currently loaded on the HSM. This will leave the SMFS intact and preserve any key material you may have stored there.

```
lunash:> hsm fm recover -erase fm
```

You may now attempt to load a patched version of your FM that addresses the cause of the issue. If this does not resolve the problem, continue to step 3.

3. Choose one of the following options:

**CAUTION!** Both of these options will erase the SMFS and any cryptographic objects you have stored there. If this is important key material, erasing the SMFS is a last resort to restore HSM functions.

- a. Erase the SMFS.

```
lunash:> hsm fm recover -erase smfs
```

- b. Erase both the loaded FMs and the SMFS

```
lunash:> hsm fm recover -erase both
```

4. Load your patched FM and restart the SMFS (see "[Loading an FM Into the HSM Firmware](#)" on page 186).

# CHAPTER 11: High-Availability Groups

SafeNet Luna HSMs can provide scalability and redundancy for cryptographic applications that are critical to your organization. For applications that require continuous, uninterrupted uptime, the SafeNet Luna HSM Client allows you to combine application partitions on multiple HSMs into a single logical group, known as a High-Availability (HA) group.

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 SafeNet 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 199](#)
- > ["Setting Up an HA Group" on page 203](#)
- > ["Verifying an HA Group" on page 207](#)
- > ["Setting an HA Group Member to Standby" on page 209](#)
- > ["Configuring HA Auto-Recovery" on page 211](#)
- > ["Enabling/Disabling HA Only Mode" on page 211](#)
- > ["HA Logging" on page 212](#)
- > ["Adding/Removing an HA Group Member" on page 216](#)
- > ["Replacing an HA Group Member" on page 220](#)
- > ["Deleting an HA Group" on page 222](#)
- > ["HA Troubleshooting" on page 223](#)

If you plan to create an HA group consisting of different kinds of SafeNet HSMs, refer also to:

- > ["Cloning Keys Between Luna 6, Luna 7, and HSM on Demand" on page 238](#)

## 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 197](#)).

## 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 199](#)). 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 196](#)).

### 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.

All key replication 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.

The cloning protocol is invoked separately for each object to be cloned 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). This ensures that the use of cloning function calls is controlled, and the protocol cannot be misused to permit the unauthorized transfer of objects to or from one of the partitions in the HA group.

## 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 SafeNet 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](#) in the *LunaCM Command Reference Guide*) 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 191](#) 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 23](#)). 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, SafeNet 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 211](#)). Thales Group 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 219](#)).

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 220](#)).

## 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 using an HA group (see ["Planning Your HA Group Deployment" on page 199](#)).

## Mixed-Version HA Groups

Generally, Thales Group 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 HSM on Demand services from SafeNet 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 SafeNet 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 G5-Based Backup HSM](#)" on page 53).

### 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 190](#). 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 201](#)
  - ["Automatic Remote Backup" on page 202](#)
  - ["HA Group Sharing" on page 202](#)

If you plan to create an HA group consisting of different kinds of SafeNet HSMs, refer also to:

- > ["Cloning Keys Between Luna 6, Luna 7, and HSM on Demand" on page 238](#)

### 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 Group 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 HSM on Demand services are supported. See ["Cloning Keys Between Luna 6, Luna 7, and HSM on Demand" on page 238](#) 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" on page 177](#) for details.

## 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.

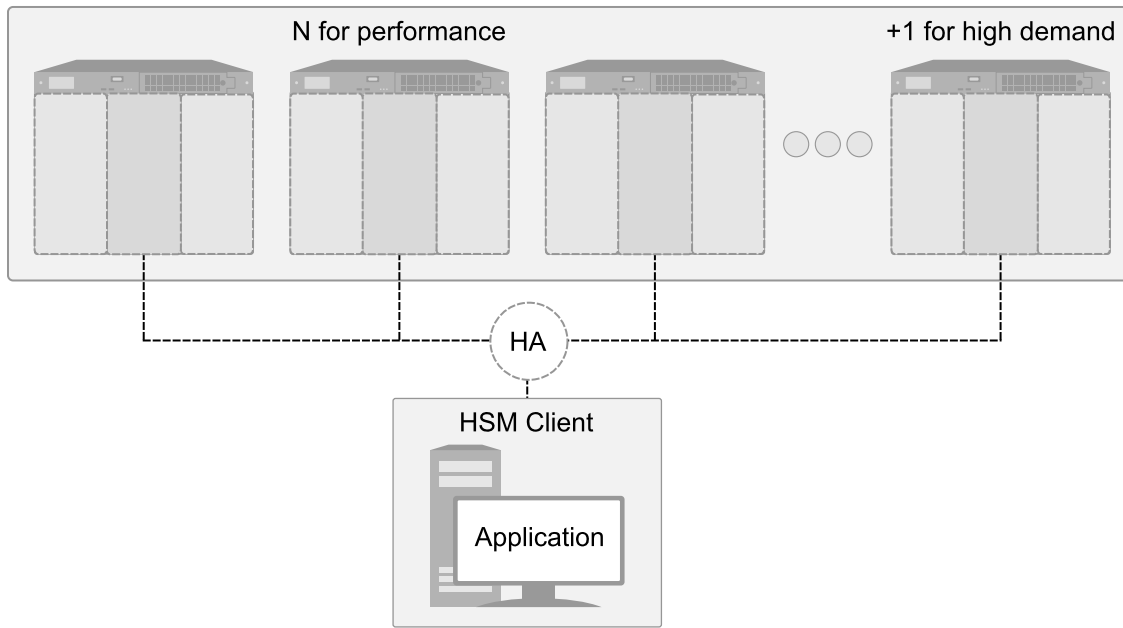
### Performance and Load Balancing

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.

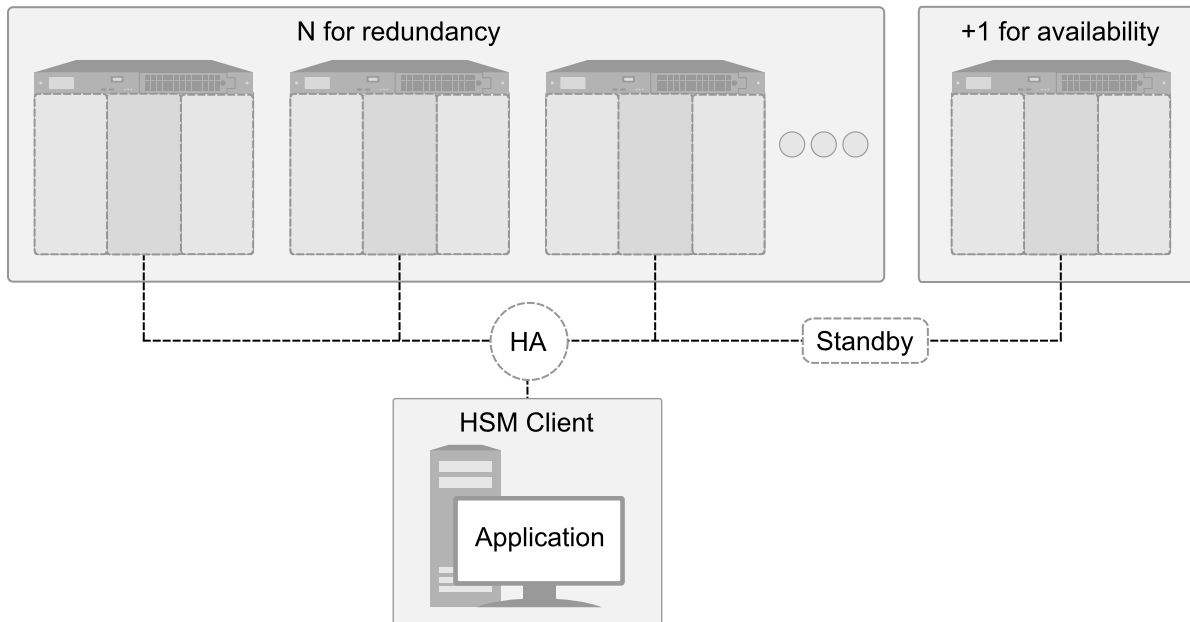
The SafeNet Luna HSM Client allows HA groups with up to 32 member partitions. The best approach in this example is to add enough group members to handle the usual number of operations, plus enough extra members to handle periods of high demand.





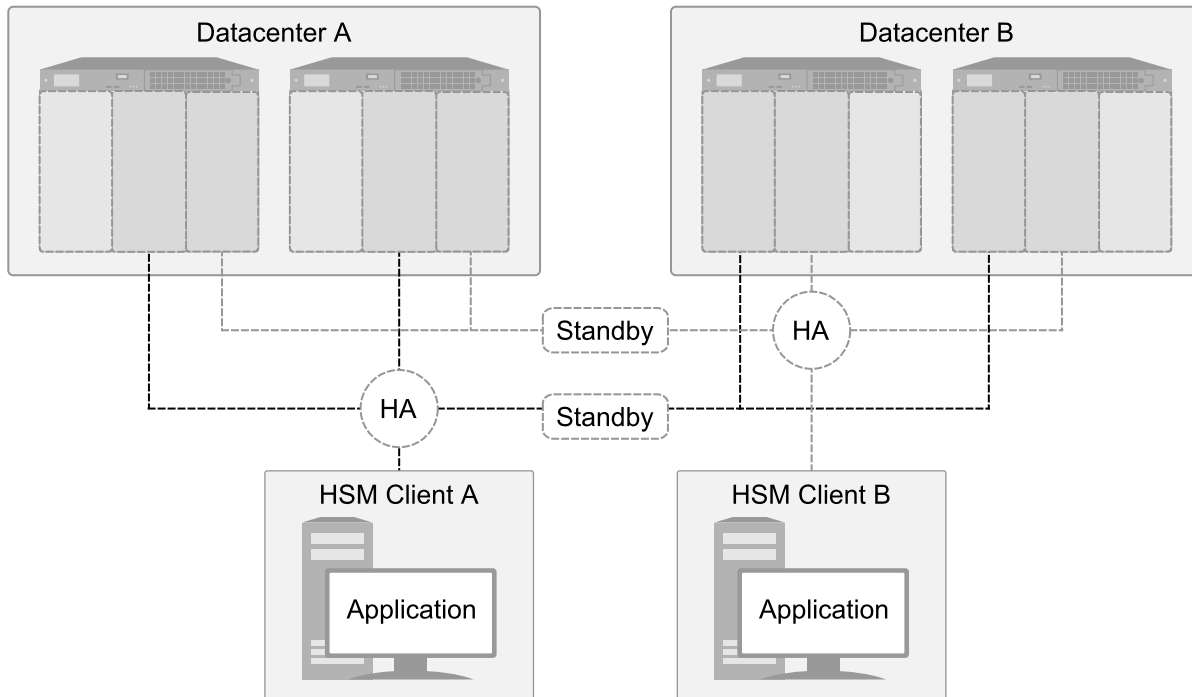
### Redundancy and Failover

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 193](#) for details). Additional group members can be added and set to standby mode for an extra layer of redundancy (see ["Standby Members" on page 196](#) for details).



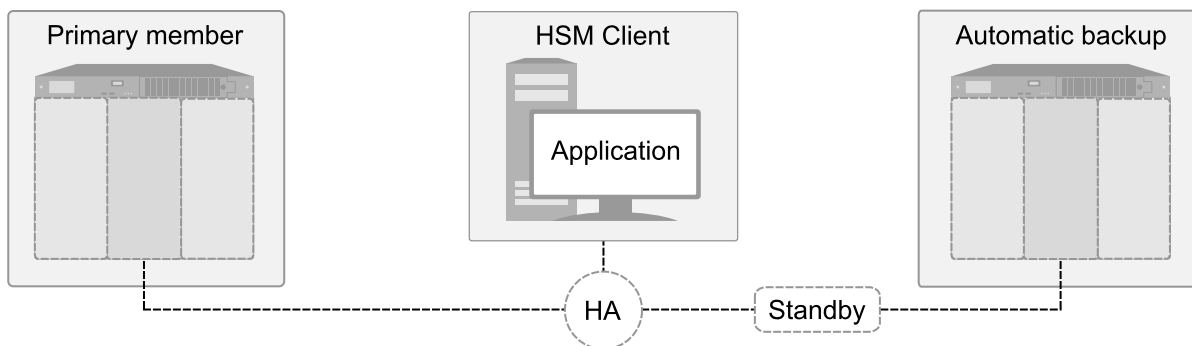
To maximize the use of your HSMs, plan which member partitions you will set to standby mode. Although the configuration above is a straightforward example of an HA group with a single standby member, it is not an ideal production configuration, because the standby member is idle unless all the other 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

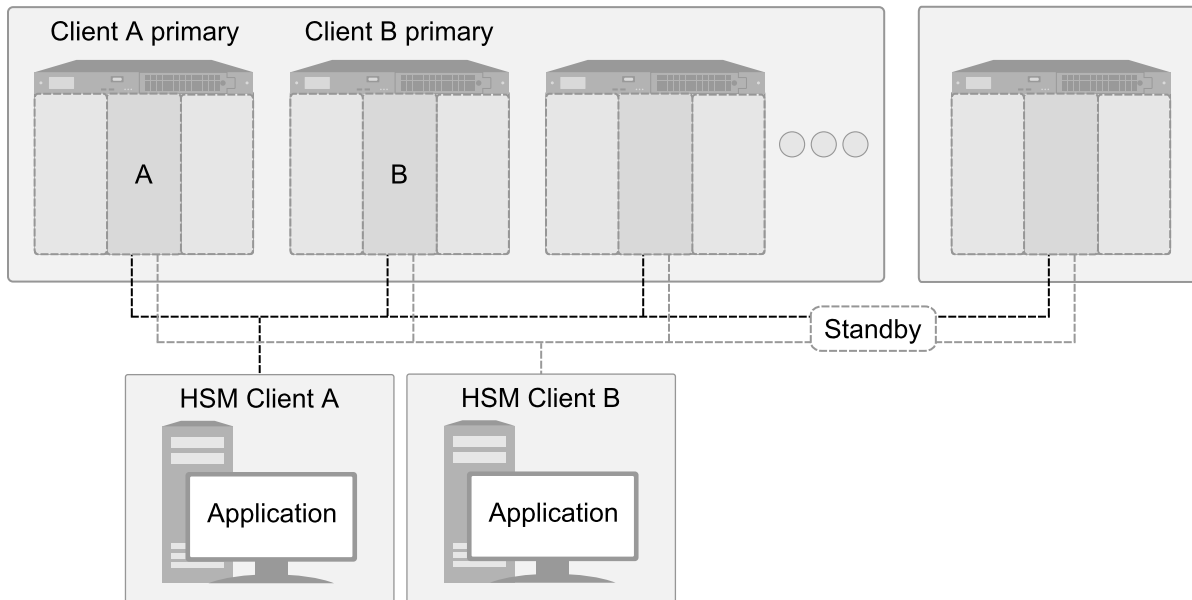
Since the contents of member partitions are always kept up-to-date, you can use an HA group to keep an automatic backup of your cryptographic objects. Set the backup member to standby mode so that it does not perform operations. If the regular member(s) fail, the standby member takes over operations.



### 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 190](#).

**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.

### 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 be the same hardware type (a mix of Network and PCIe HSMs is not supported) and use the same authentication method (Password/PED).

- > All must be running one of the supported software/firmware versions. Generally, Thales Group recommends using HSMs with the same software/firmware for HA. However, mixed-version HA groups containing Luna 6 and 7 member partitions and HSM on Demand (HSMoD) services are supported. See ["Cloning Keys Between Luna 6, Luna 7, and HSM on Demand" on page 238](#) for more information.
- > 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 ["Set the HSM Policies" on page 1](#) in the *Configuration Guide*).
- > 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 (see ["Enable the Client to Access a Partition" on page 1](#) in the *Configuration Guide*).

## 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 23](#))

**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" on page 1](#) in the *LunaCM Command Reference Guide*).

## To set up an HA group

1. Decide which partition will serve as the primary member (see ["The Primary Partition" on page 192](#)). 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 an HSM on Demand (HSMoD) service as a standby HA member. If you prefer to use HSMoD 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 153](#)):

```
[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 209](#).
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 211](#).
7. [Optional] Enable HA Only mode (recommended).  
See ["Enabling/Disabling HA Only Mode" on page 211](#).
8. [Optional] Configure HA logging.  
See ["HA Logging" on page 212](#) 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 -> 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

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> -nodelstroy -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 211](#).

## 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 196](#) 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 216](#)).
- > 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, an HSM on Demand (HSMoD) service from SafeNet Data Protection on Demand is always added to an HA group as a standby member. If you prefer to use HSMoD 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 153](#)):

```
[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, SafeNet 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 332).

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 223) When HA Only mode is enabled, the HA virtual slots are not affected by partition slot changes. Thales Group 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 SafeNet 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 the next page](#)

### Configuring HA Logging

Logging is automatically enabled when you configure an HA group (see ["Setting Up an HA Group" on page 203](#)), 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 SafeNet Luna HSM Client and the SafeNet 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<br><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<br><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><br><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<br><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><br><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<br><b>Description:</b> The user manually deactivated the partition, as determined after an HSM command (such as C_Sign) fails.                                                                                  |
| HALOG_MEMBER_NOW_ACTIVATED   | <MessagePrefix> recovery attempt <AttemptNumber> member <SerialNumber> is now activated and will be reintroduce back into the HA group.<br><b>Description:</b> Additional info about the recovered partition, which was deactivated and is now becoming activated. |
| HALOG_MEMBER_REVOKED         | <MessagePrefix> member: <SerialNumber> revoked<br><b>Description:</b> The user manually revoked the partition, as determined during a periodic recovery attempt.                                                                                                   |

| Message ID                             | Message/Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|----------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 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:<br/>       &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> |
| HALOG_REENABLEMEMBER<br>(deprecated)   | <p>&lt;MessagePrefix&gt; Re-enable auto recovery process for member: &lt;SerialNumber&gt;</p> <p><b>Description:</b> The user manually requested partition recovery, as determined during a periodic recovery attempt before an HSM command.</p>                                                                                                                                                                                                                                                       |
| HALOG_UNRECOVERABLE<br>(deprecated)    | <p>&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;</p> <p><b>Description:</b> The connection is invalid and is not eligible for recovery.</p>                                                                                                                                                                            |

| Message ID | Message/Description                                                                                                                                                                                                                                                                                                                                                                             |
|------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| No ID*     | <p>&lt;MessagePrefix&gt; member &lt;SerialNumber&gt; is not activated and is excluded from the HA group</p> <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*     | <p>&lt;MessagePrefix&gt; recovery attempt &lt;SerialNumber&gt; is not activated and cannot be reintroduced back into the HA group\n</p> <p><b>Description:</b> Recovery failed</p>                                                                                                                                                                                                              |
| No ID*     | <p>&lt;MessagePrefix&gt; recovery attempt &lt;SerialNumber&gt; is now activated and will be reintroduce back into the HA group.\n</p> <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 191).

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 193).

**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)

### 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

Thales Group recommends using auto-recovery for all HA group configurations (see "[Configuring HA Auto-Recovery](#)" on page 211). 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
```

- 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.

- 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 203 must be met.

### To replace an HA group member

- [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   |

- Prepare the new HA group member, whether that means creating a new partition on the original HSM or configuring a new SafeNet 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 203](#) 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
```

- 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
----- 1238700701509 ----- down
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.

- Remove the old partition from the group by specifying the serial number ().

```
lunacm:> hagroup removemember -group <label> -serial <serialnum>
```

LunaCM restarts.

- [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 209](#).

## 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 ).

```
lunacm:> hagroup deletegroup -group <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 may conflict.

### 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 Group drivers are running, and retry
- > reboot the client workstation
- > restore your client configuration from backup
- > re-install SafeNet 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 SafeNet 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 SafeNet 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 SafeNet 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.

### 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.

# CHAPTER 12: HSM Initialization

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

- > On a new HSM or factory-reset HSM, initialization sets the HSM SO credentials, the HSM label, and the cloning domain of the HSM Admin partition. This is often referred to as a 'hard' initialization. See ["Initializing a New or Factory-reset HSM" on the next page](#).
- > On an existing, non-factory-reset HSM, reinitialization destroys all existing partitions and objects, but retains the SO credentials and cloning domain. You have the option to change or retain the existing label. This is often referred to as a 'soft' initialization. See ["Re-initializing an Existing, Non-factory-reset HSM" on page 227](#).

**NOTE** To ensure accurate auditing, perform initialization only after you have set the system time parameters (time, date, time zone, use of NTP (Network Time Protocol)). You can use the **-authtimeconfig** option when initializing the HSM to require HSM SO authorization of any time-related changes once the HSM is initialized.

## Hard versus soft initialization

The following table summarizes the differences between a hard and soft initialization.

| Condition/Effect               | Soft init | Hard init                                                                                    |
|--------------------------------|-----------|----------------------------------------------------------------------------------------------|
| HSM SO authentication required | Yes       | No                                                                                           |
| Can set new HSM label          | Yes       | Yes                                                                                          |
| Creates new HSM SO identity    | No        | Yes                                                                                          |
| Creates new Domain             | No        | Yes                                                                                          |
| Destroys partitions            | Yes       | No (none exist to destroy, since the HSM is new or an <b>hsm factoryreset</b> was performed) |
| Destroys objects               | Yes       | No (none exist to destroy, since the HSM is new or an <b>hsm factoryreset</b> was performed) |



## Initializing a New or Factory-reset HSM

**NOTE** New HSMs are shipped in Secure Transport Mode (STM). You must recover the HSM from STM before you can initialize the HSM. See ["To initialize a new or factory-reset HSM \(hard init\)" on the next page](#) for details.

On a new, or factory reset HSM (using **hsm factoryreset**), you perform a 'hard init' to set the following:

|                           |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|---------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>HSM Label</b>          | <p>The label is a string that identifies this HSM unit uniquely.</p> <p>The HSM label created during initialization must be 1-32 characters in length. If you specify a longer label, it will automatically be truncated to 32 characters. Only alphanumeric characters and the underscore are allowed:</p> <p>abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789_</p> <p>For more information, refer to <a href="#">"Name, Label, and Password Requirements" on page 438</a>.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| <b>HSM SO credentials</b> | <p>For Multi-factor, or PED-authenticated HSMs, you create a new HSM SO (blue) PED key(set) or reuse an existing key(set) from an HSM you want to share credentials with. If you are using PED authentication, ensure that you have a PED key strategy before beginning. See <a href="#">"PED Authentication" on page 242</a>.</p> <p>For password-authenticated HSMs, you specify the HSM SO password. For proper security, it should be different from the appliance admin password, and employ standard password-security characteristics.</p> <p>In LunaSH, the HSM SO password must be 7-255 characters in length. The following characters are allowed:</p> <p>abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789 !@#\$%^&amp;*()-_=[ ]<br/>{ } / : ' , . ~</p> <p>The following characters are invalid or problematic and must not be used in the HSM SO password:</p> <p>" &amp; ; &lt; &gt; \ `  </p> <p>Spaces are allowed; to specify a password with spaces using the <b>-password</b> option, enclose the password in double quotation marks.</p> |

**Cloning domain for the HSM Admin partition**

The cloning domain is a shared identifier that makes cloning possible among a group of HSM partitions. It specifies the security domain (group of HSM partitions) within which the HSM Admin partition can share cryptographic objects through cloning, backup/restore, or in high availability configurations. Note that the HSM Admin partition cloning domain is independent of the cloning domain specified when creating application partitions on the HSM.

For Multi-factor, PED-authenticated HSMs, you create a new Domain (red) PED key(set) or re-use an existing key(set) from an HSM you want to be able to clone with.

For password-authenticated HSMs, you create a new domain string or re-use an existing string from an HSM you want to be able to clone with.

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.

**NOTE** Always specify a cloning domain when you initialize a Password-authenticated SafeNet Luna HSM in a production environment. The HSM allows you to specify "defaultdomain" at initialization, the factory-default domain. This is deprecated, as it is insecure. Anyone could clone objects to or from such an HSM. The default domain is provided for benefit of customers who have previously used the default domain, and for migration purposes. When you prepare a SafeNet Luna HSM to go into service in a real production environment, always specify a proper, secure domain string when you initialize the HSM.

**To initialize a new or factory-reset HSM (hard init)**

**CAUTION!** Ensure that you are prepared. Once initialized, re-initializing the HSM forces the deletion of all partitions and objects on the HSM.

1. If Secure Transport Mode is set, you must unlock the HSM before proceeding. New SafeNet Luna HSMs are shipped from the factory in Secure Transport Mode (STM). STM allows you to verify whether or not an HSM has been tampered while it is not in your possession, such as when it is shipped to another location, or placed into storage. See ["Secure Transport Mode" on page 328](#) in the *Administration Guide* for more information.

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

- a. As part of the delivery process for your new HSM, you should have received an email from Thales Client Services, containing two 16-digit strings, as follows. You will need both of these strings to recover the HSM from STM:

Random User String: XXXX-XXXX-XXXX-XXXX

Verification String: XXXX-XXXX-XXXX-XXXX

- b. Ensure that you have the Random User String and Verification String that were emailed to you for your new HSM.

- c. Enter the following command to recover from STM, specifying the Random User String that was emailed to you for your new HSM:  
lunash:> **hsm stm recover -randomuserstring** <XXXX-XXXX-XXXX-XXXX>
  - d. You are presented with a verification string. If the verification string matches the original verification string emailed to you for your new HSM, the HSM has not been tampered, and can be safely deployed. If the verification string does not match the original verification string emailed to you for your new HSM, the HSM has been tampered while in STM. If the verification strings do not match, contact Thales Group Technical Support immediately.
  - e. Enter **proceed** to recover from STM (regardless of whether the strings match or not), or enter **quit** to remain in STM.
2. If you are initializing a Multi-factor-authentication (PED-authenticated) HSM, have the Luna PED connected and ready (via USB, in Local PED-USB mode). If your PED is not in USB mode, see ["Changing Modes" on page 250](#) in the *HSM Administration Guide*. Alternatively, have a Remote PED instance set up, see ["About Remote PED" on page 252](#).
  3. Log into LunaSH as the appliance administrator 'admin'. You can use a serial terminal window or SSH connection.
  4. Run the **hsm init** command, specifying a label for your SafeNet Luna Network HSM:  
lunash:> **hsm init -label** <label>
  5. Respond to the prompts to complete the initialization process:
    - on a password-authenticated HSM, you are prompted for the HSM password and for the HSM Admin partition cloning domain string (cloning domains for application partitions are set when the application partitions are initialized).
    - on a Multi-factor-authenticated (PED-authenticated) HSM, you are prompted to attend to the PED to create a new HSM SO (blue) PED key for this HSM, re-use an HSM SO PED key from an existing HSM so that you can also use it to log in to this HSM, or overwrite an existing key with a new PED secret for use with this HSM. You are also prompted to create, re-use, or overwrite the Domain (red) PED key. You can create MofN quorum keysets and duplicate keys as required. See ["PED Authentication" on page 242](#) for more information.

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

- ["PED-authenticated HSM Initialization Example" on the next page](#)
- ["Password-authenticated HSM Initialization Example" on page 234](#)

## Re-initializing an Existing, Non-factory-reset HSM

On an existing, non-factory-reset HSM, re-initialization clears all existing partitions and objects, but retains the SO credentials and cloning domain. You have the option to change or retain the existing label. Re-initialization is also referred to as a soft init. If you do not want to do a soft init, and also change the SO credentials and cloning domain, you need to use the **hsm factoryreset** command to factory reset the HSM, and then perform the procedure described in ["Initializing a New or Factory-reset HSM" on page 225](#).

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

### To re-initialize an existing, non-factory-reset HSM (soft init)

1. Log in as the HSM SO.
2. If Secure Transport Mode is set, you must unlock the HSM before proceeding. See "[Secure Transport Mode](#)" on page 328 in the *Administration Guide*.
3. If you are initializing a PED-authenticated HSM, have the Luna PED connected and ready (via USB, in Local PED-USB mode). If your PED is not in USB mode, see "[Changing Modes](#)" on page 250 in the *HSM Administration Guide*.
4. Log into LunaSH as the appliance administrator 'admin'. You can use a serial terminal window or SSH connection.
5. Run the **hsm init** command, specifying a label for your SafeNet Luna Network HSM:  
lunash:> **hsm init -label** <label>

## PED-authenticated HSM Initialization Example

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

- > "[To initialize a PED-authenticated HSM](#)" below
- > "[Imprinting the Blue HSM SO PED Key](#)" on page 230
- > "[Imprinting the Red Cloning Domain PED Key](#)" on page 232
- > "[New, reuse, and overwrite options](#)" on page 232

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

### To initialize a PED-authenticated HSM

1. Your Luna PED must be connected to the HSM, either locally/directly in USB mode (see "[Changing Modes](#)" on page 250), or remotely via Remote PED connection (see "[About Remote PED](#)" on page 252).

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



This rule does not apply for local PED authentication to a locally attached G7-based backup HSM. In this case you connect a remote PED to one of the appliance USB ports and connect to the **pedserver** service running on the appliance at IP address 127.0.0.1. See ["Backup and Restore Using a G7-Based Backup HSM" on page 76](#) for more information.

2. Set the active slot to the SafeNet Luna Network HSM Admin partition, and issue the **hsm init** command. The HSM passes control to the Luna PED, and the command line directs you to attend to the PED prompts.
3. When you issue the **hsm init** command, the HSM passes control to the Luna PED, and the command line (lunash:>) directs you to attend to the PED prompts.
4. A "default" login is performed, just to get started (you don't need to supply any authentication for this step).
5. Luna PED asks: "Do you wish to reuse an existing keyset?". If the answer is **No**, the HSM creates a new secret which will reside on both the HSM and the key (or keys) that is (or are) about to be imprinted. If the answer is **Yes**, then the HSM does not create a new secret and instead waits for one to be presented via the PED.
6. Luna PED requests a blue PED key. It could be blank to begin with, or it could have a valid secret from another HSM (a secret that you wish to preserve), or it could have a secret that is no longer useful.
7. Luna PED checks the key you provide. If the PED key is not blank, and your answer to "...reuse an existing keyset" was **Yes**, then Luna PED proceeds to copy the secret from the PED key to the HSM.
8. If the key is not blank, and your answer to "...reuse an existing keyset" was **No**, then the PED inquires if you wish to overwrite its contents with a new HSM secret. If the current content of the key is of no value, you say **Yes**. If the current content of the key is a valid secret from another HSM (or if you did not expect the key to hold any data) you can remove it from the PED and replace it with a blank key or a key containing non-useful data, before you answer **Yes** to the 'overwrite' question.
9. Assuming that you are using a new secret, and not reusing an existing one, Luna PED asks if you wish to split the new HSM secret. It does this by asking for values of "M" and "N". You set those values to "1" and "1" respectively, unless you require MofN split-secret, multi-person quorum access control for your HSM (See ["M of N Split Secrets \(Quorum\)" on page 247](#) for details).
10. Luna PED asks if you wish to use a PED PIN (an additional secret; see ["PED Key Management" on page 276](#) for more info).
11. If you just press **Enter** (effectively saying 'no' to the PED PIN option), then the secret generated by the HSM is imprinted on the PED key, that same secret is retained as-is on the HSM, and the same secret becomes the piece needed to unlock the Security Officer/HSM Admin account on the HSM.
12. If you press some digits on the PED keypad (saying 'yes' to the PED PIN option), then the PED combines the HSM-generated secret with your PED PIN and feeds the combined data blob to the HSM. The HSM throws away the original secret and takes on the new, combined secret as its SO/HSM Admin secret.

13. The PED key contains the original HSM-generated secret, but also contains the flag that tells the PED whether to demand a PED PIN (which is either no digits, or a set of digits that you supplied, and must supply at all future uses of that PED key).
14. Luna PED gives you the option to create some duplicates of this imprinted key. You should make at least one duplicate for backup purposes. Make additional duplicates if your security policy permits, and your procedures require them.
15. Next, Luna PED requests a red Domain PED key. The HSM provides a cloning Domain secret and the PED gives you the option to imprint the secret from the HSM, or to use a domain that might already be on the key. You choose appropriately. If you are imprinting a new Domain secret, you have the same opportunities to split the secret, and to apply a PED PIN "modifier" to the secret. Again, you are given the option to create duplicates of the key.
16. At this point, the HSM is initialized and Luna PED passes control back to LunaSH.

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

### Imprinting the Blue HSM SO PED Key

1. Decide if you want to reuse a keyset.

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

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

2. Set MofN.

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

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

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

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

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

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

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

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

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

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

### 5. Decide if you want to duplicate your keyset.

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

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

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

## Imprinting the Red Cloning Domain PED Key

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

### 1. Decide if you want to reuse a keyset.

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

- **No:** If this is your first SafeNet Luna HSM, or if this HSM will not be cloning objects with other HSMs that are already initialized
- **Yes:** If you have another HSM and wish that HSM and the current HSM to share their cloning Domain.

### 2. Set MofN.

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

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

### 4. Optionally set a PED PIN.

### 5. Decide if you want to duplicate your keyset.

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

```
Command Result : No Error
```

## New, reuse, and overwrite options

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

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



The next two columns of the table show some differences if you are using previously-imprinted PED keys, choosing either to reuse what is found on the key (imprint it on your new HSM - see "[Shared PED Key Secrets](#)" on page 246) or, to overwrite what is found and generate a new secret to be imprinted on both the PED key and the HSM.

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

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

## Password-authenticated HSM Initialization Example

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

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

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

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

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

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

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

```
'hsm init' successful.
```

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

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

# CHAPTER 13: HSM Status Values

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

| Indicated Status of HSM        | Meaning                                                                                                                                                            | Recovery                                                                                                                                                                                                                                                                    |
|--------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| OK                             | The HSM is in a good state, working properly.                                                                                                                      | n/a                                                                                                                                                                                                                                                                         |
| Zeroized                       | The HSM is in zeroized state. All objects and roles are unusable.                                                                                                  | HSM initialization is required before the HSM can be used again. "Hard init" - HSM SO and domain are gone, no authentication required. (see Note1)                                                                                                                          |
| Decommissioned                 | The HSM has been decommissioned.                                                                                                                                   | HSM initialization is required before the HSM can be used again. "Hard init" - HSM SO and domain are gone, no authentication required. (see Note1)                                                                                                                          |
| Transport Mode                 | The HSM is in Secure Transport Mode.                                                                                                                               | STM must be disabled before the HSM can be used.                                                                                                                                                                                                                            |
| Transport Mode, zeroized       | The HSM is in Secure Transport Mode, and is also zeroized.                                                                                                         | STM must be disabled, and then HSM initialization is required before the HSM can be used.                                                                                                                                                                                   |
| Transport Mode, Decommissioned | The HSM is in Secure Transport Mode, and has been decommissioned.                                                                                                  | STM must be disabled, and then HSM initialization is required before the HSM can be used.                                                                                                                                                                                   |
| Hardware Tamper                | The HSM has been tampered. (MTK is destroyed and must be rebuilt from recovery vectors.)                                                                           | Reboot the host or restart the HSM (vreset for SafeNet Luna PCIe HSM, or ureset for SafeNet Luna USB HSM). The event is logged                                                                                                                                              |
| Hardware Tamper, Zeroized      | The HSM has been tampered. (MTK is destroyed and must be rebuilt from recovery vectors.)<br>The HSM is also in zeroized state. All objects and roles are unusable. | Reboot the host or restart the HSM (vreset for SafeNet Luna PCIe HSM, or ureset for SafeNet Luna USB HSM). The event is logged.<br><br>HSM initialization is required before the HSM can be used again. HSM SO and domain are gone, no authentication required. (see Note1) |

| Indicated Status of HSM       | Meaning                                                                                                                           | Recovery                                                                                                                                                                                                                                                                    |
|-------------------------------|-----------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| HSM Tamper,<br>Decommissioned | The HSM has been tampered. (MTK is destroyed and must be rebuilt from recovery vectors.)<br>The HSM has also been decommissioned. | Reboot the host or restart the HSM (vreset for SafeNet Luna PCIe HSM, or ureset for SafeNet Luna USB HSM). The event is logged.<br><br>HSM initialization is required before the HSM can be used again. HSM SO and domain are gone, no authentication required. (see Note1) |

**NOTE1:** A condition, not reported above, preserves the HSM SO and the associated Domain, while SO objects and all application partitions and contents are destroyed. In this case, HSM SO login is required to perform a "soft init". See "[HSM Initialization](#)" on page 224 for more information.

For a comparison of various destruction or denial actions on the HSM, see "[Comparison of Destruction/Denial Actions](#)" on page 174.

# CHAPTER 14: Key Cloning

You can clone key material between HSMs and partitions to backup 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:

- > ["Key Cloning Overview and Key Concepts" below](#)
- > ["Cloning Objects to Another Application Partition" below](#)
- > ["Cloning Keys Between Luna 6, Luna 7, and HSM on Demand" on the next page](#)

## Key Cloning 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](#).
- > 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 ["Capabilities and Policies" on page 95](#).

## 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 23](#)). 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>]
```

### 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 HSM on Demand

SafeNet Luna HSM Client allows you to clone keys between Luna 6 partitions, Luna 7 partitions, and SafeNet Data Protection on Demand (DPoD)'s HSM on Demand 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 SafeNet 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 199), in addition to the considerations listed below.

- > ["Luna/HSMoD Cloning" below](#)
- > ["Supported Software/Firmware Versions" on the next page](#)
- > ["Mismatched Partition Policies and FIPS Mode" on page 240](#)
- > ["Mismatched Key Types/Cryptographic Mechanisms" on page 240](#)
- > ["Minimum Key Sizes" on page 240](#)
- > ["SafeXcel 1746 Co-Processor" on page 240](#)
- > ["HA Performance Optimization" on page 241](#)

### Luna/HSMoD Cloning

Cloning between Luna partitions and HSMoD services require the following special considerations, in addition to the general considerations below.

**NOTE** This feature has software and/or firmware dependencies. See "[Version Dependencies by Feature](#)" on page 393 for more information.

## Authentication

HSMoD services use password authentication, and therefore they can clone objects to and from password-authenticated SafeNet Luna Network HSMs only. It is not possible to clone keys between an HSMoD service and a PED-authenticated Luna HSM.

## Network Latency and HSMoD as Active HA Member

Requests performed by cloud services like HSMoD may experience greater network latency than those sent to on-premise HSMs. Thales Group recommends using a HSMoD service as a standby HA member to achieve the best performance. By default, you can add an HSMoD service as a standby HA member only. If all other HA members fail and the HSMoD service becomes active, it will revert to standby when another member recovers.

If you prefer to use HSMoD 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 153):

```
[Toggles]
lunacm_cv_ha_ui = 0
```

## Cloning Capacity Limitations

The following limitations apply to clients accessing a HSMoD 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 an HSMoD 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 HSMoD service.

## Supported Software/Firmware Versions

Thales Group supports cloning between Luna 6/7 partitions and HSMoD services using combinations of appliance software/firmware as outlined in the table below.

| Client Software                                                              | Luna Appliance Software | Luna HSM Firmware |
|------------------------------------------------------------------------------|-------------------------|-------------------|
| <b>HSMoD 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 199). For example, Luna 6 HSMs have certain policies that have been removed from Luna 7 and HSMoD, and new policies have been introduced.

Ensure that policies common to Luna 6/7/HSMoD 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.

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 HSMoD, 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
```



## HA Performance Optimization

SafeNet 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 HSMoD services may be limited by network latency, compared to on-premises Luna HSMs. See ["Luna/HSMoD Cloning" on page 238](#).

Thales Group 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 SafeNet Luna Network HSM's vastly improved performance for:

- > key generation
- > random number generation

The load-balancing logic is determined by the SafeNet Luna HSM Client software, so the Luna 7 behavior applies to mixed-version HA (see ["Load Balancing" on page 191](#)).

**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 HSMoD service has become the primary member. By default, an HSMoD service will revert to standby once another HA member recovers.

# CHAPTER 15: PED Authentication

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

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

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

This chapter contains the following sections about PED authentication:

- > ["SafeNet Luna PED Hardware Functions" on page 248](#)
- > ["Local PED Setup" on page 251](#)
- > ["About Remote PED" on page 252](#)
- > ["Remote PED Setup" on page 257](#)
  - ["Initializing the Remote PED Vector \(RPV\) and Creating an Orange Remote PED Key \(RPK\)" on page 258](#)
  - ["Installing PEDserver and Setting Up the Remote Luna PED" on page 261](#)
  - ["Opening a Remote PED Connection" on page 262](#)
  - ["Ending or Switching the Remote PED Connection" on page 271](#)
  - ["Remote PED Troubleshooting" on page 272](#)
- > ["PED Key Management" on page 276](#)
  - ["Creating PED Keys" on page 276](#)
  - ["Performing PED Authentication" on page 281](#)
  - ["Consequences of Losing PED Keys" on page 283](#)
  - ["Identifying a PED Key Secret" on page 285](#)
  - ["Duplicating Existing PED Keys" on page 286](#)
  - ["Changing a PED Key Secret" on page 287](#)
- > ["PEDserver and PEDclient" on page 289](#)

## PED Authentication Architecture

The PED Authentication architecture consists of the following components:

- > **SafeNet Luna PED:** a PIN Entry Device with a local or remote connection to the HSM. The PED reads authentication secrets from PED keys on behalf of an HSM or partition (see ["SafeNet Luna PED Hardware Functions" on page 248](#)).
- > **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 246](#).
  - **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 247](#).
  - **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 247](#).

## 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 276.



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

## PED Key Types and Roles

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

The PED key colors correspond with the HSM roles described in "[HSM Roles](#)" on page 430. 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 the next page.<br><b>Mandatory</b>                                                                                                          |
|                          | <b>Orange</b><br> | Remote PED Vector                      | Establishes a connection to a Remote PED server.<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 the next page.<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>  | 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> |

## 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 1](#) in the *Configuration Guide*.

**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 276](#)). Copies made later are true copies with the same PED PIN, intended as backups for one person (see ["Duplicating Existing PED Keys" on page 286](#)). 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 283](#).

## 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.

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

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

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

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

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

### Activated Partitions and M of N

For security reasons, the HSM and its servers are often kept in a locked facility, and accessed under specific circumstances, directly or by secure remote channel. To accommodate these security requirements, the Crypto Officer and Crypto User roles can be Activated (to use a secondary, alpha-numeric login credential to authenticate), allowing applications to perform cryptographic functions without having to present a black or gray PED key (see "[Activation and Auto-activation on Multi-factor- \(PED-\) Authenticated Partitions](#)" on [page 23](#)). 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.

## SafeNet Luna PED Hardware Functions

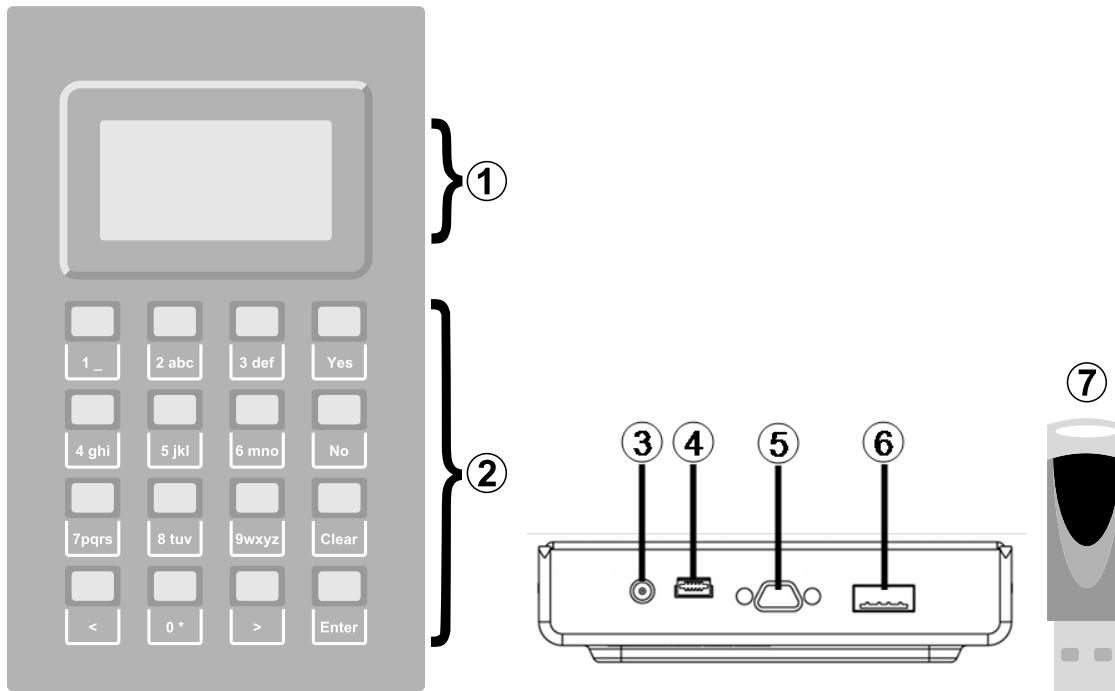
The SafeNet Luna PED reads authentication secrets from PED keys on behalf of an HSM or partition. This section contains the following information about the Luna PED device:

- > "[Physical Features](#)" below
- > "[Keypad Functions](#)" on the next page
- > "[Modes of Operation](#)" on page 250
- > "[Admin Mode Functions](#)" on page 251

### Physical Features

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





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

\* PEDs with firmware version 2.8 and above are powered by any USB 2.x or 3.x connection, and do not have an external DC power supply. The PED driver must be installed on the connected computer. If the PED is connected to a hub or to a computer without the driver, then the PED display backlight illuminates, but no PED menu is presented.)

## Keypad Functions

The Luna PED keypad functions are as follows:

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

## Modes of Operation

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

- > **Local PED-SCP:** This mode is reserved for legacy SafeNet Luna 6.x HSMs that use an MDSM connector between the PED and the HSM. It does not apply to Luna 7.x. Initial HSM configuration must be done in Local PED mode. See "[Local PED Setup](#)" on the next page for instructions.
- > **Admin:** This mode is for upgrading the PED device firmware, diagnostic tests, and PED key duplication. See "[Admin Mode Functions](#)" on the next page for the functions available in this mode.
- > **Remote PED:** In this mode, the PED is connected to a remote workstation and authenticated to the HSM with an orange PED key containing a Remote PED Vector (RPV) secret. This mode allows the SafeNet Luna Network HSM to be located in a data center or other location restricting physical access. See "[About Remote PED](#)" on page 252 for more information.
- > **Local PED-USB:** In this mode, the PED is connected directly to the HSM card with a USB mini-B to USB-A connector cable. Initial HSM configuration must be done in Local PED mode.

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

### Changing Modes

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

#### To change the Luna PED's active mode

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

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

PED V.2.7.1-5
```

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

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

**NOTE** The Luna PED must be in **Local PED-USB** mode when connected to a Release 7.x SafeNet Luna 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 Group.
- > **Self Test:** test the PED's functionality. Follow the on-screen instructions to test button functions, display, cable connections, and the ability to read PED keys. The PED returns a PASS/FAIL report once it concludes the test.

## Local PED Setup

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

### Setting Up a Local PED Connection

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

- > SafeNet Luna PED with firmware 2.7.1 or newer

- > USB mini-B to USB-A connector cable
- > Luna PED DC power supply (if included with your Luna PED)

### To set up a Local PED connection

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

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



This rule does not apply for local PED authentication to a locally attached G7-based backup HSM. In this case you connect a remote PED to one of the appliance USB ports and connect to the **pedserver** service running on the appliance at IP address 127.0.0.1. See "[Backup and Restore Using a G7-Based Backup HSM](#)" on page 76 for more information.

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 250.

The Luna PED is now ready to perform authentication for the HSM. You may proceed with setting up or deploying your SafeNet 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 281)
- > Create copies of your PED keys (see "[Duplicating Existing PED Keys](#)" on page 286)
- > Change to the Admin Mode to run tests or update PED software (see "[Changing Modes](#)" on page 250)
- > Prepare to set up a Remote PED server (see "[About Remote PED](#)" below)

## 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:

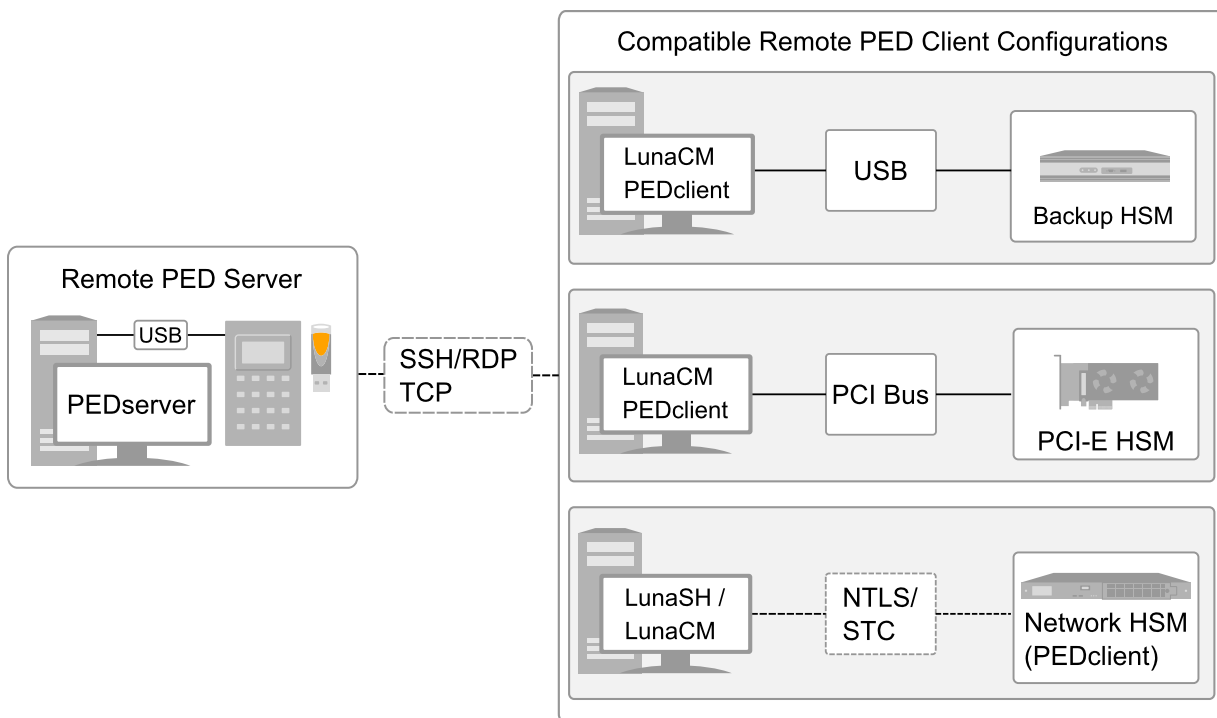
- > "[Remote PED Architecture](#)" on the next page
- > "[Remote PED Connections](#)" on the next page

> ["PEDserver-PEDclient Communications" on page 256](#)

## Remote PED Architecture

The Remote PED architecture consists of the following components:

- > **Remote PED:** a Luna PED with firmware 2.7.1 or newer, connected to a network-connected workstation, powered on, and set to Remote PED mode.
- > **Remote PED Vector (RPV):** a randomly generated, encrypted value used to authenticate between a Remote PED (via PEDserver) and a SafeNet Luna HSM (via PEDclient).
- > **Remote PED Key (RPK):** an orange PED key containing an RPV (or multiple PED keys with a split RPV in an M of N implementation).
- > **PEDserver:** software that runs on the remote workstation with a USB-connected Luna PED. PEDserver accepts requests from and serves PED actions and data to PEDclient.
- > **PEDclient:** software that requests remote PED services from PEDserver. PEDclient runs on the network-connected system hosting the HSM, which can be one of the following:
  - SafeNet Luna Network HSM
  - Host computer with SafeNet Luna PCIe HSM installed
  - Host computer with USB-connected SafeNet Luna Backup HSM, configured for remote backup

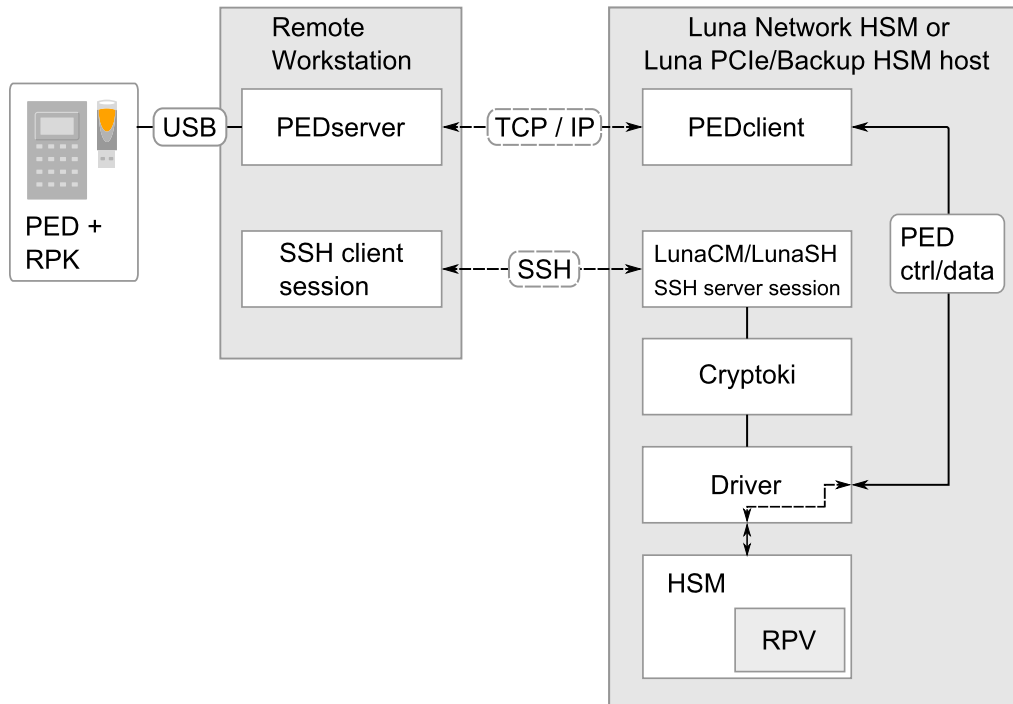


## Remote PED Connections

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

- > PEDServer is running

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



### 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 SafeNet Luna Network HSM be allowed to initiate external connections, and that the PEDserver IP port remains open. If the SafeNet 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 263.
- > **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 SafeNet 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 267.

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 271](#).

## 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 271](#).

## Timeout

PEDserver and PEDclient both have configurable timeout settings (default: 1800 seconds). See ["pedserver mode config" on page 309](#) 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)
- > SafeNet Luna PED is physically disconnected from its host
- > VPN or network connection is disrupted
- > You exit Remote PED mode on the Luna PED. If you attempt to change menus, the PED warns:

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

If the link is broken, as long as the network connection is intact (or is resumed), you can restart PEDserver on the Remote PED host and run **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 Group 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

```

## Remote PED Setup

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

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

1. ["Initializing the Remote PED Vector \(RPV\) and Creating an Orange Remote PED Key \(RPK\)" on the next page](#)
2. ["Installing PEDserver and Setting Up the Remote Luna PED" on page 261](#)
3. ["Opening a Remote PED Connection" on page 262](#)
  - ["HSM-Initiated Remote PED" on page 263](#)
  - ["PED-Initiated Remote PED" on page 267](#)
4. [OPTIONAL] ["Ending or Switching the Remote PED Connection" on page 271](#)

If you encounter issues with Remote PED, see ["Remote PED Troubleshooting" on page 272](#).

Once Remote PED is set up, see ["PED Key Management" on page 276](#).

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

The Remote PED (via PEDserver) authenticates itself to the SafeNet Luna 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 SafeNet 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](#)" below.

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

Continue to "[Installing PEDserver and Setting Up the Remote Luna PED](#)" on page 261.

**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:

- > SafeNet Luna PED with firmware 2.7.1 or newer
- > USB mini-B to USB-A connector cable
- > Luna PED DC power supply (if included with your Luna PED)
- > Blank or reusable orange PED key (or multiple keys, if you plan to make extra copies or use an M of N security scheme). See "[Creating PED Keys](#)" on page 276 for more information.

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

1. If you have not already done so, set up a Local PED connection (see "[Local PED Setup](#)" on page 251).
2. Using a serial or SSH connection, log in to the SafeNet Luna Network HSM appliance as **admin**.
3. If the HSM is initialized, login as HSM SO ("[hsm login](#)" on page 1). If not, skip to the next step.

```
lunash:>hsm login
```

4. Ensure that you have the orange PED key(s) ready. Initialize the RPV ("[hsm ped vector init](#)" on page 1).

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

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

If you are sure that you wish to initialize remote PED vector (RPV), then enter 'proceed', otherwise type 'quit'.

```
> proceed
Proceeding...
```

Luna PED operation required to initialize remote PED key vector - use orange PED key(s).

5. Attend to the Luna PED and respond to the on-screen prompts. See ["Creating PED Keys" on page 276](#) 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 page 261](#).

### 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 has software and/or firmware dependencies. See ["Version Dependencies by Feature" on page 393](#) for more information.

If you open an HSM-initiated Remote PED connection with **hsm ped connect**, and you have not already initialized the RPV or the HSM, then 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:
```

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 276](#) for more information.

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

1. In LunaSH, when prompted to "Enter PED Password" set any 8-digit numeric password that the HSM will use to identify the Remote PED server this one time. 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 ("[hsm ped vector init](#)" on page 1).

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

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

If you are sure that you wish to initialize remote PED vector (RPV), then enter 'proceed', otherwise type 'quit'.

```
> proceed
Proceeding...
```

Luna PED operation required to initialize remote PED key vector - use orange PED key(s).

4. Attend to the Luna PED and respond to the on-screen prompts. See ["Creating PED Keys" on page 276](#) 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. Return to ["HSM-Initiated Remote PED" on page 263](#) to complete the procedure.

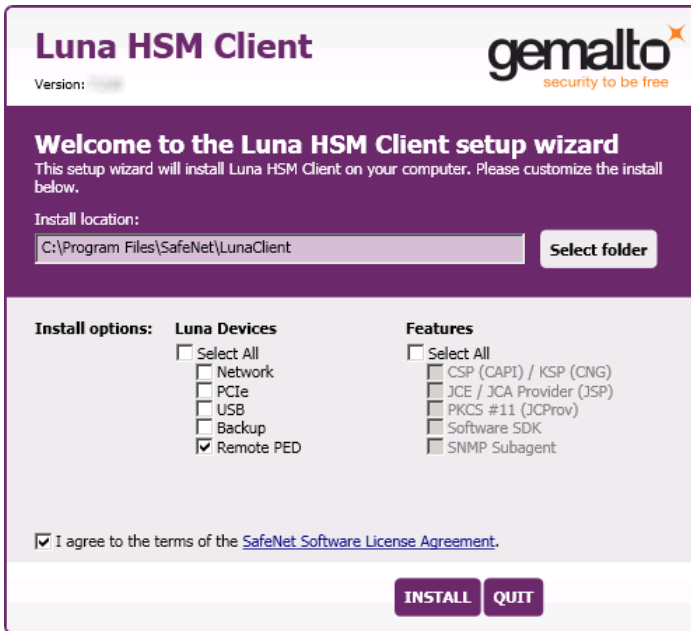
## Installing PEDserver and Setting Up the Remote Luna PED

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 SafeNet Luna HSM Client installer. You require:

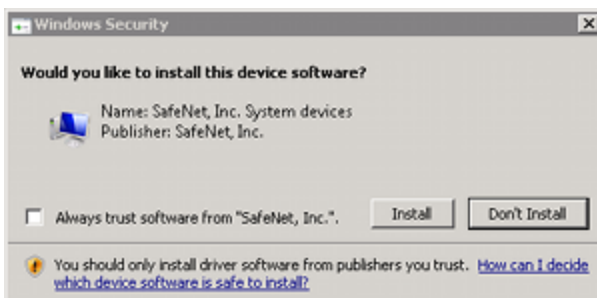
- > Network-connected workstation with compatible operating system (refer to the release notes)
- > SafeNet Luna HSM Client installer
- > SafeNet Luna PED with firmware 2.7.1 or higher
- > USB mini-B to USB-A connector cable
- > Luna PED DC power supply (PED 2.7.1 only; PED 2.8 and higher is powered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

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

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



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



3. On Windows, reboot the computer to ensure that the Luna PED driver is accepted by Windows. This step is not required for Linux or Windows Server operating systems.

4. Connect the Luna PED to a USB port on the host system using the supplied USB mini-B to USB-A connector cable.

PED version 2.8 and above is powered via the USB connection. If you are using PED version 2.7.1, connect it to power using the Luna PED DC power supply.

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

To manually set the operation mode to **Remote PED**, see ["Changing Modes" on page 250](#).

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 SafeNet Luna Network HSM be allowed to initiate external connections, and that the PEDserver IP port remains open. If the SafeNet 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" on the next page](#).

- > **PED-initiated:** The HSM and Remote PED host exchange and register certificates, creating a trusted connection. This allows the Remote PED host (via PEDserver) to initiate the connection to the SafeNet 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 267](#).

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

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

If you encounter issues, see ["Remote PED Troubleshooting" on page 272](#).

## 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 261](#))
- > Administrative access to the SafeNet Luna Network HSM via SSH (if using Remote PED for HSM-level authentication)
- > Administrative access to a SafeNet 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 \(RPV\) and Creating an Orange Remote PED Key \(RPK\)" on page 258](#))
  - 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 SafeNet Luna HSM Client install directory.
  - > **cd C:\Program Files\SafeNet\LunaClient\**
  - > **cd /usr/safenet/lunaclient**
3. Launch PEDserver (see ["pedserver" on page 303](#) for all available options). If you are launching PEDserver on an IPv6 network, you must include the **-ip** option.

```
>pedserver mode start [-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" on page 308](#)).

```
>pedserver mode show
```

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 SafeNet Luna Network HSM appliance, see ["To open a Remote PED connection from the SafeNet 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 page 266.

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

1. Open an SSH session to the SafeNet Luna Network HSM and log in to LunaSH as **admin**.
2. Initiate the Remote PED connection from the SafeNet Luna Network HSM ("[hsm ped connect](#)" on page 1).

```
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 SafeNet Luna Backup HSM connected to one of the SafeNet 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 259](#) 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.

- Verify the Remote PED connection by entering a command that requires PED authentication ("[hsm login](#)" on page 1, "[hsm init](#)" on page 1).
  - If the HSM is already initialized and you have the blue HSM SO key, you can use **hsm login**.
  - If the HSM is uninitialized, you can initialize it now with **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 276](#) 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 271](#).

- [OPTIONAL] Set a default IP address and/or port for the SafeNet Luna Network HSM to look for a configured Remote PED ("[hsm ped set](#)" on page 1).

```
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 **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 271](#).

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

1. Launch LunaCM on the client.

2. Initiate the Remote PED connection ("[ped connect](#)" on page 1).

```
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 ("[role login](#)" on page 1).

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

- If the partition is uninitialized, you can initialize it now ("[partition init](#)" on page 1). 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 276 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 271

6. [OPTIONAL] Set a default IP address and/or port for the SafeNet Luna Network HSM to look for a configured Remote PED ("[ped set](#)" on page 1).

```
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 **ped connect** (without specifying the IP/port) to initiate the Remote PED connection ("[ped connect](#)" on page 1). 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 271.

### 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 SafeNet 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 261)
- > Orange PED key with the HSM's RPV (see "[Initializing the Remote PED Vector \(RPV\) and Creating an Orange Remote PED Key \(RPK\)](#)" on page 258)
- > Administrative access to the SafeNet 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 SafeNet 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 ("[pedserver regen](#)" on page 319).

**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 -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 SafeNet Luna Network HSM's NTLS certificate ("[SCP and PSCP](#)" on page 1). Enter the appliance's admin account password when prompted. Note the period at the end of the command.

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

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

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

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

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

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

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

6. Register the SafeNet Luna Network HSM certificate with PEDserver ("[pedserver appliance register](#)" on page 307). 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 -name <appliance_name> -certificate <cert_filename> -ip <appliance_IP> -port <port>
```

```
c:\Program Files\SafeNet\LunaClient>pedserver -appliance register -name myLunaHSM -certificate
server.pem -ip 192.20.11.78 -port 9697
Ped Server Version 1.0.6 (10006)
```

Successfully registered host myLunaHSM.

7. Open an SSH session to the SafeNet Luna Network HSM and log in to LunaSH as **admin**.
8. Register the PEDserver host certificate ("[hsm ped server register](#)" on page 1).

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

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

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

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

9. Initiate the connection between PEDserver and the SafeNet Luna Network HSM ("[pedserver mode connect](#)" on page 311).

```
>pedserver mode connect -name <appliance_name>
```

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

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

```
Successfully connected to myLunaHSM.
```

- 10.** Using LunaSH, list the available registered Remote PED servers to find the server name (taken from the certificate filename during registration). Select the server you want to use to authenticate credentials for the appliance ("[hsm ped server list](#)" on page 1, "[hsm ped select](#)" on page 1).

```
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 page 271.

### 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 (lunash) to the HSM.

- > 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 **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 SafeNet 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 ("[hsm ped disconnect](#)" on page 1).

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

2. You are now able to initiate a connection to a different Remote PED host running PEDserver ("[hsm ped connect](#)" on page 1). 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 **ped set -ip <PEDserver\_IP> -port <port>**.

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

1. End the Remote PED connection ("[ped disconnect](#)" on page 1).

```
lunacm:>ped disconnect
```

2. You are now able to initiate a connection to a different Remote PED host running PEDserver ("[ped connect](#)" on page 1). 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 **ped set -ip <PEDserver\_IP> -port <port>** (set "[ped set](#)" on page 1).

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

1. End the Remote PED connection with the current host ("[hsm ped deselect](#)" on page 1).  

```
lunash:>hsm ped deselect -host <server_name>
```
2. Check the available list of Remote PED servers ("[hsm ped server list](#)" on page 1).  

```
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 267.
3. The new Remote PED server must initiate the connection to the appliance ("[pedserver mode connect](#)" on page 311).  

```
>pedserver mode connect -name <appliance_name>
```
4. In LunaSH, you are now able to select the new Remote PED server from the available list ("[hsm ped select](#)" on page 1).  

```
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](#)" below
- > "[RC\\_SOCKET\\_ERROR: PEDserver Requires Administrator Privileges](#)" below
- > "[LUNA\\_RET\\_PED\\_UNPLUGGED: Reconnect HSM-initiated Remote PED Before Issuing Commands](#)" on the next page
- > "[Remote PED Firewall Blocking](#)" on the next page
- > "[Remote PED Blocked Port Access](#)" on page 275
- > "[ped connect Fails if IP is Not Accessible](#)" on page 275
- > "[PEDserver on VPN fails](#)" on page 275

### 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 261.

### 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 SafeNet 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 ("[hsm ped connect](#)" on page 1, "[ped connect](#)" on page 1):

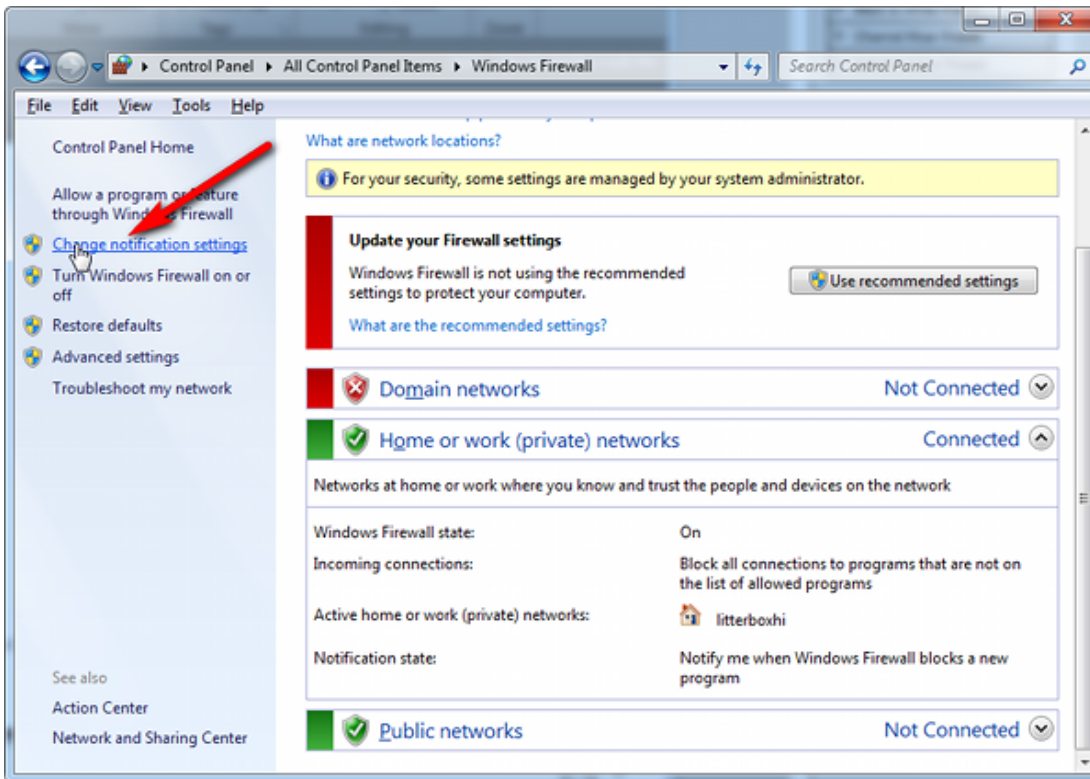
```
lunash:>hsm ped connect -ip <PEDserver_IP> -port <PEDserver_port>
```

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

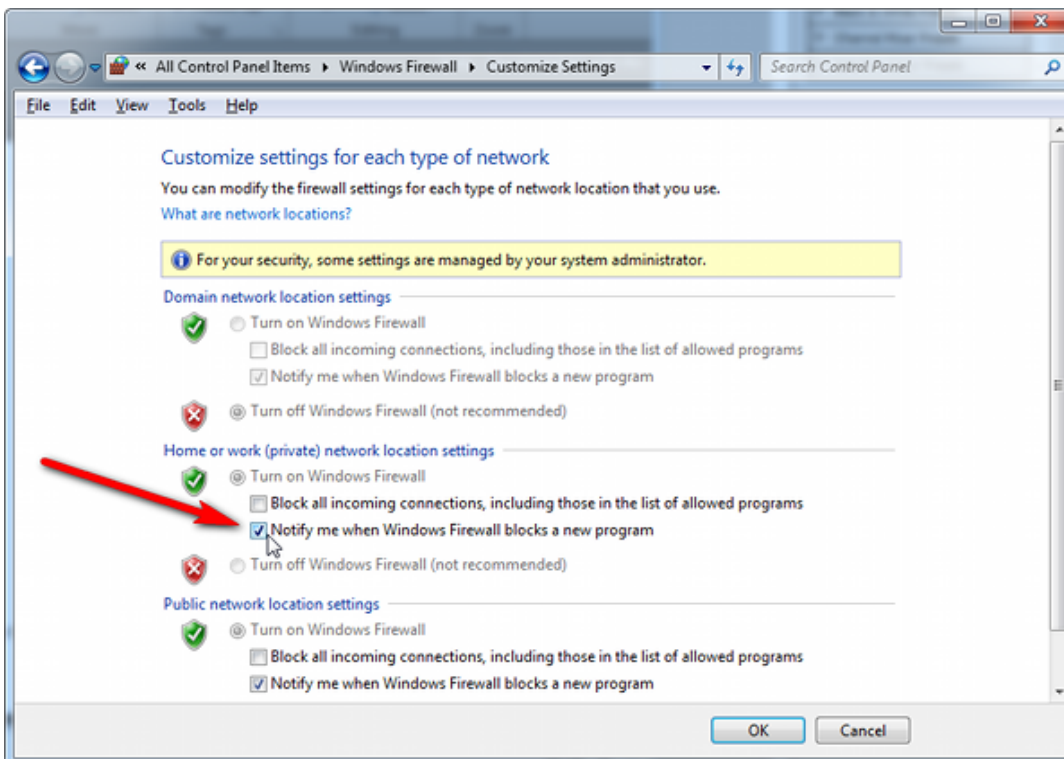
### Remote PED Firewall Blocking

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 267.

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 **ped connect** (LunaCM) or **hsm ped connect** (LunaSH) to initiate the Remote PED connection. Contact your network administrator for help.

You might choose to use a port-forwarding jump server, co-located with the SafeNet Luna 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 SafeNet 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 ("[hsm ped connect](#)" on page 1).  
`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 SafeNet 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 315).

>**pedserver -mode start -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 ("[service restart](#)" on page 1).

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.

## PED Key Management

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

- > "[Creating PED Keys](#)" below
  - "[Stage 1: Reusing Existing PED Keys](#)" on page 278
  - "[Stage 2: Defining M of N](#)" on page 279
  - "[Stage 3: Setting a PED PIN](#)" on page 280
  - "[Stage 4: Duplicating New PED Keys](#)" on page 281
- > "[Performing PED Authentication](#)" on page 281
- > "[Consequences of Losing PED Keys](#)" on page 283
- > "[Identifying a PED Key Secret](#)" on page 285
- > "[Duplicating Existing PED Keys](#)" on page 286
- > "[Changing a PED Key Secret](#)" on page 287

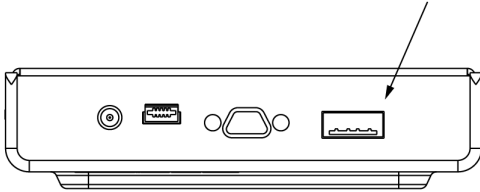
### Creating PED Keys

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

- > If you are reusing an existing PED key or keyset, the owners of those keys must be present with their keys and PED PINs ready.

- > If you plan to use an M of N authentication scheme (quorum, or split-secret), all the parties involved must be present and ready to create their authentication split. It is advisable for each key holder to create backup duplicates, so you must have a sufficient number of blank or rewritable PED keys ready before you begin.
- > If you plan to make backup duplicates of PED keys, you must have a sufficient number of blank or rewritable PED keys ready.
- > If you plan to use PED PINs, ensure that they can be privately entered on the Luna PED and memorized, or written down and securely stored.

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



### To initiate PED key creation

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

- **Blue HSM SO and Red HSM Domain Keys** ("[hsm init](#)" on page 1):

```
lunash:>hsm init
```

- **Orange Remote PED Key** ("[hsm ped vector init](#)" on page 1):

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

- **Blue Partition SO and Red Partition Domain Keys** ("[partition init](#)" on page 1):

```
lunacm:>partition init
```

- **Black Crypto Officer Key** ("[role init](#)" on page 1):

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

- **Gray Crypto User Key** ("[role init](#)" on page 1):

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

- **White Audit User Key** ("[audit init](#)" on page 1):

```
lunash:>audit init
```

The Luna PED responds, displaying:

```
Remote PED mode
Token found
```

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

### Stage 1: Reusing Existing PED Keys

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

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

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

See ["Shared PED Key Secrets" on page 246](#) and ["Domain PED Keys" on page 246](#) 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.
```

- 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](#)" on the next page for all the duplicate keys you want.

## Stage 2: Defining M of N

If you chose to create a new keyset, the Luna PED prompts you to define the M of N scheme (quorum and pool of splits) for the role, domain, or vector. See "[M of N Split Secrets \(Quorum\)](#)" on page 247 for more information. If you do not want to use M of N (authentication by one PED key), enter a value of **1** for both M and N.

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

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

>03
```

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

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

>05
```

- Continue to "[Stage 3: Setting a PED PIN](#)" on the next page. 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 247 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 283.

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:
█
```

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

#### Stage 4: Duplicating New PED Keys

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

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

You can make backups now or later. See also ["Duplicating Existing PED Keys"](#) on page 286.

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

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

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

- If you select **No**, the key creation process is complete.
  - If you select **Yes**, complete ["Stage 3: Setting a PED PIN"](#) on the previous page 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.
- If you specified an M of N scheme, you are prompted to repeat ["Stage 3: Setting a PED PIN"](#) on the previous page for each M of N split. Otherwise, the key creation process is complete.

## Performing PED Authentication

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

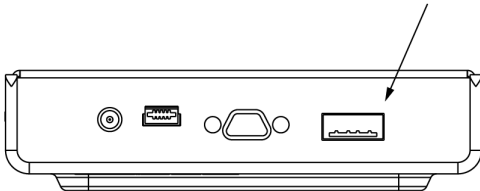
When you issue a command that requires PED interaction, the interface returns a message like the following:

```
lunash:>hsm login
```

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

```
Remote PED mode
Token found
```

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



**CAUTION!** Multiple failed authentication attempts result in zeroization of the HSM or partition, or role lockout, depending on the role. This is a security measure designed to thwart repeated, unauthorized attempts to access cryptographic material. For details, see ["Logging In as HSM Security Officer" on page 431](#) or ["Logging In to the Application Partition" on page 435](#).

## 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 SafeNet 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 285](#)
- > ["Gray Crypto User Key" on page 285](#)
- > ["White Audit User Key" on page 285](#)

### 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 \(RPV\) and Creating an Orange Remote PED Key \(RPK\)" on page 258](#).

### Blue Partition SO Key

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

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

### Red Partition Domain Key

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

1. Have the HSM SO create a new partition (or multiple partitions, to replace the entire HA group) and assign it to the same client(s).
2. Initialize the partition(s) with a new cloning domain.

3. Initialize the Crypto Officer role with the original black Crypto Officer key (and Activation password, if applicable).
4. Create objects on the new partition to replace those on the original partition.
5. As soon as possible, change all applications to use the objects on the new partition.
6. When objects on the original partition are no longer in production use, the HSM SO can delete the original partition.

### Black Crypto Officer Key

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

#### > PIN reset by Partition SO:

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

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

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

#### > Partition Activation:

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

#### > Crypto User

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

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

### Gray Crypto User Key

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

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

### White Audit User Key

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

## Identifying a PED Key Secret

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

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

- > who the key belongs to

You require:

- > SafeNet Luna PED in Admin Mode (see ["Changing Modes" on page 250](#))
- > 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:

- > SafeNet Luna PED in Admin Mode (see ["Changing Modes" on page 250](#))
- > 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 247](#).

### 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 289](#)
- > ["Black Crypto Officer Key" on page 289](#)
- > ["Gray Crypto User Key" on page 289](#)
- > ["White Audit User Key" on page 289](#)

### 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 ("[hsm login](#)" on page 1).  
lunash:>**hsm login**
2. Initiate the PED key change ("[hsm changepw](#)" on page 1).  
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 276.

### 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 ("[hsm login](#)" on page 1).  
lunash:>**hsm login**
2. Initialize the RPV ("[hsm ped vector init](#)" on page 1).  
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 ("[role login](#)" on page 1).  
lunacm:>**role login -name po**
2. Initiate the PED key change ("[role changepw](#)" on page 1).  
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 ("[role login](#)" on page 1).  
lunacm:>**role login -name co**
2. Initiate the PED key change ("[role changepw](#)" on page 1).  
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 ("[role login](#)" on page 1).  
lunacm:>**role login -name cu**
2. Initiate the PED key change ("[role changepw](#)" on page 1).  
lunacm:>**role changepw -name cu**
3. You are prompted to present the original gray key(s) and then to create a new Crypto User keyset.

### White Audit User Key

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

---

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

1. Log into LunaSH as **audit**.
2. Log in as the Audit User ("[audit login](#)" on page 1).  
lunash:>**audit login**
3. Initiate the PED key change ("[audit changepwd](#)" on page 1).  
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 SafeNet Luna Network HSM) is behind a firewall that forbids outgoing initiation of connections.

See ["pedserver" on page 303](#).

## The PEDclient Utility

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

The PEDclient utility performs the following functions:

- > It mediates between the HSM where it is installed and the Luna PED where PEDserver is installed, to provide PED services to the requesting HSM(s).
- > It resides on a computer with RBS and an attached SafeNet Luna Backup HSM, and it connects with another instance of PEDclient on a distant host of an HSM, to provide the link component for Remote Backup Service. See ["Configuring a Remote Backup HSM Server" on page 74](#) for more information.
- > It acts as the logging daemon for HSM audit logs.

**NOTE** PEDclient exists on the SafeNet Luna Network HSM appliance, but is not directly exposed. Instead, the relevant features are accessed via LunaSH **hsm ped** commands. See ["hsm ped" on page 1](#) in the *LunaSH Command Reference Guide*.

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 Backup HSM Server" on page 74](#) in the *Administration Guide* for more information.

See ["pedclient" below](#).

## 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 293</a> .                   |
| <b>deleteid</b>  | Deletes a PED ID mapping. See <a href="#">"pedclient mode deleteid" on page 295</a> .                                               |
| <b>releaseid</b> | Releases a PED ID mapping from an HSM. See <a href="#">"pedclient mode releaseid" on page 296</a> .                                 |
| <b>setid</b>     | Creates a PED ID mapping. See <a href="#">"pedclient mode setid" on page 297</a> .                                                  |
| <b>show</b>      | Queries if PEDclient is currently running and gets details about PEDclient. See <a href="#">"pedclient mode show" on page 298</a> . |
| <b>start</b>     | Starts up PEDclient. See <a href="#">"pedclient mode start" on page 299</a> .                                                       |
| <b>stop</b>      | Shuts down PEDclient. See <a href="#">"pedclient mode stop" on page 301</a> .                                                       |
| <b>testid</b>    | Tests a PED ID mapping. See <a href="#">"pedclient mode testid" on page 302</a> .                                                   |

## pedclient mode assignid

Assigns a PED ID mapping to a specified HSM.

### Syntax

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

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

### Example

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

## pedclient mode config

Modifies or shows existing configuration file settings.

### Syntax

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

| Option                           | Description                                                                                                                                          |
|----------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>-show</b>                     | Displays the contents of the configuration file.                                                                                                     |
| <b>-set</b>                      | Updates the configuration file to be up to date with other supplied options.                                                                         |
| <b>-eadmin</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>-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</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.                                                           |

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

## Example

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

## pedclient mode deleteid

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

### Syntax

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

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

### Example

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

## pedclient mode releaseid

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

### Syntax

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

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

### Example

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



## pedclient mode setid

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

### Syntax

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

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

### Example

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

## pedclient mode show

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

### Syntax

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

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

### Example

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

## pedclient mode start

Starts up the PED Client.

### Syntax

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

| Option                                 | Description                                                                                                                                                         |
|----------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>-winservice</b>                     | Starts PEDclient for Windows service. The standard parameters used for <b>pedclient mode start</b> can be used for <b>pedclient mode start -winservice</b> as well. |
| <b>-eadmin &lt;0 or 1&gt;</b>          | Optional. Specifies if the administration port is on "localhost" or on the external host name.                                                                      |
| <b>-idletimeout &lt;int&gt;</b>        | Optional. Specifies the idle connection timeout, in seconds.                                                                                                        |
| <b>-socketreadtimeout &lt;int&gt;</b>  | Optional. Specifies the socket read timeout, in seconds.                                                                                                            |
| <b>-socketwritetimeout &lt;int&gt;</b> | Optional. Specifies the socket write timeout, in seconds.                                                                                                           |
| <b>-shutdowntimeout &lt;int&gt;</b>    | Optional. Specifies the shutdown timeout for internal services, in seconds.                                                                                         |
| <b>-pstartuptimeout &lt;int&gt;</b>    | Optional. Specifies the startup timeout for the detached process, in seconds.                                                                                       |
| <b>-pshutdowntimeout &lt;int&gt;</b>   | Optional. Specifies the shutdown timeout for the detached process, in seconds.                                                                                      |
| <b>-logfilename &lt;filename&gt;</b>   | Optional. Specifies the log file name to which the logger should log messages.                                                                                      |
| <b>-loginfo &lt;0 or 1&gt;</b>         | Optional. Specifies if the logger should log "info" messages. Set to 0 for no, 1 for yes.                                                                           |
| <b>-logwarning &lt;0 or 1&gt;</b>      | Optional. Specifies if the logger should log "warning" messages. Set to 0 for no, 1 for yes.                                                                        |
| <b>-logerror &lt;0 or 1&gt;</b>        | Optional. Specifies if the logger should log "error" messages. Set to 0 for no, 1 for yes.                                                                          |
| <b>-logtrace &lt;0 or 1&gt;</b>        | Optional. Specifies if the logger should log "trace" messages. Set to 0 for no, 1 for yes.                                                                          |
| <b>-maxlogfilesize &lt;size&gt;</b>    | Optional. Specifies the maximum log file size in KB.                                                                                                                |
| <b>-locallogger</b>                    | Optional. Specifies that the Remote PED logger should be used, not the IS logging system.                                                                           |

## Example

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

## pedclient mode stop

Shuts down PEDclient.

### Syntax

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

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

### Example

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

## pedclient mode testid

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

### Syntax

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

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

### Example

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

## pedserver

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

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

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

### Syntax

#### pedserver

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

| Option           | Description                                                                                                                                                                                   |
|------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>appliance</b> | Registers or deregisters an appliance, or lists the registered appliances. Applies to server-initiated (peer-to-peer) mode only. See <a href="#">"pedserver appliance" 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 308</a> .                                                                                |
| <b>regen</b>     | Regenerates the client certificate. Applies to server-initiated (peer-to-peer) mode only. See <a href="#">"pedserver regen" on page 319</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 306. |
| <b>register</b> | Registers an appliance. See " <a href="#">pedserver appliance register</a> " on page 307       |



## 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).<br><b>Range:</b> 0-65525 |

### Example

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

## pedserver mode

Specifies the mode that PEDserver will be executed in.

### Syntax

#### pedserver mode

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

| Option            | Description                                                                                                                           |
|-------------------|---------------------------------------------------------------------------------------------------------------------------------------|
| <b>config</b>     | Modifies or shows existing configuration file settings. See " <a href="#">pedserver mode config</a> " on the next page.               |
| <b>connect</b>    | Connects to the appliance. See " <a href="#">pedserver mode connect</a> " on page 311.                                                |
| <b>disconnect</b> | Disconnects from the appliance. See " <a href="#">pedserver mode disconnect</a> " on page 312.                                        |
| <b>show</b>       | Queries if PEDserver is currently running, and gets details about PEDserver. See " <a href="#">pedserver mode show</a> " on page 313. |
| <b>start</b>      | Starts PEDserver. See " <a href="#">pedserver mode start</a> " on page 315.                                                           |
| <b>stop</b>       | Shuts down PEDserver. See " <a href="#">pedserver mode stop</a> " on page 317                                                         |

## 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 SafeNet Luna HSM Client installed. When SafeNet Luna HSM Client is installed on the host computer, use the LunaCM command **clientconfig deploy** with the **-regen** option (see "[clientconfig deploy](#)" on page 1 in the *LunaCM Command Reference Guide*) or, if necessary, **vtl createcert** (see "[vtl createCert](#)" on page 1 in the *Utilities Reference Guide*).

### Syntax

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

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

### Example

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

```
Private Key created and written to: C:\Program Files\SafeNet\LunaClient\cert\client\win2016_
serverKey.pem
```

```
Certificate created and written to: C:\Program Files\SafeNet\LunaClient\cert\client\win2016_
server.pem
```

Successfully regenerated the client certificate.

# CHAPTER 16: Performance Monitoring

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

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

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

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

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

By watching trends and correlating with what your application is doing, you can:

- > Determine the kinds of loads you are placing on the HSM.
- > Seek efficiencies in how your applications are coded and configured.
- > Plan for expansion or upgrades of your existing HSM infrastructure.
- > Plan for upgrades of electrical capacity and HVAC capacity.

## Notes about Monitor/Counter Behavior

When performing certain operations the HSM reaches its maximum performance capability before the counter reaches 100%. This occurs because the counter measures the load on the HSM's CPU and the CPU is able to saturate the asymmetric engines and still have capacity to perform other actions.

Also, symmetric cryptographic operations cause the counter to quickly rise to 90% even though there is significant remaining capacity. This behavior occurs because, as the HSM receives more concurrent symmetric commands, its CPU is able to handle them more efficiently (by performing them in bulk) – thus achieving more throughput from the same number of CPU cycles.

See "[hsm information](#)" on page 1 in the *LunaSH Reference Guide*.



# CHAPTER 17: Security in Operation

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

- > ["Client to HSM Security Best Practices" below](#)
- > ["Security Effects of Administrative Actions" on the next page](#)
- > ["Security of Your Partition Challenge" on page 326](#)

## Client to HSM Security Best Practices

---

While the SafeNet 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 SafeNet Luna HSM Client directory, on every system that connects to an application partition on a SafeNet 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)

## Security Effects of Administrative Actions

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

### Overt Security Actions

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

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

Those are discussed in their own sections.

### Actions with Security- and Content-Affecting Outcomes

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

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

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

#### Factory Reset HSM

|        |           |
|--------|-----------|
| Domain | Destroyed |
|--------|-----------|

|                                  |                                                                                                                                                         |
|----------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>HSM SO Role</b>               | Destroyed                                                                                                                                               |
| <b>Partition SO Role</b>         | Destroyed                                                                                                                                               |
| <b>Auditor Role</b>              | Destroyed                                                                                                                                               |
| <b>Partition Roles</b>           | Destroyed                                                                                                                                               |
| <b>HSM or Partition/Contents</b> | HSM/Destroyed                                                                                                                                           |
| <b>HSM Policies</b>              | Reset                                                                                                                                                   |
| <b>RPV</b>                       | Destroyed                                                                                                                                               |
| <b>Messaging</b>                 | You are about to factory reset the HSM. All contents of the HSM will be destroyed. HSM policies will be reset and the remote PED vector will be erased. |

### Zeroize HSM

|                                  |                                                                                                                                          |
|----------------------------------|------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Domain</b>                    | Destroyed                                                                                                                                |
| <b>HSM SO Role</b>               | Destroyed                                                                                                                                |
| <b>Partition SO Role</b>         | Destroyed                                                                                                                                |
| <b>Auditor Role</b>              | Unchanged                                                                                                                                |
| <b>Partition Roles</b>           | Destroyed                                                                                                                                |
| <b>HSM or Partition/Contents</b> | HSM/Destroyed                                                                                                                            |
| <b>HSM Policies</b>              | Unchanged                                                                                                                                |
| <b>RPV</b>                       | Unchanged                                                                                                                                |
| <b>Messaging</b>                 | You are about to zeroize the HSM. All contents of the HSM will be destroyed. HSM policies, remote PED vector and Auditor left unchanged. |

### Change Destructive HSM Policy

|                    |           |
|--------------------|-----------|
| <b>Domain</b>      | Unchanged |
| <b>HSM SO Role</b> | Unchanged |

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

### HSM Initialize When Zeroized (hard init)

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

### HSM Initialize From Non-Zeroized State (soft init)

|                          |           |
|--------------------------|-----------|
| <b>Domain</b>            | Unchanged |
| <b>HSM SO Role</b>       | Unchanged |
| <b>Partition SO Role</b> | Destroyed |
| <b>Auditor Role</b>      | Unchanged |

|                                  |                                                                                                                                                                    |
|----------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Partition Roles</b>           | Destroyed                                                                                                                                                          |
| <b>HSM or Partition/Contents</b> | HSM/Destroyed                                                                                                                                                      |
| <b>HSM Policies</b>              | Unchanged                                                                                                                                                          |
| <b>RPV</b>                       | Unchanged                                                                                                                                                          |
| <b>Messaging</b>                 | You are about to initialize the HSM that is already initialized. All partitions of the HSM will be destroyed. You are required to provide the current SO password. |

### HSM Firmware Rollback

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

### Partition Initialize When Zeroized (hard init)

|                          |           |
|--------------------------|-----------|
| <b>Domain</b>            | Unchanged |
| <b>HSM SO Role</b>       | Unchanged |
| <b>Partition SO Role</b> | Destroyed |

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

### Partition Initialize From Non-Zeroized State (soft init)

|                                  |                                                                                                                                                                                        |
|----------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Domain</b>                    | Unchanged                                                                                                                                                                              |
| <b>HSM SO Role</b>               | Unchanged                                                                                                                                                                              |
| <b>Partition SO Role</b>         | Destroyed                                                                                                                                                                              |
| <b>Auditor Role</b>              | Unchanged                                                                                                                                                                              |
| <b>Partition Roles</b>           | Destroyed                                                                                                                                                                              |
| <b>HSM or Partition/Contents</b> | Partition/Destroyed                                                                                                                                                                    |
| <b>HSM Policies</b>              | Unchanged                                                                                                                                                                              |
| <b>RPV</b>                       | Unchanged                                                                                                                                                                              |
| <b>Messaging</b>                 | You are about to initialize the partition that is already initialized. All contents of the partition will be destroyed. You are required to provide the current Partition SO password. |

### Elsewhere

Certain other actions can sometimes cause collateral changes to the HSM, like firmware update. They usually do not affect contents, unless a partition is full and the action changes the size of partitions or changes the amount of space-per-partition that is taken by overhead/infrastructure. These are discussed elsewhere.

## Security of Your Partition Challenge

For SafeNet 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 SafeNet 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 SafeNet 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 SafeNet Luna HSM Client computer. For interaction with HSM partitions on a SafeNet network appliance, like SafeNet Luna Network HSM, a SafeNet Luna HSM Client computer is one with SafeNet 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 SafeNet Luna HSM partition - an authorized person within your organization must participate.

**Second**, for SafeNet 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 SafeNet 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](#)" on page 1 of the *LunaCM Command Reference Guide* 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**, SafeNet 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 "[Logging In to the Application Partition](#)" on page 435 for more information.

As the owner/administrator of the HSM, you determine any tradeoffs with respect to security, convenience, and other operational parameters.

# CHAPTER 18: Secure Transport Mode

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

## Secure Transport Mode overview

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

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

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

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

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

## How does Secure Transport Mode work?

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

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



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

### When you recover an HSM from STM:

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

### STM verification email

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

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

For information about the various tamper events, see ["Tamper Events" on page 348](#).

For command syntax, see ["hsm stm" on page 1](#).

## Placing an HSM Into Secure Transport Mode

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

**CAUTION!** If the HSM contains sensitive key material, ensure that you have a full backup of the HSM contents before proceeding.

### To place an HSM into Secure Transport Mode:

1. Log in as the HSM SO.

2. Backup the HSM contents.

See "[Backup and Restore Using a G5-Based Backup HSM](#)" on page 53 for details.

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

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

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

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

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

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

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

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

## Recovering an HSM From Secure Transport Mode

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

### New HSMs

New HSMs are shipped from the factory in Secure Transport Mode (STM). You must recover from STM before you can initialize the HSM.

As part of the delivery of your new HSM, you should have received an email from Thales Client Services containing two 16-digit strings:

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

> Verification String: XXXX-XXXX-XXXX-XXXX

### To recover an HSM from STM

1. Ensure that you have the two strings that were presented when the HSM was placed into STM, or that were emailed to you if this is a new HSM.
2. If the HSM is initialized, log in as the HSM SO. If this is a new or zeroized HSM, skip to the next step.
3. Enter the following command to recover from STM, using the random user string that was displayed when the HSM was placed in STM, or that was emailed to you if this is a new HSM.:

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

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

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

4. You are presented with a verification string:

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

Enter **proceed** to recover from STM.

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

### If the verification strings do not match

1. Reconfirm that you have entered the correct random user string for your HSM.
2. If the verification strings still do not match:
 

If this is a new HSM, type "quit" to leave the HSM in Secure Transport Mode, and contact Gemalto Technical Support.

Otherwise,

  - If you feel that the Verification failure was benign, type "proceed" to release the HSM from Secure Transport Mode, and decide to either:
    - proceed with using the HSM
    - perform a factory reset and re-initialize the HSM as a safety precaution before proceeding further.

# CHAPTER 19: 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 SafeNet library.

## Order of Occurrence for Different SafeNet Luna HSMs

A host computer with SafeNet Luna HSM Client software and SafeNet libraries installed can have SafeNet Luna HSMs connected in any of three ways:

- > PCIe embedded/inserted SafeNet Luna PCIe HSM card (one or multiple HSMs installed - administrative partitions and application partitions are shown separately)
- > USB-connected SafeNet Luna USB HSMs (one or multiple - administrative partitions and application partitions are shown separately)
- > SafeNet 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 SafeNet 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 SafeNet 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:

- > SafeNet Luna Network HSM application partitions for which NTLS links are established with the current host, followed by
- > SafeNet Luna PCIe HSM cards, followed by
- > SafeNet Luna USB HSMs

For SafeNet Luna Network HSM, as seen from a client (via NTLS), only application partitions are visible. The HSM administrative partition of a remote SafeNet Luna Network HSM is never seen by a SafeNet Luna HSM Client. The SafeNet Luna Network HSM slots are listed in the order they are polled, dictated by the entries in the **SafeNet 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 SafeNet Luna PCIe HSM and SafeNet 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 SafeNet Luna PCIe HSM and SafeNet 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 SafeNet 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 SafeNet 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 (SafeNet Luna Network HSM) are not affected by this setting, because NTLS connects only application partitions, not HSM SO (Admin) partitions to clients, so a SafeNet 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.

# CHAPTER 20: SNMP Monitoring

This chapter describes Simple Network Management Protocol (SNMP v3) support for remote monitoring of conditions on a local HSM that might require administrative attention. It contains the following sections:

- > ["Overview and Installation" below](#)
- > ["The SafeNet Chrysalis-UTSP MIB" on page 337](#)
- > ["The SafeNet Luna HSM MIB" on page 338](#)
- > ["The SafeNet Appliance MIB" on page 344](#)
- > ["SNMP Operation and Limitations with SafeNet Luna Network HSM" on page 344](#)
- > ["Frequently Asked Questions" on page 346](#)

## Overview and Installation

This section provides an overview of the SNMP implementation and describes how to install the SNMP subagent.

### MIB

Thales Group provides the following MIBs (management information base) in the SafeNet Luna HSM Client installation package:

| MIB Name                  | Description                                                         |
|---------------------------|---------------------------------------------------------------------|
| CHRYSALIS-UTSP-MIB.txt    | Defines SNMP access to information about the SafeNet appliance.     |
| SAFENET-HSM-MIB.txt       | Defines SNMP access to information about the SafeNet Luna HSM.      |
| SAFENET-GLOBAL-MIB.txt    | Must be found in your system path so that symbols can be resolved.  |
| SAFENET-APPLIANCE-MIB.txt | Reports the software version of SafeNet Luna Network HSM appliance. |

Copy all MIBs in `<Luna_HSM_Client_install_dir>/snmp` to the MIB directory on your system. Only the MIBs necessary for SafeNet Luna PCIe HSM and SafeNet Luna USB HSM are included in a client installation.

For SafeNet Luna Network HSM, the host is the appliance, so all the above MIBs are installed on the appliance. See ["Traps" on page 1](#) in the *Syslog and SNMP Monitoring Guide* for information on configuring SNMP trap notifications.

**NOTE** Your SNMP application also requires the following standard SNMP MIBs:

- > **SNMPv2-SMI.txt** -- defined in RFC 2578, Section 2
- > **SNMPv2-TC.txt** -- defined in RFC 2579, Section 2

## SafeNet SNMP Subagent

We find that most customers choosing to use SNMP already have an SNMP infrastructure in place. Therefore, we provide a subagent that you can install on your managed workstations, and which can point to your agent via the socket created by the agent. This applies to SafeNet Luna USB HSM and SafeNet Luna PCIe HSM - for SafeNet Luna Network HSM, the subagent is already on the appliance.

The SNMP subagent (`luna-snmp`) is an AgentX SNMP module that extends an existing SNMP agent with support for SafeNet Luna HSM monitoring. It is an optional component of the SafeNet Luna HSM Client installation. The subagent has been tested against `net-snmp`, but should work with any SNMP agent that supports the AgentX protocol.

### To install the SNMP subagent:

After selecting one or more products from the main SafeNet Luna HSM Client installation menu, you are presented with a list of optional components, including the SNMP subagent. It is not selected by default, but can be installed with any product except the SafeNet Luna Network HSM client installed in isolation.

1. In the installation media, go to the appropriate folder for your operating system.
2. Run the installer (`install.sh` for Linux and UNIX, `LunaHSMClient.exe` for Windows).
3. Choose the SafeNet products that you wish to install, and include SNMP among your selections. The subagent is installed for any SafeNet product except SafeNet Luna Network HSM in isolation.
4. Proceed to Post-installation configuration.

### Post-installation configuration

After the SafeNet Luna HSM Client is installed, complete the following steps to configure the SNMP subagent:

1. Copy the SafeNet MIBs from `<install dir>/snmp` to the main SNMP agent's MIB directory. Or copy to another computer (your SNMP computer) if you are not running SNMP from the same computer where SafeNet Luna HSM Client software is installed.
2. If running on Windows, configure the subagent via the file `<install dir>/snmp/luna-snmp.conf` to point to the AgentX port where the main SNMP agent is listening. The file must then be copied to the same directory as `snmpd.conf`. (This assumes `net-snmp` is installed; the setup might differ if you have another agent.)

If running on a UNIX-based platform, the subagent should work without extra configuration assuming that the primary SNMP agent is listening on the default local socket (`/var/agentx/master`). You still have the option of editing and using `luna-snmp.conf`.

3. After configuration is complete, start the agent. Then start the subagent via the service tool applicable to your platform (for example, **service luna-snmp start** on Linux, or start SafeNet SNMP Subagent Service from the services in Windows).

Normally the agent is started first. However, the subagent periodically attempts to connect to the agent until it is successful. The defaults controlling this behavior are listed below. They can be overridden by changing the appropriate entries in **luna-snmp.conf**.

### Troubleshooting

If you encounter the following warning:

**Warning: Failed to connect to the agentx master agent ([NIL]):**



you must enable AgentX support by adding **master agentx** to your SNMPD configuration file. Refer to the man page for **snmpd.conf** for more information.

## Configuration Options In the luna-snmp.conf File

| Option                                                            | Description                                                                                                                                                                                                                                                                                                                                                                                                                                            | Default                                                                                                                                                                                |
|-------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| agentXSocket<br>[<transport-specifier>:]<transport-address>[,...] | Defines the address to which the subagent should connect. The default on UNIX-based systems is the Unix Domain socket <code>"/var/agentx/master"</code> .<br>Another common alternative is <code>tcp:localhost:705</code> .<br>See the section LISTENING ADDRESSES in the snmpd man page for more information about the format of addresses ( <a href="http://www.net-snmp.org/docs/man/snmpd.html">http://www.net-snmp.org/docs/man/snmpd.html</a> ). | The default, for Linux, is <code>"/var/agentx/master"</code> .<br>In the file, you can choose to un-comment <code>"tcp:localhost:705"</code> which is most commonly used with Windows. |
| agentXPingInterval<br><NUM>                                       | Makes the subagent try to reconnect every <NUM> seconds to the master if it ever becomes (or starts) disconnected.                                                                                                                                                                                                                                                                                                                                     | 15                                                                                                                                                                                     |
| agentXTimeout <NUM>                                               | Defines the timeout period (NUM seconds) for an AgentX request.                                                                                                                                                                                                                                                                                                                                                                                        | 1                                                                                                                                                                                      |
| agentXRetries <NUM>                                               | Defines the number of retries for an AgentX request.                                                                                                                                                                                                                                                                                                                                                                                                   | 5                                                                                                                                                                                      |

## The SafeNet Chrysalis-UTSP MIB

**NOTE** The Chrysalis MIB is the SafeNet MIB for all SafeNet Luna HSM products - the Chrysalis name is retained for historical continuity.

To illustrate accessing data, the command `"snmpwalk -v 3 -u admin -l authPriv -a SHA1 -A 12345678 -x AES -X 87654321 myLuna19 private"` produced this output:

- > CHRYSALIS-UTSP-MIB::hsmOperationRequests.0 = Counter64: 3858380
- > CHRYSALIS-UTSP-MIB::hsmOperationErrors.0 = Counter64: 385838
- > CHRYSALIS-UTSP-MIB::hsmCriticalEvents.0 = Counter64: 0
- > CHRYSALIS-UTSP-MIB::hsmNonCriticalEvents.0 = Counter64: 5
- > CHRYSALIS-UTSP-MIB::ntIsOperStatus.0 = INTEGER: up(1)
- > CHRYSALIS-UTSP-MIB::ntIsConnectedClients.0 = Gauge32: 0
- > CHRYSALIS-UTSP-MIB::ntIsLinks.0 = Gauge32: 0
- > CHRYSALIS-UTSP-MIB::ntIsSuccessfulClientConnections.0 = Counter64: 16571615927115620
- > CHRYSALIS-UTSP-MIB::ntIsFailedClientConnections.0 = Counter64: 1657161592711562

The various counts are recorded since the last restart.

| Item                            | Description                                                                                                                                                                                                                       |
|---------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| hsmOperationRequests            | The total number of HSM operations that have been requested.                                                                                                                                                                      |
| hsmOperationErrors              | The total number of HSM operations that have been requested, that have resulted in errors.                                                                                                                                        |
| hsmCriticalEvents               | The total number of critical HSM events that have been detected (Tamper, Decommission, Zeroization, SO creation, or Audit role creation).<br><br><b>NOTE</b> Not implemented in this release. hsmCriticalEvents always reports 0. |
| hsmNonCriticalEvents            | The total number of NON-critical HSM events that have been detected (any that are not among the critical list, above).<br><br><b>NOTE</b> Not implemented in this release. hsmNonCriticalEvents always reports 0.                 |
| ntlsOperStatus                  | The current operational status of the NTL service, where the options are:<br>1 = up,<br>2 = not running, and<br>3 = status cannot be determined.                                                                                  |
| ntlsConnectedClients            | The current number of connected clients using NTLS.                                                                                                                                                                               |
| ntlsLinks                       | The current number of links in NTLS - can be multiple per client, depending on processes.                                                                                                                                         |
| ntlsSuccessfulClientConnections | The total number of successful client connections.                                                                                                                                                                                |
| ntlsFailedClientConnections     | The total number of UNSuccessful client connections.                                                                                                                                                                              |

## The SafeNet Luna HSM MIB

The SAFENET-HSM-MIB defines HSM status information and HSM Partition information that can be viewed via SNMP.

To access tables, use a command like:

```
snmptable -a SHA -A snmppass -u snmpuser -x AES -X snmppass -l authPriv -v 3 192.20.11.59
SAFENET-HSM-MIB:hsmTable
```

The information is defined in tables, as detailed in the following sections.

### SNMP Table Updates

The SNMP tables are updated and cached every 60 seconds. Any changes made on the HSM may therefore take up to 60 seconds to be included in the tables. When a query is received to view the tables, the most recent cached version is displayed. If a change you were expecting is not displayed, wait 60 seconds and try again.

**NOTE** Some values may not get updated automatically, such as the HSM firmware version (hsmFirmwareVersion) following a firmware upgrade. To force an update, restart the SNMP agent.

## hsmTable

This table provides a list of all the HSM information on the managed element.

| Item                     | Type          | Description                                                  | Values                                                                                                                 |
|--------------------------|---------------|--------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------|
| hsmSerialNumber          | DisplayString | Serial number of the HSM - used as an index into the tables. | From factory                                                                                                           |
| hsmFirmwareVersion       | DisplayString | Version of firmware executing on the HSM.                    | As found                                                                                                               |
| hsmLabel                 | DisplayString | Label associated with the HSM.                               | Provided by SO at init time                                                                                            |
| hsmModel                 | DisplayString | Model identifier for the HSM.                                | From factory                                                                                                           |
| hsmAuthenticationMethod  | INTEGER       | Authentication mode of the HSM.                              | unknown(1), -- not known<br>password(2), -- requires passwords<br>pedKeys(3) -- requires PED                           |
| hsmRpvInitialized        | INTEGER       | Remote ped vector initialized flag of the HSM.               | notSupported(1), -- rpv not supported<br>uninitialized(2), -- rpv not initialized<br>initialized(3) -- rpv initialized |
| hsmFipsMode              | TruthValue    | FIPS 140-2 operation mode enabled flag of the HSM.           | Factory set                                                                                                            |
| hsmPerformance           | INTEGER       | Performance level of the HSM.                                |                                                                                                                        |
| hsmStorageTotalBytes     | Unsigned32    | Total storage capacity in bytes of the HSM                   | Factory set                                                                                                            |
| hsmStorageAllocatedBytes | Unsigned32    | Number of allocated bytes on the HSM                         | Calculated                                                                                                             |
| hsmStorageAvailableBytes | Unsigned32    | Number of available bytes on the HSM                         | Calculated                                                                                                             |

| Item                    | Type       | Description                                                            | Values                                        |
|-------------------------|------------|------------------------------------------------------------------------|-----------------------------------------------|
| hsmMaximumPartitions    | Unsigned32 | Maximum number of partitions allowed on the HSM                        | 2, 5, 10, 15, or 20, per license              |
| hsmPartitionsCreated    | Unsigned32 | Number of partitions created on the HSM                                | As found                                      |
| hsmPartitionsFree       | Unsigned32 | Number of partitions that can still be created on the HSM              | Calculated                                    |
| hsmBackupProtocol       | INTEGER    | Backup protocol used on the HSM                                        | unknown(1), none(2), cloning(3), keyExport(4) |
| hsmAdminLoginAttempts   | Counter32  | Number of failed Administrator login attempts left before HSM zeroized | As found, calculated                          |
| hsmAuditRoleInitialized | INTEGER    | Audit role is initialized flag                                         | notSupported(0), yes(1), no(2)                |
| hsmManuallyZeroized     | TruthValue | Was HSM manually zeroized flag                                         | As found                                      |
| hsmUpTime               | Counter64  | Up time in seconds since last HSM reset                                | Counted                                       |
| hsmBusyTime             | Counter64  | Busy time in seconds since the last HSM reset                          | Calculated                                    |
| hsmCommandCount         | Counter64  | HSM commands processed since last HSM reset                            | Counted                                       |

### The hsmPartitionTable

This table provides a list of all the partition information on the managed element.

| Item                          | Type          | Description                                      | Values                                             |
|-------------------------------|---------------|--------------------------------------------------|----------------------------------------------------|
| hsmPartitionSerialNumber      | DisplayString | Serial number for the partition                  | Generated                                          |
| hsmPartitionLabel             | DisplayString | Label assigned to the partition                  | Provided at partition creation                     |
| hsmPartitionActivated         | TruthValue    | Partition activation flag                        | Set by policy                                      |
| hsmPartitionStorageTotalBytes | Unsigned32    | Total storage capacity in bytes of the partition | Set or calculated at partition creation or re-size |

| Item                              | Type       | Description                                         | Values     |
|-----------------------------------|------------|-----------------------------------------------------|------------|
| hsmPartitionStorageAllocatedBytes | Unsigned32 | Number of allocated (in use) bytes on the partition | Calculated |
| hsmPartitionStorageAvailableBytes | Unsigned32 | Number of available (unused) bytes on the partition | Calculated |
| hsmPartitionObjectCount           | Unsigned32 | Number of objects in the partition                  | Counted    |

## hsmLicenseTable

This table provides a list of all the license information on the managed element. More than one HSM might be connected to a Host, so they are accessed with two indices; the first index identifies the HSM for which the license entry corresponds (hsmSerialNumber), the second is the index for the corresponding license (hsmLicenseID).

| Item                  | Type          | Description         | Values                                 |
|-----------------------|---------------|---------------------|----------------------------------------|
| hsmLicenseID          | DisplayString | License identifier  | Set at factory or at capability update |
| hsmLicenseDescription | DisplayString | License description | Set at factory or at capability update |

## hsmPolicyTable

This table provides a list of all the HSM policy information on the managed element.

| Item                 | Type          | Description                 | Values                                                                       |
|----------------------|---------------|-----------------------------|------------------------------------------------------------------------------|
| hsmPolicyType        | INTEGER       | Type of policy              | capability(1),<br>policy(2)                                                  |
| hsmPolicyID          | Unsigned32    | Policy identifier           | Numeric value identifies policy and is used as a index into the policy table |
| hsmPolicyDescription | DisplayString | Description of the policy   | Brief text description of what the policy does                               |
| hsmPolicyValue       | DisplayString | Current value of the policy | Brief text description to show current state/value of policy                 |

## hsmPartitionPolicyTable

This table provides a list of all the partition policy information on the managed element.

| Item                          | Type          | Description                 | Values                                                                       |
|-------------------------------|---------------|-----------------------------|------------------------------------------------------------------------------|
| hsmPartitionPolicyType        | INTEGER       | Capability or policy        | capability(1), policy(2)                                                     |
| hsmPartitionPolicyID          | Unsigned32    | Policy identifier           | Numeric value identifies policy and is used as a index into the policy table |
| hsmPartitionPolicyDescription | DisplayString | Description of the policy   | Brief text description of what the policy does                               |
| hsmPartitionPolicyValue       | DisplayString | Current value of the policy | Brief text description to show current state/value of policy                 |

### hsmClientRegistrationTable

This table provides a list of registered clients.

| Item                 | Type          | Description                                    | Values                                                                                                                                                                                                                          |
|----------------------|---------------|------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| hsmClientName        | DisplayString | Name of the client                             | Name provided on client cert                                                                                                                                                                                                    |
| hsmClientAddress     | DisplayString | Address of the client                          | IP address of the client                                                                                                                                                                                                        |
| hsmClientRequiresHTL | TruthValue    | Flag specifying if HTL required for the client | Flag set at HSM host side to control client access<br><b>Note:</b> HTL is not available in release 7.x. This value will always return <b>false</b> for 7.x HSMs.                                                                |
| hsmClientOTTEpiry    | INTEGER       | OTT expiry time (-1 if not provisioned)        | Expiry time, in seconds, for HTL OneTimeToken (range is 0-3600); -1 indicates not provisioned, 0 means never expires<br><b>Note:</b> HTL is not available in release 7.x. This value will always return <b>-1</b> for 7.x HSMs. |

### hsmClientPartitionAssignmentTable

This table provides a list of assigned partitions for a given client.

| Item                           | Type          | Description                    | Values |
|--------------------------------|---------------|--------------------------------|--------|
| hsmClientHsmSerialNumber       | DisplayString | Index into the HSM table       | --     |
| hsmClientPartitionSerialNumber | DisplayString | Index into the Partition Table | --     |

## SNMP output compared to SafeNet tools output

For comparison, the following shows LunaCM or LunaSH command outputs that provide HSM information equivalent to the SNMP information depicted in the tables above (from the HSM MIB).

### HSM Information

At the HSM level the information in the outputs of **hsm show** and **hsm showpolicies** and **hsm displaylicenses** includes the following:

- > SW Version
- > FW Version
- > HSM label
- > Serial #
- > HW Model
- > Authentication Method
- > RPV state
- > FIPS mode
- > HSM total storage space (bytes)
- > HSM used storage space (bytes)
- > HSM free storage space (bytes)
- > Performance level
- > Max # of partitions
- > # of partitions created
- > # of free partitions
- > HSM policies and their settings

### Partition Information

At the application partition level, the information in the outputs of **partition show** and **partition showpolicies** includes the following:

- > Partition Name
- > Partition Serial #
- > Activation State
- > AutoActivation State
- > Partition total storage space (bytes)
- > Partition used storage space (bytes)
- > Partition free storage space (bytes)
- > Partition Object Count
- > Partition policies and their settings

## The SafeNet Appliance MIB

The SAFENET-APPLIANCE-MIB defines appliance status information that can be viewed via SNMP. Currently, that consists of the appliance software version number.

### The appliance Table

This table provides a list of all the non-HSM host-specific information on the appliance.

| Item               | Type          | Description                        | Values          |
|--------------------|---------------|------------------------------------|-----------------|
| appSoftwareVersion | DisplayString | Appliance Software Version number. | -- from factory |

For information about the HSM inside the appliance, see ["The SafeNet Luna HSM MIB" on page 338](#).

## SNMP Operation and Limitations with SafeNet Luna Network HSM

This page applies only to SafeNet Luna Network HSM which, as a closed system, has its own agent. This contrasts with other SafeNet Luna HSMs that are installed inside a host computer, or USB-connected to a host, and therefore require you to provide an SNMP agent and configure for use with our subagent.

Various LunaSH commands govern the setup and use of SNMP with the SafeNet appliance. You provide your own SNMP application – a standard, open-source tool like net-snmp, or a commercial offering, or one that you develop yourself – and use the commands described below (and on the following pages) to enable and adjust the SNMP agent on-board the SafeNet appliance.

### SNMP-Related Commands

Please refer to the LunaSH Appliance Commands in the Reference Section of this Help for syntax and usage descriptions of the following:

- > The **sysconf snmp** command has subcommands **enable**, **disable**, **notification**, **show**, **trap**, and **user**.
  - The **sysconf snmp notification** command allows viewing and configuring the notifications that can be sent by the SNMP agent. At least one user must be configured before the SNMP agent can be accessed.
  - The **sysconf snmp enable** command enables and starts the SNMP service.
  - The **sysconf snmp disable** command stops the service.
  - The **sysconf snmp show** command shows the current status of the service.
  - The **sysconf snmp trap** command has sub-commands to set, show, and clear trap host information.
  - The **sysconf snmp user** command allows viewing and configuring the users that can access the SNMP agent. At least one user must be configured before the SNMP agent can be accessed.
- > The **service list** command reports a service: "snmpd - SNMP agent service".
- > The **service status**, **service stop**, **service start** and **service restart** commands accept the value "snmp" as a **<servicename>** parameter (that is, you can start, stop or restart the snmp service – this represents some overlap with the **sysconf enable** and **disable** commands, but is provided for completeness).



## Coverage

The following are some points of interest, with regard to our reporting.

### Memory

Swap usage - Covered by UCD-SNMP-MIB under memTotalSwap, memAvailSwap and memMinimumSwap OID

Physical Memory usage - Covered by UCD-SNMP-MIB under memTotalRea, memAvailReal, memTotalFree OID

Errors - Covered by UCD-SNMP-MIB under memSwapError and memSwapErrorMsg OID

### Paging

Size of page file - Not covered

Page file usage - Not covered

Paging errors - Not covered

Note: UCD-SNMP-MIB/memory will report all the data that we get from the "free" command.

### CPU

% Utilization Threads - Not covered

%user time - Covered by UCD-SNMP-MIB under ssCpuUsr OID

%system time - Covered by UCD-SNMP-MIB under ssCpuSystem OID

Top running processes - Not covered

### Network

Interface status - Covered

% utilization - Covered

Bytes in - Not covered

Bytes Out - Not covered

Errors - Covered

Note: All of the above are already covered by the RFC1213-MIB.

### Monitoring Internal Hardware failure

We do not currently keep any status on hardware failure.

### Environmental

We support only CPU and mother board temperature.

## HSM MIB

The above concerns status of various elements of the appliance, outside the contained HSM.

HSM status is separately handled by the SAFENET-HSM-MIB.

In the current implementation, the object `ntlsCertExpireNotification` has no value. If you query this object, the response is "Snmp No Such Object".

Information about the HSM, retrievable via SNMP, is similar to executing the following commands:

From SafeNet Luna Network HSM (LunaSH) commands:

- > **hsm show**
- > **hsm showpolicies**
- > **hsm displaylicenses**
- > **client show**

From the SafeNet Luna HSM Client (LunaCM) commands:

- > **partition showinfo**
- > **partition showpolicies**

## MIBS You Need for Network Monitoring of SafeNet Luna Network HSM

The following MIBs are not supplied as part of the SafeNet Luna Network HSM build, but can be downloaded from a number of sources. How they are implemented depends on your MIB utility. Support is restricted to active queries (trap captures only reboots).

- > LM-SENSORS-MIB
- > RFC1213-MIB
- > SNMP-FRAMEWORK-MIB
- > SNMP-MPD-MIB
- > SNMP-TARGET-MIB
- > SNMP-USER-BASED-SM-MIB
- > SNMPv2-MIB
- > SNMP-VIEW-BASED-ACM-MIB

In addition, the `SAFENET-APPLIANCE-MIB` is included within the SafeNet Luna Network HSM appliance, to report Software Version.

## MIBS You Need for Monitoring the Status of the HSM

You require the following MIB to monitor the status of the HSM:

- > `SAFENET-HSM-MIB.mib`

## Frequently Asked Questions

---

This section provides additional information by answering questions that are frequently asked by our customers.

**We want to use SNMP to remotely monitor and manage our installation – why do you not support such standard SNMP traps as CPU and Memory exhaustion?**

Those sorts of traps were specifically excluded because they can be used to establish a covert channel (an illicit signaling channel that can be used to communicate from a high assurance “area” to a lower assurance one in an effort to circumvent the security policy). Resource exhaustion events/alerts are the oldest known form of covert channel signaling. Exercise care with any HSM product that does allow such traps - what other basic security holes might be present?

# CHAPTER 21: Tamper Events

SafeNet Luna Network HSMs detect hardware anomalies (such as card over-temperature) and physical events (such as card removal or chassis intrusion), and register them as tamper events. A tamper event is considered a security breach, and effectively locks the HSM.

If **Policy 48: Do Controlled Tamper Recovery** is enabled (the default), the HSM SO must clear the tamper condition before the HSM is reset, to return the HSM to normal operation (see "[HSM Capabilities and Policies](#)" on page 95). While the HSM is in the tamper condition, only the subset of LunaSH commands required to view the HSM status or clear the tamper condition are available. For PED-authenticated HSMs, the cached PED key data that allows activation is zeroized, and activation is disabled. When an HSM is in the tamper state, only the HSM SO is able to log in to the HSM.

You can enable **Policy 40: Decommission on Tamper** to decommission the HSM when a tamper event occurs, so that partitions and roles are deleted from the HSM. By default, **Policy 40: Decommission on Tamper** is disabled, and the contents of the HSM are not affected by the tamper event.

If both policies are disabled, the HSM sends a warning when a tamper event occurs but does not make partition data inaccessible. We do not recommend disabling both policies.

If both policies are enabled, the HSM SO role is deleted when a tamper event occurs, so you do not need to log in this role to clear the tamper condition.

There are several conditions that can result in a tamper. The tamper state is indicated by the **HSM Tamper State** field in the output of the LunaSH **hsm show** command. If tamper events have been detected and not cleared, the field will read **Tamper(s) detected**. Use the **hsm tamper show** command to view detailed information for the tamper event, including whether it requires an HSM reset in addition to a tamper clear.

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

| Tamper event           | Response                                                                                                                                                                                                                                               |
|------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Chassis intrusion      | Halt the HSM. Deactivate activated partitions.<br>Decommission the HSM if <b>policy 40: Decommission on Tamper</b> is enabled.                                                                                                                         |
| Card removal           | Halt the HSM. Deactivate activated partitions.<br>Decommission the HSM if <b>policy 40: Decommission on Tamper</b> is enabled.                                                                                                                         |
| Over/under temperature | Halt the HSM. Deactivate activated partitions.<br>Decommission the HSM if <b>policy 40: Decommission on Tamper</b> is enabled.<br>Warnings are logged for mild over/under temperature events. Warnings are self-clearing if the condition is resolved. |

| Tamper event              | Response                                                                                                                                                                                                                                           |
|---------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Over/under voltage        | Halt the HSM. Deactivate activated partitions.<br>Decommission the HSM if <b>policy 40: Decommission on Tamper</b> is enabled.<br>Warnings are logged for mild over/under voltage events. Warnings are self-clearing if the condition is resolved. |
| Battery removal/depletion | Halt the HSM. Deactivate activated partitions.<br>Decommission the HSM.<br>Warnings are logged for low battery conditions.                                                                                                                         |

## Recovering from a Tamper Event

How you recover from a tamper event depends on how the following HSM policies are set. See "[HSM Capabilities and Policies](#)" on page 95 for more information:

|                                                 |                                                                                                                                                                                                                                                                                                                                      |
|-------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Policy 40: Decommission on tamper</b>        | If enabled, the HSM is decommissioned when a tamper event occurs. You must clear the tamper condition before you can re-initialize the HSM SO, re-create your partitions, restore the partition contents from backup, and re-initialize the partition roles (Partition SO, Crypto Officer, and Crypto User, and Audit, as relevant). |
| <b>Policy 48: Do Controlled Tamper Recovery</b> | If enabled, the tamper condition that halted the HSM must be cleared by the HSM SO (by issuing the <b>tamper clear</b> command), before the HSM can be reset to resume normal operations.                                                                                                                                            |

### Activation and auto-activation is disabled on tamper

If you are using activation or auto-activation on your PED-authenticated partitions, it is disabled when a tamper is detected, or if any uncleared tamper conditions are detected on reboot. See "[Activation and Auto-activation on Multi-factor- \(PED-\) Authenticated Partitions](#)" on page 23 and "[Partition Capabilities and Policies](#)" on page 106 for more information.

### To recover from a tamper

1. Use the following command to display the last tamper event:

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

**NOTE** The **hsm tamper show** command only shows the last tamper event, even if several tampers have occurred. To view a complete list of the tamper events that have occurred on the HSM, use the LunaSH **hsm supportinfo** command.

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

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

4. If the tamper message indicates that a reset is required, use the LunaSH **sysconf appliance reboot** command to reboot the HSM:

```
lunash:> sysconf appliance reboot
```

5. Verify that all tampers have been cleared:

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

6. If the HSM was decommissioned as a result of the tamper, you must re-create your partitions, re-initialize the partition roles (Partition SO, Crypto Officer, and Crypto User, and Audit as relevant), and restore the partition contents from backup. See the following sections in the Configuration Guide .
  - a. To re-create your partitions, see "[Create Application Partitions](#)" on page 1.
  - b. Re-initialize the partition roles. See "[Configure Application Partitions](#)" on page 1.
  - c. To restore the partition contents from backup, see "[Backup and Restore Using a G5-Based Backup HSM](#)" on page 53.
7. If the **Policy 22: Allow Activation** and/or **Policy 23: Allow AutoActivation** are enabled on your PED-authenticated partitions, the CO and CU (if enabled) must log in to reactivate those roles:

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

# CHAPTER 22: Troubleshooting

This chapter lists the HSM error codes and offers troubleshooting tips for some common issues. It contains the following sections:

- > ["General Troubleshooting Tips" below](#)
- > ["System Operational and Error Messages" on the next page](#)
- > ["Keycard and Token Return Codes" on page 353](#)
- > ["Library Codes" on page 371](#)
- > ["Vendor-Defined Return Codes" on page 376](#)

## General Troubleshooting Tips

---

Here are just a few quick things to check if you are experiencing problems:

- > Ensure that the date and time are set correctly.
- > Check that NTLS is bound to the correct Ethernet port. It must be bound to a port if it is to work, and that port must be the one that is connected for NTLS.
- > Ensure that the client is registered with the correct ip/hostname (or that you spelled it correctly, didn't accidentally transpose any characters, used only valid characters, etc.).
- > Ensure that the client is given access to the correct partition (again, be sure that it is spelled correctly; be careful of similarly named or numbered partitions).
- > Ensure that the **sysconf regencert** command was properly executed (with the IP address, if using IP mode).
- > Check the output of the syslog for any information on potential problems with **syslog tail**.
- > If you see an apparent 'hang' condition, connect and check the PED - it may be waiting for a PED action.
- > Check if you allowed the PED to time out, or if you started a command that needed PED action while the PED was not connected. You will need to re-issue the failed command after re-inserting the token, and pay attention to the PED.
- > If RSA signing seems slow, check the Capabilities and Policies to ensure that Confirmation (policy #29) is switched off - if your security policy demands that signing operations must be verified on the HSM, then expect almost a 50% performance reduction.
- > If you perform a Restore from Backup operation and some or all of the objects are shown with an error message like "LUNA\_RET\_SM\_ACCESS\_DOES\_NOT\_VALIDATE", you might have interrupted the restore operation (even a **partition contents** command could have this effect). Re-issue the Restore command, ensuring that no other commands are run against the partition while the operation is in progress - if other persons might be using their own SSH sessions to access the appliance, it might be best to disconnect the network cable and perform your restore operation from the local (serial) console.

## System Operational and Error Messages

### Extra slots that say "token not present"?

This happens for two reasons:

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

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

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

For SafeNet Luna Network HSM, which has its configuration file internal to the appliance, and not directly accessible for modification, you cannot change the default cryptographic slot allotments.

### Error: 'hsm update firmware' failed. (10A0B : LUNA\_RET\_OPERATION\_RESTRICTED) when attempting to perform hsm update firmware

You must ensure that STM is disabled before you run the firmware update.

Also, as with any update, you should backup any important HSM contents before proceeding.

### KR\_ECC\_POINT\_INVALID Error when decrypting a file encrypted from BSAFE through ECIES using ECC key with any of the curves from the x9\_t2 section

As indicated on the BSAFE web site, they support only the NIST-approved curves (prime, Binary, and Koblitz). That includes most/all the curves from test items 0 through 37 in CK Demo: the "secp", "X9\_62\_prime", and "sect" curves.

The X9.62 curves that are failing in this task are X9.62 binary/char2 curves which do not appear to be supported by BSAFE. So, you appear to be encountering a BSAFE limitation and not a SafeNet Luna HSM problem.

### Error during SSL Connect (RC\_OPERATION\_TIMED\_OUT) logged to /var/log/messages by the SafeNet Luna HSM Client

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

The following is a list of some potential causes:

- > Network issue.



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

## Slow/interrupted response from the HSM, and the "hsm show" command shows LUNA\_RET\_SM\_SESSION\_REALLOC\_ERROR

```
Appliance Details:
=====
Software Version: 7.0.0
Error: 'hsm show' failed. (310102 : LUNA_RET_SM_SESSION_REALLOC_ERROR)
```

Command Result : 65535 (Luna Shell execution)

The error LUNA\_RET\_SM\_SESSION\_REALLOC\_ERROR means the HSM cannot expand the session table.

The HSM maintains a table for all of the open sessions. For performance reasons, the table is quite small initially. As sessions are opened (and not closed) the table fills up. When the table gets full, the HSM tries to expand the table. If there is not enough available RAM to grow the table, this error is returned.

RAM can be used up by an application that creates and does not delete a large number of session objects, as well as by an application that opens and fails to close a large number of sessions.

The obvious solution is proper housekeeping. Your applications must clean up after themselves, by closing sessions that are no longer in use - this deletes session objects associated with those sessions. If your application practice is to have long-lived sessions, and to open many objects in a given session, then your application should explicitly delete those session objects as soon as each one is no longer necessary.

By far, we see more of the former problem - abandoned sessions - and very often in conjunction with Java-based applications. Proper garbage collection includes deleting session objects when they are no longer useful, or simply closing sessions as soon as they are not required. Formally closing a session (or stopping/restarting the HSM) deletes all session objects within each affected session. These actions keep the session table small, so it uses the least possible HSM volatile memory.

## Low Battery Message

The K7 HSM card, used in the SafeNet Luna Network HSM and SafeNet Luna PCIe HSM products, is equipped with a non-replaceable battery that is expected to last the life of the product. If you notice a log message or other warning about 'battery low', or similar, contact Technical Support.

## Keycard and Token Return Codes

The following table summarizes HSM error codes:

| HSM Error                               | Hex Code   | PKCS#11 or SFNT Defined CKR Error    |
|-----------------------------------------|------------|--------------------------------------|
| LUNA_RET_OK                             | 0x00000000 | CKR_OK                               |
| LUNA_RET_CANCEL                         | 0x00010000 | CKR_CANCEL                           |
| LUNA_RET_FLAGS_INVALID                  | 0x00040000 | CKR_FLAGS_INVALID, removed from v2.0 |
| LUNA_RET_TOKEN_NOT_PRESENT              | 0x00E00000 | CKR_TOKEN_NOT_PRESENT                |
| LUNA_RET_FORMER_INVALID_ENTRY_TYPE      | 0x00300130 | CKR_DEVICE_ERROR                     |
| LUNA_RET_SP_TX_ERROR                    | 0x00300131 | CKR_DEVICE_ERROR                     |
| LUNA_RET_SP_RX_ERROR                    | 0x00300132 | CKR_DEVICE_ERROR                     |
| LUNA_RET_PED_ID_INVALID                 | 0x00300140 | CKR_DEVICE_ERROR                     |
| LUNA_RET_PED_UNSUPPORTED_PROTOCOL       | 0x00300141 | CKR_DEVICE_ERROR                     |
| LUNA_RET_PED_UNPLUGGED                  | 0x00300142 | CKR_PED_UNPLUGGED                    |
| LUNA_RET_PED_ERROR                      | 0x00300144 | CKR_DEVICE_ERROR                     |
| LUNA_RET_PED_UNSUPPORTED_CRYPTOPROTOCOL | 0x00300145 | CKR_DEVICE_ERROR                     |
| LUNA_RET_PED_DEK_INVALID                | 0x00300146 | CKR_DEVICE_ERROR                     |
| LUNA_RET_PED_CLIENT_NOT_RUNNING         | 0x00300147 | CKR_PED_CLIENT_NOT_RUNNING           |
| LUNA_RET_CL_ALIGNMENT_ERROR             | 0x00300200 | CKR_DEVICE_ERROR                     |
| LUNA_RET_CL_QUEUE_LOCATION_ERROR        | 0x00300201 | CKR_DEVICE_ERROR                     |
| LUNA_RET_CL_QUEUE_OVERLAP_ERROR         | 0x00300202 | CKR_DEVICE_ERROR                     |
| LUNA_RET_CL_TRANSMISSION_ERROR          | 0x00300203 | CKR_DEVICE_ERROR                     |
| LUNA_RET_CL_NO_TRANSMISSION             | 0x00300204 | CKR_DEVICE_ERROR                     |
| LUNA_RET_CL_COMMAND_MALFORMED           | 0x00300205 | CKR_DEVICE_ERROR                     |
| LUNA_RET_CL_MAILBOXES_NOT_AVAILABLE     | 0x00300206 | CKR_DEVICE_ERROR                     |

| HSM Error                                         | Hex Code   | PKCS#11 or SFNT Defined CKR Error |
|---------------------------------------------------|------------|-----------------------------------|
| LUNA_RET_MM_NOT_ENOUGH_MEMORY                     | 0x00310000 | CKR_DEVICE_ERROR                  |
| LUNA_RET_MM_INVALID_HANDLE                        | 0x00310001 | CKR_DEVICE_ERROR                  |
| LUNA_RET_MM_USAGE_ALREADY_SET                     | 0x00310002 | CKR_DEVICE_ERROR                  |
| LUNA_RET_MM_ACCESS_OUTSIDE_ALLOCATION_RANGE       | 0x00310003 | CKR_DEVICE_ERROR                  |
| LUNA_RET_MM_INVALID_USAGE                         | 0x00310004 | CKR_DEVICE_ERROR                  |
| LUNA_RET_MM_ITERATOR_PAST_END                     | 0x00310005 | CKR_DEVICE_ERROR                  |
| LUNA_RET_MM_FATAL_ERROR                           | 0x00310006 | CKR_DEVICE_ERROR                  |
| LUNA_RET_TEMPLATE_INCOMPLETE                      | 0x00D00000 | CKR_TEMPLATE_INCOMPLETE           |
| LUNA_RET_TEMPLATE_INCONSISTENT                    | 0x00D10000 | CKR_TEMPLATE_INCONSISTENT*        |
| LUNA_RET_ATTRIBUTE_TYPE_INVALID                   | 0x00120000 | CKR_ATTRIBUTE_TYPE_INVALID        |
| LUNA_RET_ATTRIBUTE_VALUE_INVALID                  | 0x00130000 | CKR_ATTRIBUTE_VALUE_INVALID       |
| LUNA_RET_ATTRIBUTE_READ_ONLY                      | 0x00100000 | CKR_ATTRIBUTE_READ_ONLY           |
| LUNA_RET_ATTRIBUTE_SENSITIVE                      | 0x00110000 | CKR_ATTRIBUTE_SENSITIVE           |
| LUNA_RET_OBJECT_HANDLE_INVALID                    | 0x00820000 | CKR_OBJECT_HANDLE_INVALID         |
| LUNA_RET_MAX_OBJECT_COUNT                         | 0x00820001 | CKR_MAX_OBJECT_COUNT_EXCEEDED     |
| LUNA_RET_ATTRIBUTE_NOT_FOUND                      | 0x00120010 | CKR_ATTRIBUTE_TYPE_INVALID        |
| LUNA_RET_CAN_NOT_CREATE_SECRET_KEY                | 0x00D10011 | CKR_TEMPLATE_INCONSISTENT         |
| LUNA_RET_CAN_NOT_CREATE_PRIVATE_KEY               | 0x00D10012 | CKR_TEMPLATE_INCONSISTENT         |
| LUNA_RET_SECRET_KEY_MUST_BE_SENSITIVE             | 0x00130013 | CKR_ATTRIBUTE_VALUE_INVALID       |
| LUNA_RET_SECRET_KEY_MUST_HAVE_SENSITIVE_ATTRIBUTE | 0x00D00014 | CKR_TEMPLATE_INCOMPLETE           |
| LUNA_RET_PRIVATE_KEY_MUST_BE_SENSITIVE            | 0x00130015 | CKR_ATTRIBUTE_VALUE_INVALID       |

| HSM Error                                          | Hex Code   | PKCS#11 or SFNT Defined CKR Error |
|----------------------------------------------------|------------|-----------------------------------|
| LUNA_RET_PRIVATE_KEY_MUST_HAVE_SENSITIVE_ATTRIBUTE | 0x00D00016 | CKR_TEMPLATE_INCOMPLETE           |
| LUNA_RET_SIGNING_KEY_MUST_BE_LOCAL                 | 0x00680001 | CKR_KEY_FUNCTION_NOT_PERMITTED    |
| LUNA_RET_MULTI_FUNCTION_KEYS_NOT_ALLOWED           | 0x00D10018 | CKR_TEMPLATE_INCONSISTENT         |
| LUNA_RET_CAN_NOT_CHANGE_KEY_FUNCTION               | 0x00100019 | CKR_ATTRIBUTE_READ_ONLY           |
| LUNA_RET_KEY_SIZE_RANGE                            | 0x00620000 | CKR_KEY_SIZE_RANGE                |
| LUNA_RET_KEY_TYPE_INCONSISTENT                     | 0x00630000 | CKR_KEY_TYPE_INCONSISTENT         |
| LUNA_RET_KEY_INVALID_FOR_OPERATION                 | 0x00630001 | CKR_KEY_TYPE_INCONSISTENT         |
| LUNA_RET_KEY_PARITY                                | 0x00630002 | CKR_KEY_TYPE_INCONSISTENT         |
| LUNA_RET_KEY_UNEXTRACTABLE                         | 0x006a0000 | CKR_KEY_UNEXTRACTABLE             |
| LUNA_RET_KEY_EXTRACTABLE                           | 0x006a0001 | KR_KEY_UNEXTRACTABLE              |
| LUNA_RET_KEY_INDIGESTIBLE                          | 0x00670000 | CKR_KEY_INDIGESTIBLE              |
| LUNA_RET_KEY_NOT_WRAPPABLE                         | 0x00690000 | CKR_KEY_NOT_WRAPPABLE             |
| LUNA_RET_KEY_NOT_UNWRAPPABLE                       | 0x00690001 | CKR_KEY_NOT_WRAPPABLE             |
| LUNA_RET_ARGUMENTS_BAD                             | 0x00070000 | CKR_ARGUMENTS_BAD                 |
| LUNA_RET_INVALID_ENTRY_TYPE                        | 0x00070001 | CKR_INVALID_ENTRY_TYPE            |
| LUNA_RET_DATA_INVALID                              | 0x00200000 | CKR_DATA_INVALID                  |
| LUNA_RET_SM_DATA_INVALID                           | 0x00200002 | CKR_DATA_INVALID                  |
| LUNA_RET_NO_RNG_SEED                               | 0x00200015 | CKR_DATA_INVALID                  |
| LUNA_RET_FUNCTION_NOT_SUPPORTED                    | 0x00540000 | CKR_FUNCTION_NOT_SUPPORTED        |
| LUNA_RET_NO_OFFBOARD_STORAGE                       | 0x00540001 | CKR_FUNCTION_NOT_SUPPORTED        |

| HSM Error                           | Hex Code   | PKCS#11 or SFNT Defined CKR Error |
|-------------------------------------|------------|-----------------------------------|
| LUNA_RET_CL_COMMAND_NON_BACKUP      | 0x00540002 | CKR_FUNCTION_NOT_SUPPORTED        |
| LUNA_RET_BUFFER_TOO_SMALL           | 0x01500000 | CKR_BUFFER_TOO_SMALL              |
| LUNA_RET_DATA_LEN_RANGE             | 0x00210000 | CKR_DATA_LEN_RANGE                |
| LUNA_RET_GENERAL_ERROR              | 0x00050000 | CKR_GENERAL_ERROR                 |
| LUNA_RET_DEVICE_ERROR               | 0x00300000 | CKR_DEVICE_ERROR                  |
| LUNA_RET_UNKNOWN_COMMAND            | 0x00300001 | CKR_FUNCTION_NOT_SUPPORTED        |
| LUNA_RET_TOKEN_LOCKED_OUT           | 0x00300002 | CKR_PIN_LOCKED                    |
| LUNA_RET_RNG_ERROR                  | 0x00300003 | CKR_DEVICE_ERROR                  |
| LUNA_RET_DES_SELF_TEST_FAILURE      | 0x00300004 | CKR_DEVICE_ERROR                  |
| LUNA_RET_CAST_SELF_TEST_FAILURE     | 0x00300005 | CKR_DEVICE_ERROR                  |
| LUNA_RET_CAST3_SELF_TEST_FAILURE    | 0x00300006 | CKR_DEVICE_ERROR                  |
| LUNA_RET_CAST5_SELF_TEST_FAILURE    | 0x00300007 | CKR_DEVICE_ERROR                  |
| LUNA_RET_MD2_SELF_TEST_FAILURE      | 0x00300008 | CKR_DEVICE_ERROR                  |
| LUNA_RET_MD5_SELF_TEST_FAILURE      | 0x00300009 | CKR_DEVICE_ERROR                  |
| LUNA_RET_SHA_SELF_TEST_FAILURE      | 0x0030000a | CKR_DEVICE_ERROR                  |
| LUNA_RET_RSA_SELF_TEST_FAILURE      | 0x0030000b | CKR_DEVICE_ERROR                  |
| LUNA_RET_RC2_SELF_TEST_FAILURE      | 0x0030000c | CKR_DEVICE_ERROR                  |
| LUNA_RET_RC4_SELF_TEST_FAILURE      | 0x0030000d | CKR_DEVICE_ERROR                  |
| LUNA_RET_RC5_SELF_TEST_FAILURE      | 0x0030000e | CKR_DEVICE_ERROR                  |
| LUNA_RET_SO_LOGIN_FAILURE_THRESHOLD | 0x0030000f | CKR_SO_LOGIN_FAILURE_THRESHOLD    |
| LUNA_RET_RNG_SELF_TEST_FAILURE      | 0x00300010 | CKR_DEVICE_ERROR                  |

| HSM Error                                   | Hex Code   | PKCS#11 or SFNT Defined CKR Error |
|---------------------------------------------|------------|-----------------------------------|
| LUNA_RET_SM_UNKNOWN_COMMAND                 | 0x00300011 | CKR_DEVICE_ERROR                  |
| LUNA_RET_UM_TSN_MISSING                     | 0x00300012 | CKR_DEVICE_ERROR                  |
| LUNA_RET_SM_TSV_MISSING                     | 0x00300013 | CKR_DEVICE_ERROR                  |
| LUNA_RET_SM_UNKNOWN_TOSM_STATE              | 0x00300014 | CKR_DEVICE_ERROR                  |
| LUNA_RET_DSA_PARAM_GEN_FAILURE              | 0x00300015 | CKR_DEVICE_ERROR                  |
| LUNA_RET_DSA_SELF_TEST_FAILURE              | 0x00300016 | CKR_DEVICE_ERROR                  |
| LUNA_RET_SEED_SELF_TEST_FAILURE             | 0x00300017 | CKR_DEVICE_ERROR                  |
| LUNA_RET_AES_SELF_TEST_FAILURE              | 0x00300018 | CKR_DEVICE_ERROR                  |
| LUNA_RET_FUNCTION_NOT_SUPPORTED_BY_HARDWARE | 0x00300019 | CKR_DEVICE_ERROR                  |
| LUNA_RET_HAS160_SELF_TEST_FAILURE           | 0x0030001a | CKR_DEVICE_ERROR                  |
| LUNA_RET_KCDSA_PARAM_GEN_FAILURE            | 0x0030001b | CKR_DEVICE_ERROR                  |
| LUNA_RET_KCDSA_SELF_TEST_FAILURE            | 0x0030001c | CKR_DEVICE_ERROR                  |
| LUNA_RET_HSM_INTERNAL_BUFFER_TOO_SMALL      | 0x0030001d | CKR_DEVICE_ERROR                  |
| LUNA_RET_COUNTER_WRAPAROUND                 | 0x0030001e | CKR_DEVICE_ERROR                  |
| LUNA_RET_TIMEOUT                            | 0x0030001f | CKR_TIMEOUT                       |
| LUNA_RET_NOT_READY                          | 0x00300020 | CKR_DEVICE_ERROR                  |
| LUNA_RET_RETRY                              | 0x00300021 | CKR_DEVICE_ERROR                  |
| LUNA_RET_SHA1_RSA_SELF_TEST_FAILURE         | 0x00300022 | CKR_DEVICE_ERROR                  |
| LUNA_RET_SELF_TEST_FAILURE                  | 0x00300023 | CKR_DEVICE_ERROR                  |
| LUNA_RET_INCOMPATIBLE                       | 0x00300024 | CKR_DEVICE_ERROR                  |
| LUNA_RET_RIPEMD160_SELF_TEST_FAILURE        | 0x00300034 | CKR_DEVICE_ERROR                  |

| HSM Error                            | Hex Code   | PKCS#11 or SFNT Defined CKR Error |
|--------------------------------------|------------|-----------------------------------|
| LUNA_RET_TOKEN_LOCKED_OUT_CL         | 0x00300100 | CKR_DEVICE_ERROR                  |
| LUNA_RET_TOKEN_LOCKED_OUT_MM         | 0x00300101 | CKR_DEVICE_ERROR                  |
| LUNA_RET_TOKEN_LOCKED_OUT_UM         | 0x00300102 | CKR_DEVICE_ERROR                  |
| LUNA_RET_TOKEN_LOCKED_OUT_SM         | 0x00300103 | CKR_DEVICE_ERROR                  |
| LUNA_RET_TOKEN_LOCKED_OUT_RN         | 0x00300104 | CKR_DEVICE_ERROR                  |
| LUNA_RET_TOKEN_LOCKED_OUT_CA         | 0x00300105 | CKR_DEVICE_ERROR                  |
| LUNA_RET_TOKEN_LOCKED_OUT_PM         | 0x00300106 | CKR_DEVICE_ERROR                  |
| LUNA_RET_TOKEN_LOCKED_OUT_OH         | 0x00300107 | CKR_DEVICE_ERROR                  |
| LUNA_RET_TOKEN_LOCKED_OUT_CCM        | 0x00300108 | CKR_DEVICE_ERROR                  |
| LUNA_RET_TOKEN_LOCKED_OUT_SHA_DIGEST | 0x00300109 | CKR_DEVICE_ERROR                  |
| LUNA_RET_SM_ACCESS_REALLOC_ERROR     | 0x00310101 | CKR_DEVICE_ERROR                  |
| LUNA_RET_SM_SESSION_REALLOC_ERROR    | 0x00310102 | CKR_DEVICE_ERROR                  |
| LUNA_RET_SM_MEMORY_ALLOCATION_ERROR  | 0x00310103 | CKR_DEVICE_ERROR                  |
| LUNA_RET_ENCRYPTED_DATA_INVALID      | 0x00400000 | CKR_ENCRYPTED_DATA_INVALID        |
| LUNA_RET_ENCRYPTED_DATA_LEN_RANGE    | 0x00410000 | CKR_ENCRYPTED_DATA_LEN_RANGE      |
| LUNA_RET_FUNCTION_CANCELED           | 0x00500000 | CKR_FUNCTION_CANCELED             |
| LUNA_RET_KEY_HANDLE_INVALID          | 0x00600000 | CKR_KEY_HANDLE_INVALID            |
| LUNA_RET_MECHANISM_INVALID           | 0x00700000 | CKR_MECHANISM_INVALID             |
| LUNA_RET_MECHANISM_PARAM_INVALID     | 0x00710000 | CKR_MECHANISM_PARAM_INVALID       |
| LUNA_RET_OPERATION_ACTIVE            | 0x00900000 | CKR_OPERATION_ACTIVE              |
| LUNA_RET_OPERATION_NOT_INITIALIZED   | 0x00910000 | CKR_OPERATION_NOT_INITIALIZED     |

| HSM Error                                    | Hex Code   | PKCS#11 or SFNT Defined CKR Error    |
|----------------------------------------------|------------|--------------------------------------|
| LUNA_RET_UM_PIN_INCORRECT                    | 0x00a00000 | CKR_PIN_INCORRECT                    |
| LUNA_RET_UM_PIN_INCORRECT_CONTAINER_ZEROIZED | 0x00a00001 | CKR_PIN_INCORRECT                    |
| LUNA_RET_UM_PIN_INCORRECT_CONTAINER_LOCKED   | 0x00a00002 | CKR_PIN_INCORRECT                    |
| LUNA_RET_UM_PIN_LEN_RANGE                    | 0x00a20000 | CKR_PIN_LEN_RANGE                    |
| LUNA_RET_SM_PIN_EXPIRED                      | 0x00a30000 | CKR_PIN_EXPIRED                      |
| LUNA_RET_SM_EXCLUSIVE_SESSION_EXISTS         | 0x00b20000 | CKR_SESSION_EXCLUSIVE_EXISTS         |
| LUNA_RET_SM_SESSION_HANDLE_INVALID           | 0x00b30000 | CKR_SESSION_HANDLE_INVALID           |
| LUNA_RET_SIGNATURE_INVALID                   | 0x00c00000 | CKR_SIGNATURE_INVALID                |
| LUNA_RET_SIGNATURE_LEN_RANGE                 | 0x00c10000 | CKR_SIGNATURE_LEN_RANGE              |
| LUNA_RET_UNWRAPPING_KEY_HANDLE_INVALID       | 0x00f00000 | CKR_UNWRAPPING_KEY_HANDLE_INVALID    |
| LUNA_RET_UNWRAPPING_KEY_SIZE_RANGE           | 0x00f10000 | CKR_UNWRAPPING_KEY_SIZE_RANGE        |
| LUNA_RET_UNWRAPPING_KEY_TYPE_INCONSISTENT    | 0x00f20000 | CKR_UNWRAPPING_KEY_TYPE_INCONSISTENT |
| LUNA_RET_USER_ALREADY_LOGGED_IN              | 0x01000000 | CKR_USER_ALREADY_LOGGED_IN           |
| LUNA_RET_SM_OTHER_USER_LOGGED_IN             | 0x01000001 | CKR_USER_ALREADY_LOGGED_IN           |
| LUNA_RET_USER_NOT_LOGGED_IN                  | 0x01010000 | CKR_USER_NOT_LOGGED_IN               |
| LUNA_RET_SM_NOT_LOGGED_IN                    | 0x01010001 | CKR_USER_NOT_LOGGED_IN               |
| LUNA_RET_USER_PIN_NOT_INITIALIZED            | 0x01020000 | CKR_USER_PIN_NOT_INITIALIZED         |
| LUNA_RET_USER_TYPE_INVALID                   | 0x01030000 | CKR_USER_TYPE_INVALID                |



| HSM Error                                 | Hex Code   | PKCS#11 or SFNT Defined CKR Error  |
|-------------------------------------------|------------|------------------------------------|
| LUNA_RET_WRAPPED_KEY_INVALID              | 0x01100000 | CKR_WRAPPED_KEY_INVALID            |
| LUNA_RET_WRAPPED_KEY_LEN_RANGE            | 0x01120000 | CKR_WRAPPED_KEY_LEN_RANGE          |
| LUNA_RET_WRAPPING_KEY_HANDLE_INVALID      | 0x01130000 | CKR_WRAPPING_KEY_HANDLE_INVALID    |
| LUNA_RET_WRAPPING_KEY_SIZE_RANGE          | 0x01140000 | CKR_WRAPPING_KEY_SIZE_RANGE        |
| LUNA_RET_WRAPPING_KEY_TYPE_INCONSISTENT   | 0x01150000 | CKR_WRAPPING_KEY_TYPE_INCONSISTENT |
| LUNA_RET_CERT_VERSION_NOT_SUPPORTED       | 0x00300300 | CKR_DEVICE_ERROR                   |
| LUNA_RET_SIM_AUTHFORM_INVALID             | 0x0020011e | CKR_SIM_AUTHFORM_INVALID           |
| LUNA_RET_CCM_TOO_LARGE                    | 0x00210001 | CKR_DATA_LEN_RANGE                 |
| LUNA_RET_TEST_VS_BSAFE_FAILED             | 0x00300820 | CKR_DEVICE_ERROR                   |
| LUNA_RET_SFNT3120_ERROR                   | 0x00300821 | CKR_DEVICE_ERROR                   |
| LUNA_RET_SFNT3120_SELFTEST_FAILED         | 0x00300822 | CKR_DEVICE_ERROR                   |
| LUNA_RET_SFNT3120_CRC                     | 0x00300823 | CKR_DEVICE_ERROR                   |
| LUNA_RET_SFNT3120_ALG_NO_SOFTWARE_SUPPORT | 0x00300824 | CKR_DEVICE_ERROR                   |
| LUNA_RET_ISES_ERROR                       | 0x00300880 | CKR_DEVICE_ERROR                   |
| LUNA_RET_ISES_INIT_FAILED                 | 0x00300881 | CKR_DEVICE_ERROR                   |
| LUNA_RET_ISES_LNAU_TEST_FAILED            | 0x00300882 | CKR_DEVICE_ERROR                   |
| LUNA_RET_ISES_RNG_TEST_FAILED             | 0x00300883 | CKR_DEVICE_ERROR                   |
| LUNA_RET_ISES_CMD_FAILED                  | 0x00300884 | CKR_DEVICE_ERROR                   |
| LUNA_RET_ISES_CMD_PARAMETER_INVALID       | 0x00300885 | CKR_DEVICE_ERROR                   |
| LUNA_RET_ISES_TEST_VS_BSAFE_FAILED        | 0x00300886 | CKR_DEVICE_ERROR                   |

| HSM Error                                    | Hex Code   | PKCS#11 or SFNT Defined CKR Error |
|----------------------------------------------|------------|-----------------------------------|
| LUNA_RET_RM_ELEMENT_VALUE_INVALID            | 0x00200a00 | CKR_DATA_INVALID                  |
| LUNA_RET_RM_ELEMENT_ID_INVALID               | 0x00200a01 | CKR_DATA_INVALID                  |
| LUNA_RET_RM_NO_MEMORY                        | 0x00310a02 | CKR_DEVICE_MEMORY                 |
| LUNA_RET_RM_BAD_HSM_PARAMS                   | 0x00300a03 | CKR_DEVICE_ERROR                  |
| LUNA_RET_RM_POLICY_ELEMENT_DESTRUCTIVE       | 0x00200a04 | CKR_DATA_INVALID                  |
| LUNA_RET_RM_POLICY_ELEMENT_NOT_DESTRUCTIVE   | 0x00200a05 | CKR_DATA_INVALID                  |
| LUNA_RET_RM_CONFIG_CHANGE_ILLEGAL            | 0x00010a06 | CKR_CANCEL                        |
| LUNA_RET_RM_CONFIG_CHANGE_FAILS_DEPENDENCIES | 0x00010a07 | CKR_CANCEL                        |
| LUNA_RET_LICENSE_ID_UNKNOWN                  | 0x00200a08 | CKR_DATA_INVALID                  |
| LUNA_RET_LICENSE_CAPACITY_EXCEEDED           | 0x00010a09 | CKR_LICENSE_CAPACITY_EXCEEDED     |
| LUNA_RET_RM_POLICY_WRITE_RESTRICTED          | 0x00010a0a | CKR_CANCEL                        |
| LUNA_RET_OPERATION_RESTRICTED                | 0x00010a0b | CKR_OPERATION_NOT_ALLOWED         |
| LUNA_RET_CANNOT_PERFORM_OPERATION_TWICE      | 0x00010a0c | CKR_CANCEL                        |
| LUNA_RET_BAD_PPID                            | 0x00200a0d | CKR_DATA_INVALID                  |
| LUNA_RET_BAD_FW_VERSION                      | 0x00200a0e | CKR_DATA_INVALID                  |
| LUNA_RET_OPERATION_SHOULD_BE_DESTRUCTIVE     | 0x00200a0f | CKR_DATA_INVALID                  |
| LUNA_RET_RM_CONFIG_ILLEGAL                   | 0x00200a10 | CKR_DATA_INVALID                  |
| LUNA_RET_BAD_SN                              | 0x00200a11 | CKR_DATA_INVALID                  |
| LUNA_RET_CHALLENGE_TYPE_INVALID              | 0x00200b00 | CKR_DATA_INVALID                  |

| HSM Error                               | Hex Code   | PKCS#11 or SFNT Defined CKR Error |
|-----------------------------------------|------------|-----------------------------------|
| LUNA_RET_CHALLENGE_REQUIRES_PED         | 0x00010b01 | CKR_CANCEL                        |
| LUNA_RET_CHALLENGE_NOT_REQUIRED         | 0x00010b02 | CKR_CANCEL                        |
| LUNA_RET_CHALLENGE_RESPONSE_INCORRECT   | 0x00a00b03 | CKR_PIN_INCORRECT                 |
| LUNA_RET_OH_OBJECT_VERSION_INVALID      | 0x00300c00 | CKR_DEVICE_ERROR                  |
| LUNA_RET_OH_OBJECT_TYPE_INVALID         | 0x00300c01 | CKR_DEVICE_ERROR                  |
| LUNA_RET_OH_OBJECT_ALREADY_EXISTS       | 0x00010c02 | CKR_CANCEL                        |
| LUNA_RET_OH_OBJECT_OWNER_DOES_NOT_EXIST | 0x00200c03 | CKR_DATA_INVALID                  |
| LUNA_RET_STORAGE_TYPE_INCONSISTENT      | 0x00200c04 | CKR_DATA_INVALID                  |
| LUNA_RET_CONTAINER_CAN_NOT_HAVE_MEMBERS | 0x00200c05 | CKR_DATA_INVALID                  |
| LUNA_RET_SAVED_STATE_INVALID            | 0x01600000 | CKR_SAVED_STATE_INVALID           |
| LUNA_RET_STATE_UNSAVEABLE               | 0x01800000 | CKR_STATE_UNSAVEABLE              |
| LUNA_RET_ERROR                          | 0x80000000 | CKR_GENERAL_ERROR                 |
| LUNA_RET_CONTAINER_HANDLE_INVALID       | 0x80000001 | CKR_CONTAINER_HANDLE_INVALID      |
| LUNA_RET_INVALID_PADDING_TYPE           | 0x80000002 | CKR_DATA_INVALID                  |
| LUNA_RET_NOT_FOUND                      | 0x80000007 | CKR_FUNCTION_FAILED               |
| LUNA_RET_TOO_MANY_CONTAINERS            | 0x80000008 | CKR_TOO_MANY_CONTAINERS           |
| LUNA_RET_CONTAINER_LOCKED               | 0x80000009 | CKR_PIN_LOCKED                    |
| LUNA_RET_CONTAINER_IS_DISABLED          | 0x8000000a | CKR_PARTITION_DISABLED            |
| LUNA_RET_SECURITY_PARAMETER_MISSING     | 0x8000000b | CKR_SECURITY_PARAMETER_MISSING    |
| LUNA_RET_DEVICE_TIMEOUT                 | 0x8000000c | CKR_DEVICE_TIMEOUT                |

| HSM Error                                 | Hex Code   | PKCS#11 or SFNT Defined CKR Error    |
|-------------------------------------------|------------|--------------------------------------|
| LUNA_RET_OBJECT_DELETED                   | 0x8000000d | HSM Internal ONLY                    |
| LUNA_RET_INVALID_FUF_TARGET               | 0x8000000e | CKR_INVALID_FUF_TARGET               |
| LUNA_RET_INVALID_FUF_HEADER               | 0x8000000f | CKR_INVALID_FUF_HEADER               |
| LUNA_RET_INVALID_FUF_VERSION              | 0x80000010 | CKR_INVALID_FUF_VERSION              |
| LUNA_RET_KCV_PARAMETER_ALREADY_EXISTS     | 0x80000100 | CKR_CLONING_PARAMETER_ALREADY_EXISTS |
| LUNA_RET_KCV_PARAMETER_COULD_NOT_BE_ADDED | 0x80000101 | CKR_DEVICE_MEMORY                    |
| LUNA_RET_INVALID_CERTIFICATE_DATA         | 0x80000102 | CKR_CERTIFICATE_DATA_INVALID         |
| LUNA_RET_INVALID_CERTIFICATE_TYPE         | 0x80000103 | CKR_CERTIFICATE_DATA_INVALID         |
| LUNA_RET_INVALID_CERTIFICATE_VERSION      | 0x80000104 | CKR_CERTIFICATE_DATA_INVALID         |
| LUNA_RET_INVALID_MODULUS_SIZE             | 0x80000105 | CKR_ATTRIBUTE_VALUE_INVALID          |
| LUNA_RET_WRAPPING_ERROR                   | 0x80000107 | CKR_WRAPPING_ERROR                   |
| LUNA_RET_UNWRAPPING_ERROR                 | 0x80000108 | CKR_UNWRAPPING_ERROR                 |
| LUNA_RET_INVALID_PRIVATE_KEY_TYPE         | 0x80000109 | CKR_DATA_INVALID                     |
| LUNA_RET_TSN_MISMATCH                     | 0x8000010a | CKR_DATA_INVALID                     |
| LUNA_RET_KCV_PARAMETER_MISSING            | 0x8000010b | CKR_CLONING_PARAMETER_MISSING        |
| LUNA_RET_TWC_PARAMETER_MISSING            | 0x8000010c | CKR_CERTIFICATE_DATA_MISSING         |
| LUNA_RET_TUK_PARAMETER_MISSING            | 0x8000010d | CKR_CERTIFICATE_DATA_MISSING         |
| LUNA_RET_CPK_PARAMETER_MISSING            | 0x8000010e | CKR_KEY_NEEDED                       |

| HSM Error                         | Hex Code   | PKCS#11 or SFNT Defined CKR Error |
|-----------------------------------|------------|-----------------------------------|
| LUNA_RET_MASKING_NOT_SUPPORTED    | 0x8000010f | CKR_FUNCTION_NOT_SUPPORTED        |
| LUNA_RET_INVALID_ACCESS_LEVEL     | 0x80000110 | CKR_ARGUMENTS_BAD                 |
| LUNA_RET_MAC_MISSING              | 0x80000111 | CKR_MAC_MISSING                   |
| LUNA_RET_DAC_POLICY_PID_MISMATCH  | 0x80000112 | CKR_DAC_POLICY_PID_MISMATCH       |
| LUNA_RET_DAC_MISSING              | 0x80000113 | CKR_DAC_MISSING                   |
| LUNA_RET_BAD_DAC                  | 0x80000114 | CKR_BAD_DAC                       |
| LUNA_RET_SSK_MISSING              | 0x80000115 | CKR_SSK_MISSING                   |
| LUNA_RET_BAD_MAC                  | 0x80000116 | CKR_BAD_MAC                       |
| LUNA_RET_DAK_MISSING              | 0x80000117 | CKR_DAK_MISSING                   |
| LUNA_RET_BAD_DAK                  | 0x80000118 | CKR_BAD_DAK                       |
| LUNA_RET_HOK_MISSING              | 0x80000119 | CKR_CERTIFICATE_DATA_MISSING      |
| LUNA_RET_CITS_DAK_MISSING         | 0x8000011a | CKR_CITS_DAK_MISSING              |
| LUNA_RET_SIM_AUTHORIZATION_FAILED | 0x8000011b | CKR_SIM_AUTHORIZATION_FAILED      |
| LUNA_RET_SIM_VERSION_UNSUPPORTED  | 0x8000011c | CKR_SIM_VERSION_UNSUPPORTED       |
| LUNA_RET_SIM_CORRUPT_DATA         | 0x8000011d | CKR_SIM_CORRUPT_DATA              |
| LUNA_RET_ECC_MIC_MISSING          | 0x8000011e | CKR_CERTIFICATE_DATA_MISSING      |
| LUNA_RET_ECC_HOK_MISSING          | 0x8000011f | CKR_CERTIFICATE_DATA_MISSING      |
| LUNA_RET_ECC_HOC_MISSING          | 0x80000120 | CKR_CERTIFICATE_DATA_MISSING      |

| HSM Error                               | Hex Code   | PKCS#11 or SFNT Defined CKR Error |
|-----------------------------------------|------------|-----------------------------------|
| LUNA_RET_ECC_DAK_MISSING                | 0x80000121 | CKR_CERTIFICATE_DATA_MISSING      |
| LUNA_RET_ECC_DAC_MISSING                | 0x80000122 | CKR_CERTIFICATE_DATA_MISSING      |
| LUNA_RET_ROOT_CERT_MISSING              | 0x80000123 | CKR_CERTIFICATE_DATA_MISSING      |
| LUNA_RET_HOC_MISSING                    | 0x80000124 | CKR_CERTIFICATE_DATA_MISSING      |
| LUNA_RET_INVALID_CERTIFICATE_FUNCTION   | 0x80000125 | CKR_CERTIFICATE_DATA_INVALID      |
| LUNA_RET_N_TOO_LARGE                    | 0x80000200 | CKR_ARGUMENTS_BAD                 |
| LUNA_RET_N_TOO_SMALL                    | 0x80000201 | CKR_ARGUMENTS_BAD                 |
| LUNA_RET_M_TOO_LARGE                    | 0x80000202 | CKR_ARGUMENTS_BAD                 |
| LUNA_RET_M_TOO_SMALL                    | 0x80000203 | CKR_ARGUMENTS_BAD                 |
| LUNA_RET_WEIGHT_TOO_LARGE               | 0x80000204 | CKR_ARGUMENTS_BAD                 |
| LUNA_RET_WEIGHT_TOO_SMALL               | 0x80000205 | CKR_ARGUMENTS_BAD                 |
| LUNA_RET_TOTAL_WEIGHT_INVALID           | 0x80000206 | CKR_ARGUMENTS_BAD                 |
| LUNA_RET_MISSING_SPLITS                 | 0x80000207 | CKR_ARGUMENTS_BAD                 |
| LUNA_RET_SPLIT_DATA_INVALID             | 0x80000208 | CKR_ARGUMENTS_BAD                 |
| LUNA_RET_SPLIT_ID_INVALID               | 0x80000209 | CKR_ARGUMENTS_BAD                 |
| LUNA_RET_M_OF_N_PARAMETER_NOT_AVAILABLE | 0x8000020a | CKR_OPERATION_NOT_INITIALIZED     |
| LUNA_RET_M_OF_N_ACTIVATION_REQUIRED     | 0x8000020b | CKR_OPERATION_NOT_INITIALIZED     |
| LUNA_RET_TOO_MANY_WEIGHTS               | 0x8000020e | CKR_ARGUMENTS_BAD                 |
| LUNA_RET_MISSING_WEIGHT_VALUE           | 0x8000020f | CKR_ARGUMENTS_BAD                 |

| HSM Error                              | Hex Code   | PKCS#11 or SFNT Defined CKR Error |
|----------------------------------------|------------|-----------------------------------|
| LUNA_RET_MISSING_VALUE_FOR_M           | 0x80000210 | CKR_ARGUMENTS_BAD                 |
| LUNA_RET_MISSING_VALUE_FOR_N           | 0x80000211 | CKR_ARGUMENTS_BAD                 |
| LUNA_RET_MISSING_NUMBER_OF_VECTORS     | 0x80000212 | CKR_ARGUMENTS_BAD                 |
| LUNA_RET_MISSING_VECTOR                | 0x80000213 | CKR_ARGUMENTS_BAD                 |
| LUNA_RET_VECTOR_TOO_LARGE              | 0x80000214 | CKR_ARGUMENTS_BAD                 |
| LUNA_RET_VECTOR_TOO_SMALL              | 0x80000215 | CKR_ARGUMENTS_BAD                 |
| LUNA_RET_TOO_MANY_VECTORS_PROVIDED     | 0x80000216 | CKR_ARGUMENTS_BAD                 |
| LUNA_RET_INVALID_VECTOR_SIZE           | 0x80000217 | CKR_ARGUMENTS_BAD                 |
| LUNA_RET_M_OF_N_PARAMETER_EXIST        | 0x80000218 | CKR_FUNCTION_FAILED               |
| LUNA_RET_VECTOR_VERSION_INVALID        | 0x80000219 | CKR_DATA_INVALID                  |
| LUNA_RET_VECTOR_OF_DIFFERENT_SET       | 0x8000021a | CKR_ARGUMENTS_BAD                 |
| LUNA_RET_VECTOR_DUPLICATE              | 0x8000021b | CKR_ARGUMENTS_BAD                 |
| LUNA_RET_VECTOR_TYPE_INVALID           | 0x8000021c | CKR_ARGUMENTS_BAD                 |
| LUNA_RET_MISSING_COMMAND_PARAMETER     | 0x8000021d | CKR_ARGUMENTS_BAD                 |
| LUNA_RET_M_OF_N_CLONING_IS_NOT_ALLOWED | 0x8000021e | CKR_FUNCTION_NOT_SUPPORTED        |
| LUNA_RET_M_OF_N_IS_NOT_REQUIRED        | 0x8000021f | CKR_OPERATION_NOT_INITIALIZED     |
| LUNA_RET_M_OF_N_IS_NOT_INITIALIZED     | 0x80000220 | CKR_OPERATION_NOT_INITIALIZED     |
| LUNA_RET_M_OF_N_SECRET_INVALID         | 0x80000221 | CKR_GENERAL_ERROR                 |
| LUNA_RET_CCM_NOT_PRESENT               | 0x80000300 | CKR_FUNCTION_NOT_SUPPORTED        |
| LUNA_RET_CCM_NOT_SUPPORTED             | 0x80000301 | CKR_FUNCTION_NOT_SUPPORTED        |

| HSM Error                             | Hex Code   | PKCS#11 or SFNT Defined CKR Error |
|---------------------------------------|------------|-----------------------------------|
| LUNA_RET_CCM_UNREMOVABLE              | 0x80000302 | CKR_DATA_INVALID                  |
| LUNA_RET_CCM_CERT_INVALID             | 0x80000303 | CKR_DATA_INVALID                  |
| LUNA_RET_CCM_SIGN_INVALID             | 0x80000304 | CKR_DATA_INVALID                  |
| LUNA_RET_CCM_UPDATE_DENIED            | 0x80000305 | CKR_DATA_INVALID                  |
| LUNA_RET_CCM_FWUPDATE_DENIED          | 0x80000306 | CKR_DATA_INVALID                  |
| LUNA_RET_SM_ACCESS_ID_INVALID         | 0x80000400 | CKR_DATA_INVALID                  |
| LUNA_RET_SM_ACCESS_ALREADY_EXISTS     | 0x80000401 | CKR_DATA_INVALID                  |
| LUNA_RET_SM_MULTIPLE_ACCESS_DISABLED  | 0x80000402 | CKR_FUNCTION_NOT_SUPPORTED        |
| LUNA_RET_SM_UNKNOWN_ACCESS_TYPE       | 0x80000403 | CKR_ARGUMENTS_BAD                 |
| LUNA_RET_SM_BAD_ACCESS_HANDLE         | 0x80000404 | CKR_DATA_INVALID                  |
| LUNA_RET_SM_BAD_CONTEXT_NUMBER        | 0x80000405 | CKR_DATA_INVALID                  |
| LUNA_RET_SM_UNKNOWN_SESSION_TYPE      | 0x80000406 | CKR_DATA_INVALID                  |
| LUNA_RET_SM_CONTEXT_ALREADY_ALLOCATED | 0x80000407 | CKR_DATA_INVALID                  |
| LUNA_RET_SM_CONTEXT_NOT_ALLOCATED     | 0x80000408 | CKR_DEVICE_MEMORY                 |
| LUNA_RET_SM_CONTEXT_BUFFER_OVERFLOW   | 0x80000409 | CKR_DEVICE_MEMORY                 |
| LUNA_RET_SM_TOSM_DOES_NOT_VALIDATE    | 0x8000040A | CKR_USER_NOT_LOGGED_IN            |
| LUNA_RET_SM_ACCESS_DOES_NOT_VALIDATE  | 0x8000040B | CKR_USER_NOT_AUTHORIZED           |
| LUNA_RET_MTK_ZEROIZED                 | 0x80000531 | CKR_MTK_ZEROIZED                  |
| LUNA_RET_MTK_STATE_INVALID            | 0x80000532 | CKR_MTK_STATE_INVALID             |
| LUNA_RET_MTK_SPLIT_INVALID            | 0x80000533 | CKR_MTK_SPLIT_INVALID             |
| LUNA_RET_INVALID_IP_PACKET            | 0x80000600 | CKR_DEVICE_ERROR                  |



| HSM Error                              | Hex Code   | PKCS#11 or SFNT Defined CKR Error |
|----------------------------------------|------------|-----------------------------------|
| LUNA_RET_INVALID_BOARD_TYPE            | 0x80000700 | CKR_DEVICE_ERROR                  |
| LUNA_RET_ECC_NOT_SUPPORTED             | 0x80000601 | CKR_FUNCTION_NOT_SUPPORTED        |
| LUNA_RET_ECC_BUFFER_OVERFLOW           | 0x80000602 | CKR_DEVICE_ERROR                  |
| LUNA_RET_ECC_POINT_INVALID             | 0x80000603 | CKR_ECC_POINT_INVALID**           |
| LUNA_RET_ECC_SELF_TEST_FAILURE         | 0x80000604 | CKR_DEVICE_ERROR                  |
| LUNA_RET_ECC_UNKNOWN_CURVE             | 0x80000605 | CKR_ECC_UNKNOWN_CURVE             |
| LUNA_RET_HA_NOT_SUPPORTED              | 0x80000900 | CKR_FUNCTION_NOT_SUPPORTED        |
| LUNA_RET_HA_USER_NOT_INITIALIZED       | 0x80000901 | CKR_OPERATION_NOT_INITIALIZED     |
| LUNA_RET_HSM_STORAGE_FULL              | 0x80000902 | CKR_HSM_STORAGE_FULL              |
| LUNA_RET_CONTAINER_OBJECT_STORAGE_FULL | 0x80000903 | CKR_CONTAINER_OBJECT_STORAGE_FULL |
| LUNA_RET_KEY_NOT_ACTIVE                | 0x80000904 | CKR_KEY_NOT_ACTIVE                |
| LUNA_RET_CB_NOT_SUPPORTED              | 0x80000a01 | CKR_FUNCTION_NOT_SUPPORTED        |
| LUNA_RET_CB_PARAM_INVALID              | 0x80000a02 | CKR_CALLBACK_ERROR                |
| LUNA_RET_CB_NO_MEMORY                  | 0x80000a03 | CKR_DEVICE_MEMORY                 |
| LUNA_RET_CB_TIMEOUT                    | 0x80000a04 | CKR_CALLBACK_ERROR                |
| LUNA_RET_CB_RETRY                      | 0x80000a05 | CKR_CALLBACK_ERROR                |
| LUNA_RET_CB_ABORTED                    | 0x80000a06 | CKR_CALLBACK_ERROR                |
| LUNA_RET_CB_SYS_ERROR                  | 0x80000a07 | CKR_CALLBACK_ERROR                |
| LUNA_RET_CB_HIOS_HANDLE_INVALID        | 0x80000a10 | CKR_CALLBACK_ERROR                |
| LUNA_RET_CB_HIOS_ID_INVALID            | 0x80000a11 | CKR_CALLBACK_ERROR                |

| HSM Error                                | Hex Code   | PKCS#11 or SFNT Defined CKR Error |
|------------------------------------------|------------|-----------------------------------|
| LUNA_RET_CB_HIOS_CLOSED                  | 0x80000a12 | CKR_CALLBACK_ERROR                |
| LUNA_RET_CB_HIOS_CANCELED                | 0x80000a13 | CKR_CALLBACK_ERROR                |
| LUNA_RET_CB_HIOS_IO_ERROR                | 0x80000a14 | CKR_CALLBACK_ERROR                |
| LUNA_RET_CB_HIOS_SEND_TIMEOUT            | 0x80000a15 | CKR_CALLBACK_ERROR                |
| LUNA_RET_CB_HIOS_RECV_TIMEOUT            | 0x80000a16 | CKR_CALLBACK_ERROR                |
| LUNA_RET_CB_HIOS_STATE_INVALID           | 0x80000a17 | CKR_CALLBACK_ERROR                |
| LUNA_RET_CB_HIOS_OUTPUT_BUFFER_TOO_SMALL | 0x80000a18 | CKR_CALLBACK_ERROR                |
| LUNA_RET_CB_HIOS_INPUT_BUFFER_TOO_SMALL  | 0x80000a19 | CKR_CALLBACK_ERROR                |
| LUNA_RET_CB_HANDLE_INVALID               | 0x80000a20 | CKR_CALLBACK_ERROR                |
| LUNA_RET_CB_ID_INVALID                   | 0x80000a21 | CKR_CALLBACK_ERROR                |
| LUNA_RET_CB_REMOTE_ABORT                 | 0x80000a22 | CKR_CALLBACK_ERROR                |
| LUNA_RET_CB_REMOTE_CLOSED                | 0x80000a23 | CKR_CALLBACK_ERROR                |
| LUNA_RET_CB_REMOTE_ABANDONED             | 0x80000a24 | CKR_CALLBACK_ERROR                |
| LUNA_RET_CB_MUST_READ                    | 0x80000a25 | CKR_CALLBACK_ERROR                |
| LUNA_RET_CB_MUST_WRITE                   | 0x80000a26 | CKR_CALLBACK_ERROR                |
| LUNA_RET_CB_INVALID_CALL_FOR_THE_STATE   | 0x80000a27 | CKR_CALLBACK_ERROR                |
| LUNA_RET_CB_SYNC_ERROR                   | 0x80000a28 | CKR_CALLBACK_ERROR                |
| LUNA_RET_CB_PROT_DATA_INVALID            | 0x80000a29 | CKR_CALLBACK_ERROR                |
| LUNA_RET_LOG_FILE_NOT_OPEN               | 0x80000d00 | CKR_LOG_FILE_NOT_OPEN             |
| LUNA_RET_LOG_FILE_WRITE_ERROR            | 0x80000d01 | CKR_LOG_FILE_WRITE_ERROR          |
| LUNA_RET_LOG_BAD_FILE_NAME               | 0x80000d02 | CKR_LOG_BAD_FILE_NAME             |

| HSM Error                                | Hex Code   | PKCS#11 or SFNT Defined CKR Error   |
|------------------------------------------|------------|-------------------------------------|
| LUNA_RET_LOG_FULL                        | 0x8000d03  | CKR_LOG_FULL                        |
| LUNA_RET_LOG_NO_KCV                      | 0x8000d04  | CKR_LOG_NO_KCV                      |
| LUNA_RET_LOG_BAD_RECORD_HMAC             | 0x8000d05  | CKR_LOG_BAD_RECORD_HMAC             |
| LUNA_RET_LOG_BAD_TIME                    | 0x8000d06  | CKR_LOG_BAD_TIME                    |
| LUNA_RET_LOG_AUDIT_NOT_INITIALIZED       | 0x8000d07  | CKR_LOG_AUDIT_NOT_INITIALIZED       |
| LUNA_RET_LOG_RESYNC_NEEDED               | 0x8000d08  | CKR_LOG_RESYNC_NEEDED               |
| LUNA_RET_AUDIT_LOGIN_TIMEOUT_IN_PROGRESS | 0x8000d09  | CKR_AUDIT_LOGIN_TIMEOUT_IN_PROGRESS |
| LUNA_RET_AUDIT_LOGIN_FAILURE_THRESHOLD   | 0x8000d0a  | CKR_AUDIT_LOGIN_FAILURE_THRESHOLD   |
| LUNA_RET_XTC_ERROR                       | 0x80001600 | CKR_XTC_ERROR                       |
| LUNA_RET_CONTEXT_INVALID                 | 0x80001601 | CKR_CONTEXT_INVALID                 |
| LUNA_RET_SESSION_COUNT                   | 0x80001603 | CKR_MAX_SESSION_COUNT               |
| LUNA_RET_BUSY                            | 0x80001604 | CKR_BUSY                            |

\* This error (CKR\_TEMPLATE\_INCONSISTENT) might be encountered when using CKDemo in a new client with firmware older than version 6.22.0. Try CKDemo option 98, sub-option 16. If it is set to "enhanced roles", try selecting it to set it to "legacy Luna roles". The setting is a toggle, and flips every time you select it.

\*\* This error, or "unable to read public key", might be encountered when using BSAFE to encrypt data with ECC public key using curves from the Brainpool suite. As indicated on the BSAFE website (May 2012) they do not appear to support Brainpool curves. Therefore, your own applications should not attempt that combination, and you should avoid attempting to specify Brainpool curves with BSAFE ECC when using SafeNet's CKDemo utility.

## Library Codes

| Hex value  | Decimal value | Return code/error description  |
|------------|---------------|--------------------------------|
| 0          | 0             | OKAY, NO ERROR                 |
| 0xC0000000 | 3221225472    | PROGRAMMING ERROR: RETURN CODE |

| Hex value  | Decimal value | Return code/error description              |
|------------|---------------|--------------------------------------------|
| 0xC0000001 | 3221225473    | OUT OF MEMORY                              |
| 0xC0000002 | 3221225474    | NON-SPECIFIC ERROR                         |
| 0xC0000003 | 3221225475    | UNEXPECTED NULL POINTER                    |
| 0xC0000004 | 3221225476    | PROGRAMMING ERROR: LOGIC                   |
| 0xC0000005 | 3221225477    | OPERATION WOULD BLOCK IF ATTEMPTED         |
| 0xC0000006 | 3221225478    | BUFFER IS TOO SMALL                        |
| 0xC0000100 | 3221225728    | OPERATION CANCEL                           |
| 0xC0000101 | 3221225729    | INVALID SLOT IDENTIFIER                    |
| 0xC0000102 | 3221225730    | INVALID DATA                               |
| 0xC0000103 | 3221225731    | INVALID PIN                                |
| 0xC0000104 | 3221225732    | NO TOKEN PRESENT                           |
| 0xC0000105 | 3221225733    | FUNCTION IS NOT SUPPORTED                  |
| 0xC0000106 | 3221225734    | NON-CRYPTOKI ELEMENT CLONE                 |
| 0xC0000107 | 3221225735    | INVALID BUFFER SIZE FOR CHALLENGE          |
| 0xC0000108 | 3221225736    | PIN IS LOCKED                              |
| 0xC0000109 | 3221225737    | INVALID VERSION                            |
| 0xC000010a | 3221225738    | NEEDED KEY NOT PROVIDED                    |
| 0xC000010b | 3221225739    | USER NAME IS IN USE                        |
| 0xC0000200 | 3221225984    | INVALID DISTINGUISHED ENCODING RULES CLASS |
| 0xC0000303 | 3221226243    | OPERATION TIMED OUT                        |
| 0xC0000304 | 3221226244    | RESET FAILED                               |
| 0xC0000400 | 3221226496    | INVALID TOKEN STATE                        |

| Hex value  | Decimal value | Return code/error description |
|------------|---------------|-------------------------------|
| 0xC0000401 | 3221226497    | DATA APPEARS CORRUPTED        |
| 0xC0000402 | 3221226498    | INVALID FILENAME              |
| 0xC0000403 | 3221226499    | FILE IS READ-ONLY             |
| 0xC0000404 | 3221226500    | FILE ERROR                    |
| 0xC0000405 | 3221226501    | INVALID OBJECT IDENTIFIER     |
| 0xC0000406 | 3221226502    | INVALID SOCKET ADDRESS        |
| 0xC0000407 | 3221226503    | INVALID LISTEN SOCKET         |
| 0xC0000408 | 3221226504    | CACHE IS NOT CURRENT          |
| 0xC0000409 | 3221226505    | CACHE IS NOT MAPPED           |
| 0xC000040a | 3221226506    | OBJECT IS NOT IN LIST         |
| 0xC000040b | 3221226507    | INVALID INDEX                 |
| 0xC000040c | 3221226508    | OBJECT ALREADY EXISTS         |
| 0xC000040d | 3221226509    | SEMAPHORE ERROR               |
| 0xC000040e | 3221226510    | END OF LIST ENCOUNTERED       |
| 0xC000040f | 3221226511    | WOULD ASSIGN SAME VALUE       |
| 0xC0000410 | 3221226512    | INVALID GROUP NAME            |
| 0xC0000411 | 3221226513    | NOT HSM BACKUP TOKEN          |
| 0xC0000412 | 3221226514    | NOT PARTITION BACKUP TOKEN    |
| 0xC0000413 | 3221226515    | SIM NOT SUPPORTED             |
| 0xC0000500 | 3221226752    | SOCKET ERROR                  |
| 0xC0000501 | 3221226753    | SOCKET WRITE ERROR            |
| 0xC0000502 | 3221226754    | SOCKET READ ERROR             |
| 0xC0000503 | 3221226755    | CLIENT MESSAGE ERROR          |

| Hex value  | Decimal value | Return code/error description         |
|------------|---------------|---------------------------------------|
| 0xC0000504 | 3221226756    | SERVER DISCONNECTED                   |
| 0xC0000505 | 3221226757    | CLIENT DISCONNECTED                   |
| 0xC0000506 | 3221226758    | SOCKET WOULD BLOCK                    |
| 0xC0000507 | 3221226759    | SOCKET ADDRESS IS IN USE              |
| 0xC0000508 | 3221226760    | SOCKET BAD FILE DESCRIPTOR            |
| 0xC0000509 | 3221226761    | HOST RESOLUTION ERROR                 |
| 0xC000050a | 3221226762    | INVALID HOST CERTIFICATE              |
| 0xC0000600 | 3221227008    | NO BUFFER AVAILABLE                   |
| 0xC0000601 | 3221227009    | INVALID ENUMERATION OPTION            |
| 0xC0000700 | 3221227264    | SSL ERROR                             |
| 0xC0000701 | 3221227265    | SSL CTX ERROR                         |
| 0xC0000702 | 3221227266    | SSL CIPHER LIST ERROR                 |
| 0xC0000703 | 3221227267    | SSL CERT VERIFICATION LOCATION ERROR  |
| 0xC0000704 | 3221227268    | SSL LOAD SERVER CERT ERROR            |
| 0xC0000705 | 3221227269    | SSL LOAD SERVER PRIVATE KEY ERROR     |
| 0xC0000706 | 3221227270    | SSL VALIDATE SERVER PRIVATE KEY ERROR |
| 0xC0000707 | 3221227271    | SSL CREATE SSL ERROR                  |
| 0xC0000708 | 3221227272    | SSL LOAD CLIENT CERT ERROR            |
| 0xC0000709 | 3221227273    | SSL GET CERTIFICATE ERROR             |
| 0xC000070a | 3221227274    | SSL INVALID CERT STRUCTURE            |
| 0xC000070b | 3221227275    | SSL LOAD CLIENT PRIVATE KEY ERROR     |
| 0xC000070c | 3221227276    | SSL GET PEER CERT ERROR               |

| Hex value  | Decimal value | Return code/error description |
|------------|---------------|-------------------------------|
| 0xC000070d | 3221227277    | SSL WANT READ ERROR           |
| 0xC000070e | 3221227278    | SSL WANT WRITE ERROR          |
| 0xC000070f | 3221227279    | SSL WANT X509 LOOKUP ERROR    |
| 0xC0000710 | 3221227280    | SSL SYSCALL ERROR             |
| 0xC0000711 | 3221227281    | SSL FAILED HANDSHAKE          |
| 0xC0000800 | 3221227520    | INVALID CERTIFICATE TYPE      |
| 0xC0000900 | 3221227776    | INVALID PORT                  |
| 0xC0000901 | 3221227777    | SESSION SCRIPT EXISTS         |
| 0xC0001000 | 3221229568    | PARTITION LOCKED              |
| 0xC0001001 | 3221229569    | PARTITION NOT ACTIVATED       |
| 0xc0002000 | 3221233664    | FAILED TO CREATE THREAD       |
| 0xc0002001 | 3221233665    | CALLBACK ERROR                |
| 0xc0002002 | 3221233666    | UNKNOWN CALLBACK COMMAND      |
| 0xc0002003 | 3221233667    | SHUTTING DOWN                 |
| 0xc0002004 | 3221233668    | REMOTE SIDE DISCONNECTED      |
| 0xc0002005 | 3221233669    | SOCKET CLOSED                 |
| 0xC0002006 | 3221233670    | INVALID COMMAND               |
| 0xC0002007 | 3221233671    | UNKNOWN COMMAND               |
| 0xC0002008 | 3221233672    | UNKNOWN COMMAND VERSION       |
| 0xC0002009 | 3221233673    | FILE LOCK FAILED              |
| 0xC0002010 | 3221233680    | FILE LOCK ERROR               |
| 0xc0002011 | 3221233681    | FAILED TO CREATE PROCESS      |
| 0xc0002012 | 3221233682    | USB PED NOT FOUND             |

| Hex value  | Decimal value | Return code/error description |
|------------|---------------|-------------------------------|
| 0xc0002013 | 3221233683    | USB PED NOT RESPONDING        |
| 0xc0002014 | 3221233684    | USB PED OPERATION CANCELLED   |
| 0xc0002015 | 3221233685    | USB PED TOO MANY CONNECTED    |
| 0xc0002016 | 3221233686    | USB PED OUT OF SYNC           |
| 0xC0001100 | 3221229824    | UNABLE TO CONNECT             |

## Vendor-Defined Return Codes

| Code       | Name                                 |
|------------|--------------------------------------|
| 0x80000004 | CKR_RC_ERROR                         |
| 0x80000005 | CKR_CONTAINER_HANDLE_INVALID         |
| 0x80000006 | CKR_TOO_MANY_CONTAINERS              |
| 0x80000007 | CKR_USER_LOCKED_OUT                  |
| 0x80000008 | CKR_CLONING_PARAMETER_ALREADY_EXISTS |
| 0x80000009 | CKR_CLONING_PARAMETER_MISSING        |
| 0x8000000a | CKR_CERTIFICATE_DATA_MISSING         |
| 0x8000000b | CKR_CERTIFICATE_DATA_INVALID         |
| 0x8000000c | CKR_ACCEL_DEVICE_ERROR               |
| 0x8000000d | CKR_WRAPPING_ERROR                   |
| 0x8000000e | CKR_UNWRAPPING_ERROR                 |
| 0x8000000f | CKR_MAC_MISSING                      |
| 0x80000010 | CKR_DAC_POLICY_PID_MISMATCH          |
| 0x80000011 | CKR_DAC_MISSING                      |
| 0x80000012 | CKR_BAD_DAC                          |



| Code       | Name                           |
|------------|--------------------------------|
| 0x80000013 | CKR_SSK_MISSING                |
| 0x80000014 | CKR_BAD_MAC                    |
| 0x80000015 | CKR_DAK_MISSING                |
| 0x80000016 | CKR_BAD_DAK                    |
| 0x80000017 | CKR_SIM_AUTHORIZATION_FAILED   |
| 0x80000018 | CKR_SIM_VERSION_UNSUPPORTED    |
| 0x80000019 | CKR_SIM_CORRUPT_DATA           |
| 0x8000001a | CKR_USER_NOT_AUTHORIZED        |
| 0x8000001b | CKR_MAX_OBJECT_COUNT_EXCEEDED  |
| 0x8000001c | CKR_SO_LOGIN_FAILURE_THRESHOLD |
| 0x8000001d | CKR_SIM_AUTHFORM_INVALID       |
| 0x8000001e | CKR_CITS_DAK_MISSING           |
| 0x8000001f | CKR_UNABLE_TO_CONNECT          |
| 0x80000020 | CKR_PARTITION_DISABLED         |
| 0x80000021 | CKR_CALLBACK_ERROR             |
| 0x80000022 | CKR_SECURITY_PARAMETER_MISSING |
| 0x80000023 | CKR_SP_TIMEOUT                 |
| 0x80000024 | CKR_TIMEOUT                    |
| 0x80000025 | CKR_ECC_UNKNOWN_CURVE          |
| 0x80000026 | CKR_MTK_ZEROIZED               |
| 0x80000027 | CKR_MTK_STATE_INVALID          |
| 0x80000028 | CKR_INVALID_ENTRY_TYPE         |
| 0x80000029 | CKR_MTK_SPLIT_INVALID          |

| Code       | Name                                |
|------------|-------------------------------------|
| 0x8000002a | CKR_HSM_STORAGE_FULL                |
| 0x8000002b | CKR_DEVICE_TIMEOUT                  |
| 0x8000002c | CKR_CONTAINER_OBJECT_STORAGE_FULL   |
| 0x8000002d | CKR_PED_CLIENT_NOT_RUNNING          |
| 0x8000002e | CKR_PED_UNPLUGGED                   |
| 0x8000002f | CKR_ECC_POINT_INVALID               |
| 0x80000030 | CKR_OPERATION_NOT_ALLOWED           |
| 0x80000031 | CKR_LICENSE_CAPACITY_EXCEEDED       |
| 0x80000032 | CKR_LOG_FILE_NOT_OPEN               |
| 0x80000033 | CKR_LOG_FILE_WRITE_ERROR            |
| 0x80000034 | CKR_LOG_BAD_FILE_NAME               |
| 0x80000035 | CKR_LOG_FULL                        |
| 0x80000036 | CKR_LOG_NO_KCV                      |
| 0x80000037 | CKR_LOG_BAD_RECORD_HMAC             |
| 0x80000038 | CKR_LOG_BAD_TIME                    |
| 0x80000039 | CKR_LOG_AUDIT_NOT_INITIALIZED       |
| 0x8000003A | CKR_LOG_RESYNC_NEEDED               |
| 0x8000003B | CKR_AUDIT_LOGIN_TIMEOUT_IN_PROGRESS |
| 0x8000003C | CKR_AUDIT_LOGIN_FAILURE_THRESHOLD   |
| 0x8000003D | CKR_INVALID_FUF_TARGET              |
| 0x8000003E | CKR_INVALID_FUF_HEADER              |
| 0x8000003F | CKR_INVALID_FUF_VERSION             |
| 0x80000040 | CKR_ECC_ECC_RESULT_AT_INF           |

| Code       | Name                                      |
|------------|-------------------------------------------|
| 0x80000041 | CKR_AGAIN                                 |
| 0x80000042 | CKR_TOKEN_COPIED                          |
| 0x80000043 | CKR_SLOT_NOT_EMPTY                        |
| 0x80000044 | CKR_USER_ALREADY_ACTIVATED                |
| 0x80000045 | CKR_STC_NO_CONTEXT                        |
| 0x80000046 | CKR_STC_CLIENT_IDENTITY_NOT_CONFIGURED    |
| 0x80000047 | CKR_STC_PARTITION_IDENTITY_NOT_CONFIGURED |
| 0x80000048 | CKR_STC_DH_KEYGEN_ERROR                   |
| 0x80000049 | CKR_STC_CIPHER_SUITE_REJECTED             |
| 0x8000004a | CKR_STC_DH_KEY_NOT_FROM_SAME_GROUP        |
| 0x8000004b | CKR_STC_COMPUTE_DH_KEY_ERROR              |
| 0x8000004c | CKR_STC_FIRST_PHASE_KDF_ERROR             |
| 0x8000004d | CKR_STC_SECOND_PHASE_KDF_ERROR            |
| 0x8000004e | CKR_STC_KEY_CONFIRMATION_FAILED           |
| 0x8000004f | CKR_STC_NO_SESSION_KEY                    |
| 0x80000050 | CKR_STC_RESPONSE_BAD_MAC                  |
| 0x80000051 | CKR_STC_NOT_ENABLED                       |
| 0x80000052 | CKR_STC_CLIENT_HANDLE_INVALID             |
| 0x80000053 | CKR_STC_SESSION_INVALID                   |
| 0x80000054 | CKR_STC_CONTAINER_INVALID                 |
| 0x80000055 | CKR_STC_SEQUENCE_NUM_INVALID              |
| 0x80000056 | CKR_STC_NO_CHANNEL                        |
| 0x80000057 | CKR_STC_RESPONSE_DECRYPT_ERROR            |

| Code       | Name                                  |
|------------|---------------------------------------|
| 0x80000058 | CKR_STC_RESPONSE_REPLAYED             |
| 0x80000059 | CKR_STC_REKEY_CHANNEL_MISMATCH        |
| 0x8000005a | CKR_STC_RSA_ENCRYPT_ERROR             |
| 0x8000005b | CKR_STC_RSA_SIGN_ERROR                |
| 0x8000005c | CKR_STC_RSA_DECRYPT_ERROR             |
| 0x8000005d | CKR_STC_RESPONSE_UNEXPECTED_KEY       |
| 0x8000005e | CKR_STC_UNEXPECTED_NONCE_PAYLOAD_SIZE |
| 0x8000005f | CKR_STC_UNEXPECTED_DH_DATA_SIZE       |
| 0x80000060 | CKR_STC_OPEN_CIPHER_MISMATCH          |
| 0x80000061 | CKR_STC_OPEN_DHNIST_PUBKEY_ERROR      |
| 0x80000062 | CKR_STC_OPEN_KEY_MATERIAL_GEN_FAIL    |
| 0x80000063 | CKR_STC_OPEN_RESP_GEN_FAIL            |
| 0x80000064 | CKR_STC_ACTIVATE_MACTAG_U_VERIFY_FAIL |
| 0x80000065 | CKR_STC_ACTIVATE_MACTAG_V_GEN_FAIL    |
| 0x80000066 | CKR_STC_ACTIVATE_RESP_GEN_FAIL        |
| 0x80000067 | CKR_CHALLENGE_INCORRECT               |
| 0x80000068 | CKR_ACCESS_ID_INVALID                 |
| 0x80000069 | CKR_ACCESS_ID_ALREADY_EXISTS          |
| 0x8000006a | CKR_KEY_NOT_KEKABLE                   |
| 0x8000006b | CKR_MECHANISM_INVALID_FOR_FP          |
| 0x8000006c | CKR_OPERATION_INVALID_FOR_FP          |
| 0x8000006d | CKR_SESSION_HANDLE_INVALID_FOR_FP     |
| 0x8000006e | CKR_CMD_NOT_ALLOWED_HSM_IN_TRANSPORT  |

| Code       | Name                                          |
|------------|-----------------------------------------------|
| 0x8000006f | CKR_OBJECT_ALREADY_EXISTS                     |
| 0x80000070 | CKR_PARTITION_ROLE_DESC_VERSION_INVALID       |
| 0x80000071 | CKR_PARTITION_ROLE_POLICY_VERSION_INVALID     |
| 0x80000072 | CKR_PARTITION_ROLE_POLICY_SET_VERSION_INVALID |
| 0x80000073 | CKR_REKEK_KEY                                 |
| 0x80000074 | CKR_KEK_RETRY_FAILURE                         |
| 0x80000075 | CKR_RNG_RESEED_TOO_EARLY                      |
| 0x80000076 | CKR_HSM_TAMPERED                              |
| 0x80000077 | CKR_CONFIG_CHANGE_ILLEGAL                     |
| 0x80000078 | CKR_SESSION_CONTEXT_NOT_ALLOCATED             |
| 0x80000079 | CKR_SESSION_CONTEXT_ALREADY_ALLOCATED         |
| 0x8000007a | CKR_INVALID_BL_ITB_AUTH_HEADER                |
| 0x80000114 | CKR_OBJECT_READ_ONLY                          |
| 0x80000136 | CKR_KEY_NOT_ACTIVE                            |
| 0x80000400 | CKR_ACCESS_ID_INVALID                         |
| 0x80001600 | CKR_XTC_ERROR                                 |
| 0x80001601 | CKR_CONTEXT_INVALID                           |
| 0x80001603 | CKR_MAX_SESSION_COUNT                         |
| 0x80001604 | CKR_BUSY                                      |

## HSM Alarm-codes overview

The SafeNet Luna PCIe HSM alarm messages indicate error conditions on the HSM card that might require user intervention. The alarms apply to a SafeNet Luna HSM, compliant with security level FIPS 140-2 Level 3. The alarm messages provide appropriate detail to alert HSM users of important events. Each alarm message has a unique character string for the message ID that allows higher level tools on the host system to parse for the alarm message IDs and generate notifications.

Messages are saved to the system log file in Linux host systems, allowing host application software like SNMP to parse the log file, and to the Windows Event Viewer in Windows host systems

Messages can be retrieved with the "dmesg" utility, to read messages from the driver log, which collects messages from the bootloader (BL), the firmware (FW), or from the Host Driver itself.

## Alarm Generation and Handling

### Alarm Generation

Alarm messages can be generated due to the HSM BL, FW, and Host Driver SW detecting unexpected conditions. Other alarm messages are generated after unexpected interrupts or tamper events. For each of these problems detailed error information and an alarm message is output to notify the user that something special has happened.

At least one alarm message is output as a result of each tamper event by BL, FW, or Host Driver. Depending on the type of tamper all of them may report an alarm message related to the same tamper event. The message timestamps assist you to identify which alarm messages are for the same tamper event. Tamper alarm messages from BL, FW, and Host Driver have the same text description for the same tamper event. A specific type of tamper event is not reported again until FW clears the tamper information in the tamper circuit. If the tamper event happens after that, then either a new tamper condition has been detected or the same tamper event is still active and cannot be cleared.

### Alarm Handling for Special Situations

Alarm messages are still generated during rare occurrences where BL, FW, or Host Driver might be in an abnormal state.

As long as the Host Driver is running, the BL and FW are able to output their alarm messages to the DLOG (driver log), which can be parsed to notify the user. If either BL or FW stops execution due to error detection, they output an alarm message to the Host Driver, which stores it in DLOG. All BL and FW checking for alarm conditions is stopped but all HW tamper event monitoring (soft and hard tampers) is still enabled including Host Driver monitoring. The card reset caused by these tampers restarts BL and possibly FW and the alarm messages are output. The following situations are also handled:

- > **BL starts before Host Driver is loaded (System power-up):** Without Host Driver available, BL outputs all alarms only to an internal HSM log. When the Host Driver loads it resets the HSM card, causing BL to start again. BL can then send any new alarms to the host driver and either stop or proceed to FW, as the situation allows.
  - For an L3 card if FW is started it will output alarm messages for any existing tamper conditions. Any tamper event alarm messages including those not sent out while the Host Driver was not loaded can be fetched from the FRAM Log.

**NOTE** If needed, use Lunadiag to output the FRAM Log in order to determine the tamper information, or to pass on to Gemalto Technical Support if requested. (On the Network HSM, the lunash:> **hsm supportinfo** command invokes Lunadiag to retrieve the relevant information from the FRAM Log.)

- > **FW halted due to internal error:** In order to get to FW the Host Driver must be running so the FW halted alarm message will be stored in DLOG. No further BL or FW alarm messages are generated in this state until the next card reset.
- > **FW in locked state (tamper clear required):** An alarm message is generated to signal locked state is active. FW is still doing periodic checks and FW alarm messages are still possible. Only a small subset of FW commands is available.
- > **FW in Secure Transport Mode (STM):** An alarm message is generated to signal STM is active. FW is still doing periodic checks and FW alarm messages are still possible. Only a small subset of FW commands are available.
- > **Host Driver loses communications with the HSM card:** If the Host Driver has any errors communicating with the K7 (BL or FW) it will generate alarm messages. The Host Driver also periodically checks that the K7 card is still present on the PCIe bus (i.e. chassis open causes a cold reset of the K7) and if there is no response for a pre-determined period of time an alarm message is generated.

## FRAM LOG

The Boot Loader and firmware also store all alarm event information in the FRAM Log in the non-volatile FRAM device on the K7. There is no specific FRAM Log partition for DLOG or alarm messages. Use LUNADIAG to retrieve the FRAM Log contents and return it to Gemalto Support for further analysis. In the event the Host Driver is unavailable to receive this information, it is still present in the FRAM Log and can be retrieved long after the alarm event has finished.

## HSM Alarm Codes

| ALM ID             | Alarm Message                     | Description                                                                                                                          | Info               |
|--------------------|-----------------------------------|--------------------------------------------------------------------------------------------------------------------------------------|--------------------|
| <b>Host Driver</b> |                                   |                                                                                                                                      | <b>Tamper Flag</b> |
| 0001               | Soft tamper - over voltage        | HSM voltage is above the operating range. HSM will stay in reset until voltage goes back in range.                                   | HCCSR:<br>VST      |
| 0002               | Soft tamper - temperature (nnC)   | HSM temperature (nn degrees Celsius) is outside the range (-2C to 80C). HSM will stay in reset until temperature goes back in range. | HRCSR:<br>TST      |
| 0003               | Soft tamper - indeterminate cause | A soft tamper occurred but cannot determine the cause.                                                                               |                    |
| 0004               | Hard tamper - high temperature    | HSM temperature is higher than 88C.                                                                                                  | HT_T               |
| 0005               | Hard tamper - low temperature     | HSM temperature is lower than -40C                                                                                                   | LT_T               |

| ALM ID | Alarm Message                     | Description                                                                  | Info           |
|--------|-----------------------------------|------------------------------------------------------------------------------|----------------|
| 0006   | Hard tamper - over voltage        | HSM voltage is higher than the maximum allowed.                              | OV_T,<br>TC3_T |
| 0009   | Hard tamper - oscillator failure  | HSM tamper clock oscillator has failed                                       | OSC_T          |
| 0010   | Decommission signal triggered     | Decommission button (connector P9) has been pressed.                         | TC2_T          |
| 0011   | Hard tamper - indeterminate cause | A hard tamper occurred but cannot determine the cause.                       |                |
| 0012   | Hardware Error                    | Error detected in device hardware                                            |                |
| 0013   | High Temperature - nnC            | HSM has reached nn degrees Celsius and needs to be cooled to avoid tampering |                |
| 0014   | Low Battery                       | HSM battery voltage is below 2.75V and needs to be replaced soon.            |                |
| 0015   | PCIe Link Failure                 | HSM no longer appears on PCIe bus. Chassis may have been opened.             |                |
| 0016   | Device Error                      | Internal error detected during communications with HSM                       |                |
| 0017   | Request Timed Out                 | Request to HSM took too long                                                 |                |

| Boot Loader |                                         |                                                                                                    | Tamper Flag |
|-------------|-----------------------------------------|----------------------------------------------------------------------------------------------------|-------------|
| 1000        | Unknown alarm ID xx in boot loader      | Illegal alarm ID used in Boot Loader.                                                              |             |
| 1001        | HSM restart required                    | Soft or hard tamper occurred. HSM needs to be restarted (reset) before firmware is allowed to run. |             |
| 1003        | HSM halted - internal boot loader error | Boot Loader detected an error during diagnostics and did not jump to FW.                           |             |



| ALM ID          | Alarm Message                              | Description                                                                                                                                  | Info              |
|-----------------|--------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------|-------------------|
| 1004            | Warning - boot loader diagnostic error     | Boot Loader detected an error during diagnostics that does not stop execution but needs to be investigated (i.e. fan, VPD, or RTC problems). |                   |
| 1005            | HSM FW signature check failed              | The FW image on the HSM failed authentication and will not be executed.                                                                      |                   |
| 1006            | Soft tamper temperature/voltage            | HSM voltage or temperature is outside the acceptable range. HSM will stay in reset until back in range.                                      | PORSM status reg. |
| 1007            | Hard tamper - high temperature             | HSM voltage or temperature is outside the acceptable range. HSM will stay in reset until back in range.                                      | HT_T              |
| 1008            | Hard tamper - low temperature              | HSM temperature is lower than -40C.                                                                                                          | LT_T              |
| 1009            | Hard tamper - over voltage                 | HSM voltage is higher than the maximum allowed.                                                                                              | OV_T, TC3_T       |
| 1012            | Hard tamper - oscillator failure           | HSM tamper clock oscillator has failed                                                                                                       | OSC_T             |
| 1013            | Hard tamper - tamper configuration invalid | HSM tamper configuration lost (set to defaults) due to power loss.                                                                           | FS_T              |
| 1014            | Chassis opened                             | Chassis open switch (connector P7) has been triggered.                                                                                       | TC1_T             |
| 1015            | HSM removed from chassis                   | HSM was removed from host chassis then re-inserted                                                                                           | CS                |
| 1016            | Decommission signal triggered              | Decommission button (connector P9) has been pressed.                                                                                         | TC2_T             |
| <b>Firmware</b> |                                            |                                                                                                                                              |                   |
| 2000            | Unknown alarm ID xx in firmware            | Illegal alarm ID used in firmware.                                                                                                           |                   |

| ALM ID | Alarm Message                        | Description                                                                                                                                                                                                                                                     | Info |
|--------|--------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------|
| 2001   | High temperature warning activated   | HSM temperature is above 75C (FW checks every 2 minutes). This warning will not re-appear unless temperature drops below 75C and goes back up again.                                                                                                            |      |
| 2002   | High temperature warning deactivated | HSM temperature has dropped below 75C.                                                                                                                                                                                                                          |      |
| 2003   | Battery low voltage warning          | Battery voltage is below 2.75V (FW checks every hour). This warning will not re-appear unless voltage goes above 2.75V then back down. Battery should to be replaced soon.                                                                                      |      |
| 2004   | Battery depleted                     | Battery voltage is below 2.5V (FW checks every hour). HSM FW will be halted. Battery must to be replaced.                                                                                                                                                       |      |
| 2005   | HSM deactivated                      | Auto-activation data has been cleared                                                                                                                                                                                                                           |      |
| 2006   | HSM decommissioned by FW             | All user crypto material has been invalidated due to KEK CRC failure, decommission signal, or tamper (if decommission on tamper enabled).                                                                                                                       |      |
| 2007   | HSM zeroized                         | All user crypto material has been erased. HSM product credentials still exist. This can occur for a variety of reasons including manual zeroization.                                                                                                            |      |
| 2008   | Internal data corruption             | Settings to control tamper monitoring are incorrect or Critical Security Parameter data (MTK) is invalid (For L3 card, the tamper monitoring settings if incorrect are corrected. ). Otherwise there was an unexpected tamper security write protection change. |      |
| 2009   | HSM halted - internal firmware error | FW detected an error which caused it to halt itself. Can also be errors generated by the kernel such as: bad exception, out of memory, unrecoverable errors.                                                                                                    |      |

| ALM ID | Alarm Message                                  | Description                                                                                                                                                                               | Info           |
|--------|------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------|
| 2010   | HSM locked - tamper clear required             | Limited set of FW commands available due to an HSM tamper condition. Tamper needs to be cleared before proceeding. Controlled tamper recovery must be enabled for this message to appear. |                |
| 2011   | HSM unlocked - tamper clear done               | Tamper was cleared when in controlled tamper recovery mode.                                                                                                                               |                |
| 2012   | HSM in secure transport mode                   | Checked on every FW start-up to remind the user to do a recovery operation. Limited set of FW commands available.                                                                         |                |
| 2013   | HSM recovered from secure transport mode       | HSM in secure transport mode was recovered back to normal mode.                                                                                                                           |                |
| 2014   | Auto-activation data invalid – HSM deactivated | FW checked auto-activation data validity and failed. Re-activation required.                                                                                                              |                |
| 2015   | Hard tamper - high temperature                 | (L3 only) HSM temperature was higher than 88C.                                                                                                                                            | HT_T           |
| 2016   | Hard tamper - low temperature                  | (L3 only) HSM temperature was lower than -40C.                                                                                                                                            | LT_T           |
| 2017   | Hard tamper - over voltage                     | (L3 only) HSM voltage was higher than the maximum allowed.                                                                                                                                | OV_T,<br>TC3_T |
| 2018   | Hard tamper - oscillator failure               | (L3 only) HSM tamper clock oscillator has failed                                                                                                                                          | OSC_T          |
| 2019   | Hard tamper - tamper configuration invalid     | (L3 only) HSM tamper configuration lost (set to defaults) due to power loss.                                                                                                              | FS_T           |
| 2020   | Chassis opened                                 | Chassis open switch (connector P7) has been triggered.                                                                                                                                    | TC1_T          |
| 2021   | HSM was removed from chassis                   | HSM was removed from host chassis just before this FW execution. HSM will be deactivated.                                                                                                 | CS             |

| ALM ID | Alarm Message                 | Description                                          | Info  |
|--------|-------------------------------|------------------------------------------------------|-------|
| 2022   | Decommission signal triggered | Decommission button (connector P9) has been pressed. | TC2_T |
| 2023   | HSM fan x failure             | Fault detected in HSM on-board fan (fan 1 or fan 2). |       |

## HSM Alarm-codes samples

This section shows the details of some of the alarm event scenarios.

ALM = alarm message.

### Temperature - High Warning

If HSM temperature reaches 75 degrees Celsius and then drops back below 75C the following actions occur:

- > Temperature  $\geq$  75C
  - After 5 minutes at this temperature or higher, the Host Driver receives a 'High Temperature Warning' interrupt and issues an ALM
  - Firmware checks temperature at start-up and once per hour
  - Firmware issues ALM for high temperature warning activated
- > Temperature  $<$  75C
  - Firmware issues ALM for high temperature warning deactivated

### Temperature – High Soft Tamper

When the temperature starts below 75C and reaches the high soft tamper limit of 80C and then drops back below 75C the following actions occur:

- > Temperature  $\geq$  75C
  - After 5 minutes at this temperature or higher, the Host Driver receives a High Temperature Warning interrupt and issues an ALM
  - Firmware issues ALM for activation of high temperature warning
- > Temperature  $\geq$  80C
  - Soft Tamper reset – card put into reset. Stays in reset until temperature lowers.
  - Host Driver receives soft tamper interrupt and issues ALM (only one when soft tamper condition starts).
- > Temperature  $<$  80C
  - Bootloader issues soft tamper ALM, then an ALM that HSM restart is required and waits for host reset.
  - User receives ALM and goes to LunaCM/Lunash to do an “hsm restart” command.
  - Bootloader starts – jumps to firmware.

- Firmware starts – no actions taken for the soft tamper. If temperature  $\geq 75\text{C}$ , firmware re-issues ALM for activation of high temperature warning.
- > Temperature  $< 75\text{C}$
- Firmware issues ALM for deactivation of high temperature warning.

## Temperature – High Hard Tamper

When the temperature starts below  $75\text{C}$  and reaches high hard tamper limit of  $88\text{C}$  and then drops back below  $75\text{C}$  the following actions occur:

- > Same as soft tamper described above up to when card is held in soft tamper reset
- > Temperature  $> 88\text{C}$
- Hard Tamper reset – Card in hard tamper reset for 5 seconds then returns to soft tamper reset. K7 HW does erase/reset of all internal temporary memory. Tamper chip latches time and type of tamper. Host driver receives hard tamper interrupt and issues ALM.
  - HSM also erases auto-activation and STM data in tamper chip
  - If decommission on tamper is enabled then key encryption data is erased in tamper chip as well
- > Temperature  $< 80\text{C}$
- Bootloader starts – issues hard tamper ALM and logs it in FRAM Log
  - Bootloader issues ALM that HSM restart is required and waits for host reset.
  - User receives ALM and goes to LunaCM/Lunash to perform an **hsm restart** command.
  - Bootloader starts – jumps to firmware.
  - Firmware starts – saves hard tamper latches. If controlled tamper recovery is enabled, firmware locks HSM commands to a minimal subset only, and issues ALM for HSM locked. User must go to LunaCM/Lunash and perform a “tamper clear” command to get a full HSM command set. When tamper clear is issued, firmware outputs an ALM for HSM unlocked.
  - Firmware – issues deactivation and decommission (if enabled for tamper) ALMs
  - Firmware - temperature  $\geq 75\text{C}$ , firmware re-issues ALM for activation of high temperature warning
- > Temperature  $< 75\text{C}$
- Firmware issues ALM for deactivation of high temperature warning
- > Temperature  $< 80\text{C}$
- Bootloader starts – issues hard tamper ALM
  - Bootloader erases all of flash except for Boot Loader area and issues ALM for 'HSM permanently tampered'
  - Bootloader issues ALM that 'HSM restart is required' and waits for host reset.
  - User receives ALM and goes to LunaCM/Lunash to do an “hsm restart” command.
  - Bootloader starts – Only bootloader commands are available. Bootloader again issues 'ALM for HSM permanently tampered'. User can dump the FRAM Log using LUNADIAG.

## Hard Tamperers During Storage

When the HSM is powered off its tamper detection is powered by the on-card battery. Some hard tamperers can occur when main power is not applied. The condition that caused the tamper might not be present (for example high or low temperature) when the HSM is powered back on, while others might never turn off (for example enclosure penetration, oscillator failure). If they occur while in storage, then after the HSM is powered up, the bootloader runs and logs the tamper events in FRAM Log and the serial port. Since the host K7 driver has not started yet, none of the messages from the bootloader are sent to the host, but other alarm messages are output later to notify the user.

- Bootloader waits for the host driver to be loaded
- When the host driver starts up it immediately resets the HSM causing the bootloader to run again
- Bootloader does not re-log the same tamper events
- Bootloader jumps to firmware which outputs the ALM for the tamper event. If controlled tamper recovery is enabled firmware also outputs an ALM for the 'HSM is locked and a tamper clear is required'. The user can then use LunaCM or Lunash to clear the tamper

**NOTE** If needed, use Lunadiag to output the FRAM Log in order to determine the tamper information, or to pass on to Gemalto Technical Support if requested. (On the Network HSM, the lunash:> **hsm supportinfo** command invokes Lunadiag to retrieve the relevant information from the FRAM Log.)

## Decommission with power on

If the HSM is powered on and a decommission is triggered either by the decommission switch or by a tamper (if decommission on tamper is enabled) then the HSM goes into reset for 5 seconds. The following alarm messages are output to FRAM Log, serial port, and host driver:

- > The host driver immediately receives an interrupt and outputs an 'ALM for decommission triggered'
- > After 5 seconds lapses, the bootloader starts running and also outputs an 'ALM for decommission triggered'
- > Bootloader outputs an ALM for 'HSM restart required' and then waits
- > User gets alarm notification and performs an HSM restart
- > Bootloader restarts and jumps to firmware which finishes the decommission operations and firmware outputs an ALM for 'HSM decommissioned by firmware' and an ALM for 'HSM locked' (if enabled)

## Decommission with power off

If the HSM is powered off and a decommission is triggered either by the decommission switch or by a tamper (if decommission on tamper is enabled) then the decommission is latched in the tamper chip. When the HSM is powered on the following alarm messages are output:

- > Bootloader starts running and outputs an ALM for 'Decommission triggered' only to FRAM Log and serial port since the host driver is not loaded yet
- > Bootloader waits for the driver to be loaded which then forces a host reset
- > Bootloader restarts and jumps to firmware which finishes the decommission operations and firmware outputs an ALM for 'HSM decommissioned by firmware' and an ALM for 'HSM locked' (if enabled)

**NOTE** If needed, use Lunadiag to output the FRAM Log in order to determine the tamper information, or to pass on to Gemalto Technical Support if requested. (On the Network HSM, the lunash:> **hsm supportinfo** command invokes Lunadiag to retrieve the relevant information from the FRAM Log.)

### Chassis open with power on

If the HSM is powered on and the chassis open switch triggered then a cold reset is performed on the HSM which effectively removes the HSM from the PCIe bus. After about 10 seconds the HSM is released from reset and the following alarm messages are output:

- > Host Driver notices the device is no longer present on the PCIe bus and outputs an ALM for 'HSM missing from PCIe bus'
- > Bootloader starts running and outputs an ALM for 'HSM chassis opened' only to FRAM Log and serial port
- > Bootloader waits for the driver to be loaded
- > User gets notification of missing HSM and powers off then on the host system
- > Bootloader starts running and does not re-log the same tamper events
- > Bootloader waits for the host driver to be loaded
- > When the host driver starts up it immediately resets the HSM causing Bootloader to run again
- > Bootloader jumps to firmware which finishes the chassis opened operations and firmware outputs an ALM for 'HSM chassis opened' and an ALM for 'HSM locked' (if enabled).

**NOTE** If the chassis is still open then the HSM performs a cold reset after the tampers are cleared by firmware.

**NOTE** If needed, use Lunadiag to output the FRAM Log in order to determine the tamper information, or to pass on to Gemalto Technical Support if requested. (On the Network HSM, the lunash:> **hsm supportinfo** command invokes Lunadiag to retrieve the relevant information from the FRAM Log.)

### Chassis open with power off

If the HSM is powered off and the chassis open switch triggered then the chassis open is latched in the tamper chip. When the HSM is powered on the following alarm messages are output:

- > Bootloader starts running and outputs an ALM for 'HSM chassis opened' only to FRAM Log and serial port
- > Bootloader waits for the driver to be loaded which then forces a host reset
- > Bootloader starts running and does not re-log the same tamper events
- > Bootloader jumps to firmware which finishes the chassis opened operations and firmware outputs an ALM for 'HSM chassis opened' and an ALM for 'HSM locked' (if enabled)

**NOTE** If the chassis is still open then the HSM performs a cold reset after the tampers are cleared by firmware.

## Card removal

When an HSM is powered off and removed from the chassis a card removal latch is saved in the tamper chip. When the HSM is powered on the following alarm messages are output:

- > Bootloader starts running and outputs an ALM for 'card removal' only to FRAM Log and serial port
- > Bootloader waits for the driver to be loaded which then forces a host reset
- > Bootloader starts running and does not re-log the same tamper events
- > Bootloader restarts and jumps to firmware which outputs an ALM for 'HSM was removed from the chassis' and an ALM for 'HSM locked' (if enabled)

**NOTE** If needed, use Lunadiag to output the FRAM Log in order to determine the tamper information, or to pass on to Gemalto Technical Support if requested. (On the Network HSM, the `lunash:> hsm supportinfo` command invokes Lunadiag to retrieve the relevant information from the FRAM Log.)



# CHAPTER 23: Updates and Upgrades

Thales Group releases periodic updates to the SafeNet Luna Network HSM appliance software and the HSM firmware, as well as updated versions of the SafeNet Luna HSM Client software. If you have recently purchased a new SafeNet Luna Network HSM and your organization requires FIPS certification, you can download and install a FIPS-validated version of the HSM firmware. You can download these updates as they become available from the Thales Group Customer Support Portal: <https://supportportal.gemalto.com>.

Depending on the model of SafeNet Luna Network HSM you selected at time of purchase, you may also be able to purchase upgrades to the HSM's capabilities, or increase the number of partitions you can create. These upgrades are provided through the Thales Group Licensing Portal (GLP).

The following chapter provides tested update paths and procedures for installing update packages, as well as a list of the version dependencies for certain features. It contains the following sections:

- > "Update Considerations" below
- > "Version Dependencies by Feature" below
- > "Updating the SafeNet Luna HSM Client" on page 396
- > "Updating the SafeNet Luna Network HSM Appliance Software" on page 397
- > "Updating the SafeNet Luna HSM Firmware" on page 398
- > "Updating the SafeNet Luna Backup HSM Firmware" on page 399
- > "Rolling Back the SafeNet Luna HSM Firmware" on page 400
- > "Upgrading HSM Capabilities and Partition Licenses" on page 401

## Update Considerations

---

Before you install any of the updates, consider the following guidelines:

- > Back up all important cryptographic material.
- > Stop all client applications running cryptographic operations on the HSM.
- > If you are using STC on the HSM Admin channel, disable it by running `lunash:> hsm stc disable` before you update the HSM firmware.
- > 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.

## Version Dependencies by Feature

---

Some of the SafeNet Luna Network HSM functionality described in the documentation has been introduced in updates since the initial product release. For your own reasons, you may wish to apply some aspects of a product update and not others. For example:

- > you may choose to update appliance or client software while keeping an earlier, FIPS-certified firmware version
- > if you are maintaining a large number of client workstations, it may be cumbersome to apply software updates to all of them

The following table outlines the SafeNet Luna Network HSM functions that depend on a certain software/firmware version, or have other requirements you must consider.

| Function                                                                                                                                                                                                             | Minimum Version Requirements                                          | Notes                                                                                                                                                                                                                                                                                                                          |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>DPoD HSM on Demand Support</b><br>> <a href="#">Adding a DPoD HSM on Demand Service</a>                                                                                                                           | <b>Client:</b> 10.1                                                   | Refer to <a href="#">"Cloning Keys Between Luna 6, Luna 7, and HSM on Demand"</a> on page 238 for more information on using an HSMoD service with Luna HSMs.                                                                                                                                                                   |
| <b>Remote PED Server Support on Linux Clients</b><br>> <a href="#">"Remote PED Setup"</a> on page 257                                                                                                                | <b>Client:</b> 10.1                                                   |                                                                                                                                                                                                                                                                                                                                |
| <b>Client NTLS Certificates can be Signed by a Trusted Certificate Authority</b><br>> <a href="#">"Creating an NTLS Connection Using a Client Certificate Signed by a Trusted Certificate Authority"</a> on page 131 | <b>Client:</b> 10.1                                                   |                                                                                                                                                                                                                                                                                                                                |
| <b>SafeNet Luna Backup HSM (G7 model) Support</b><br>> <a href="#">"Backup and Restore Using a G7-Based Backup HSM"</a> on page 76                                                                                   | <b>Client:</b> 7.5                                                    |                                                                                                                                                                                                                                                                                                                                |
| <b>Functionality Modules</b><br>> <a href="#">"Functionality Modules"</a> on page 177<br>> <a href="#">About the FM SDK Guide</a>                                                                                    | <b>Firmware:</b> 7.4.0<br><b>Appliance:</b> 7.4<br><b>Client:</b> 7.4 | Refer to <a href="#">"Preparing the SafeNet Luna Network HSM to Use FMs"</a> on page 180 for an overview of hardware/software/firmware requirements.                                                                                                                                                                           |
| <b>Appliance Re-image</b><br>> <a href="#">"Re-Imaging the Appliance to Factory Baseline"</a> on page 168                                                                                                            | <b>Firmware:</b> 7.3.0<br><b>Appliance:</b> 7.3                       | The Appliance Re-image feature is not supported on HSMs that use Functionality Modules. If you have ever enabled <b>HSM policy 50: Allow Functionality Modules</b> , even if the policy is currently disabled, you cannot re-image the HSM appliance. See <a href="#">"FM Deployment Constraints"</a> on page 177 for details. |

| Function                                                                                                                                                                                                                                                                                                                                                                                                      | Minimum Version Requirements                                          | Notes                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Partition Utilization Metrics</b><br>> <a href="#">"Partition Utilization Metrics" on page 26</a>                                                                                                                                                                                                                                                                                                          | <b>Firmware:</b> 7.3.0<br><b>Appliance:</b> 7.3<br><b>Client:</b> 7.3 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| <b>Improved SafeNet Luna HSM Client</b><br>> Version-Compatible SafeNet Luna HSM Client (Luna HSMs version 6.2.1 and higher)<br>> <a href="#">"Cloning Keys Between Luna 6, Luna 7, and HSM on Demand" on page 238</a><br>> <a href="#">"Modifying the installed SafeNet Luna HSM Client software" on page 1</a><br>> User-Defined SafeNet Luna HSM Client install paths<br>> Luna Minimal Client (for Linux) | <b>Client:</b> 7.2                                                    | <ul style="list-style-type: none"> <li>&gt; SafeNet Luna HSM Client 10.1 or higher is required to use Luna partitions with DPoD's HSM on Demand services</li> <li>&gt; The <b>PE1756Enabled</b> setting on Luna 6.x HSMs is not supported for use with the Version-Compatible SafeNet Luna HSM Client</li> <li>&gt; Minimum OS requirements for SafeNet Luna HSM Client 7.2 must be met (Refer to the CRN for details)</li> <li>&gt; Minimal Client does not include tools, and is intended for customer application containers connecting to the Network HSM. A separate full SafeNet Luna HSM Client installation and configuration must be performed on the container host (and the resulting config file and certificate folders saved on the host), to establish NTLS or STC connections for use by the containers.</li> </ul> |
| <b>Initialize the orange RPV key remotely</b><br>> <a href="#">"Remote RPV Initialization" on page 259</a>                                                                                                                                                                                                                                                                                                    | <b>Appliance:</b> 7.2<br><b>Client:</b> 7.2                           |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| <b>Configure Cipher Suites</b><br>> <a href="#">Set TLS Ciphers</a>                                                                                                                                                                                                                                                                                                                                           | <b>Appliance:</b> 7.2<br><b>Client:</b> 7.2                           | The Luna 7.2 appliance update includes the <b>sysconf tls ciphers</b> LunaSH commands, but you must update SafeNet Luna HSM Client to use any of the newly-included ciphers. For older clients, the ciphers available for negotiation are those that are common to your client version and to the updated Network HSM.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |

| Function                                                                                                                                                                                   | Minimum Version Requirements                                             | Notes                                                                                                                                                                                                                                                                                                                                      |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Customize system logging by severity level</b><br>> <a href="#">"Customizing Severity Levels" on page 1</a><br>> <a href="#">"Customizing Remote Logging Severity Levels" on page 1</a> | <b>Appliance:</b> 7.2                                                    | If you were using remote logging before you upgraded the appliance software to 7.2, you must delete any existing remote hosts (see <a href="#">"syslog remotehost delete" on page 1</a> ) and re-add them before you can customize severity levels.                                                                                        |
| <b>Re-name/Re-label partitions</b><br>> <a href="#">"partition rename" on page 1</a><br>> <a href="#">"partition changelabel" on page 1</a>                                                | <b>Firmware:</b><br>7.2.0<br><b>Appliance:</b> 7.2<br><b>Client:</b> 7.2 |                                                                                                                                                                                                                                                                                                                                            |
| <b>Crypto User can clone public objects</b>                                                                                                                                                | <b>Firmware:</b><br>7.2.0                                                | The Crypto User (CU) role has always been able to create public objects, but not clone them. In HA mode, this would cause the replication and subsequent object creation operations to fail. Firmware 7.2.0 allows the CU to clone public objects, and therefore to perform operations on HA groups without Crypto Officer authentication. |
| <b>Configure partition policies for export of private keys</b><br>> <a href="#">"Configuring the Partition for Cloning or Export of Private Keys" on page 118</a>                          | <b>Firmware:</b><br>7.1.0                                                | You can configure partition policies for Cloning or Key Export Mode manually, as long as you have updated the HSM firmware. To set these modes using Policy Templates, you must meet the Policy Template requirements.                                                                                                                     |
| <b>Policy Templates</b><br>> <a href="#">"Setting HSM Policies Using a Template" on page 104</a><br>> <a href="#">"Setting Partition Policies Using a Template" on page 114</a>            | <b>Firmware:</b><br>7.1.0<br><b>Appliance:</b> 7.1<br><b>Client:</b> 7.1 |                                                                                                                                                                                                                                                                                                                                            |

## Updating the SafeNet Luna HSM Client

To update the SafeNet 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 [SafeNet Luna HSM Client Software Installation](#)).

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.

## Updating the SafeNet Luna Network HSM Appliance Software

The SafeNet Luna Network HSM appliance software consists of the LunaSH command-line shell and its underlying software components. Use the following procedure to install the SafeNet Luna Network HSM 10.1 appliance software update.

The update package includes an image of the latest HSM firmware, which you must install to take advantage of all the new features in this release. When you install the appliance software update, the latest firmware image is stored on the appliance file system but not installed. The system can only hold one firmware version in reserve at a time.

Firmware installation is a separate procedure (see ["Updating the SafeNet Luna HSM Firmware" on the next page](#)).

**NOTE** The appliance software update cannot be rolled back directly. You can re-image to a predetermined configuration and then update to a desired appliance software version [see ["Re-Imaging the Appliance to Factory Baseline" on page 168](#)]. The HSM firmware, however, can be rolled back to the previously-installed version (see ["Rolling Back the SafeNet Luna HSM Firmware" on page 400](#)).

To update the appliance software and firmware, you must transfer and apply a secure package file to the SafeNet Luna Network HSM. You require:

- > SafeNet Luna Network HSM 10.1 appliance software update package file (<filename>.spkg)
- > the secure package authentication code, provided in a text file accompanying the update package

### To upgrade the SafeNet Luna Network HSM appliance software

1. Transfer the secure package update file to the SafeNet Luna Network HSM using **scp** or **pscp** (see ["SCP and PSCP" on page 1](#) in the *Utilities Guide*).

|                   |                                                               |
|-------------------|---------------------------------------------------------------|
| <b>Linux/UNIX</b> | <b>scp</b> <path>/<filename>.spkg admin@<appliance_host/IP>:  |
| <b>Windows</b>    | <b>pscp</b> <path>\<filename>.spkg admin@<appliance_host/IP>: |

2. Stop all client applications to the SafeNet Luna Network HSM appliance.
3. Using a serial or SSH connection, log in to the appliance as **admin** (see ["Logging In to LunaSH" on page 421](#)).
4. Log in as HSM SO (see ["Logging In as HSM Security Officer" on page 431](#)).  
lunash:> **hsm login**
5. [Optional Step] Verify that the secure package file is present on the SafeNet Luna Network HSM.  
lunash:> **package listfile**
6. [Optional Step] Verify the package file, specifying the authorization code you received from Thales Group.  
lunash:> **package verify** <filename>.spkg **-authcode** <code\_string>
7. Install the update on the SafeNet Luna Network HSM.  
lunash:> **package update** <filename>.spkg **-authcode** <code\_string>

The installation/update process takes approximately one and a half minutes. A series of messages shows the progress of the update. At the end of this process, a message “Software update completed!” appears.

8. Reboot the SafeNet Luna Network HSM appliance.

```
lunash:> sysconf appliance reboot
```

The latest firmware update package is now stored in reserve on the appliance, waiting to be installed. See ["Updating the SafeNet Luna HSM Firmware" below](#) to install the firmware.

## Updating the SafeNet Luna HSM Firmware

A new SafeNet Luna Network HSM is delivered with the current FIPS- validated firmware installed on the HSM card, and the most recently released firmware version saved on the SafeNet Luna Network HSM hard drive as an optional update. When you install an appliance software update, this optional update is replaced with the latest firmware version. If you wish to use a different HSM firmware version, you can download it from the Thales Group Support Portal.

To update the firmware on a SafeNet Luna Backup HSM, see ["Updating the SafeNet Luna Backup HSM Firmware" on the next page](#).

**CAUTION!** Use an uninterruptible power supply (UPS) to power your HSM. There is a small chance that a power failure during an update could leave your HSM in an unrecoverable condition.

### Updating the HSM Firmware After an Appliance Software Update

After an appliance software update, the latest firmware version is saved on the appliance and ready to install.

#### To update the HSM firmware after a software appliance update

1. Log in to LunaSH on the appliance as **admin**.
2. At the LunaSH prompt, login as HSM SO.
3. [Optional Step] Check that the desired firmware version is ready to install.

```
lunash:> hsm firmware show
```

**CAUTION!** If you are using STC on the HSM Admin channel, disable it by running `lunash:> hsm stc disable` before you update the HSM firmware.

4. Update the firmware to the version currently stored on the appliance.

```
lunash:> hsm firmware upgrade
```

### Updating the HSM Firmware to a Different Version

If you are not installing the firmware update provided in the appliance software update, download your desired HSM firmware from the Thales Group Support Portal. You require:

- > SafeNet Luna Network HSM firmware update package file (<filename>.**spkg**)

- > the secure package authentication code, provided in a text file accompanying the update package

### To update the HSM firmware to a version downloaded from the Support Portal

1. Transfer the secure package update file to the SafeNet Luna Network HSM using **scp** or **pscp** (see "[SCP and PSCP](#)" on page 1 in the *Utilities Guide*).

|                   |                                                                         |
|-------------------|-------------------------------------------------------------------------|
| <b>Linux/UNIX</b> | <b>scp</b> <filepath>/<packagename>.spkg admin@<appliance_host_or_IP>:  |
| <b>Windows</b>    | <b>pscp</b> <filepath>\<packagename>.spkg admin@<appliance_host_or_IP>: |

2. Stop all client applications to the SafeNet Luna Network HSM appliance.
3. Using a serial or SSH connection, log in to the appliance as **admin**.
4. At the LunaSH prompt, login as HSM SO.  
lunash:> **hsm login**
5. [Optional Step] Verify that the secure package file is present on the SafeNet Luna Network HSM.  
lunash:> **package listfile**
6. [Optional Step] Verify the package file, specifying the authorization code you received from Thales Group.  
lunash:> **package verify** <filename>.spkg **-authcode** <code\_string>
7. Install the firmware update package, specifying the authorization code you received from Thales Group.  
lunash:> **package update** <filename>.spkg **-authcode** <code\_string>

**NOTE** If you are using a service provider model, you can use the **-useevp** option to specify the OpenSSL EVP (Digital EnVELOPe library) API to validate the update package, rather than invoking the HSM. This allows you to install the update package without logging in as HSM SO. See "[package update](#)" on page 1 in the *LunaSH Command Reference Guide*.

The package update process takes a few seconds. The firmware package is now stored on the appliance, waiting to be applied to the HSM.

8. [Optional Step] Check that the desired firmware version is ready to apply.

lunash:> **hsm firmware show**

**CAUTION!** If you are using STC on the HSM Admin channel, disable it by running lunash:> **hsm stc disable** before you update the HSM firmware.

9. Update the firmware to the version currently stored on the appliance.

lunash:> **hsm firmware upgrade**

## Updating the SafeNet Luna Backup HSM Firmware

To update the firmware on a SafeNet Luna Backup HSM, use LunaCM on a client computer that is connected to the SafeNet Luna Backup HSM. You require:

- > SafeNet Luna Backup HSM 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.

### To update the SafeNet Luna Backup HSM firmware

1. Copy the firmware file (<filename>.**fuf**) and the authentication code file (<filename>.**txt**) to the SafeNet 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 ("role login" on page 1).
 

```
lunacm:> role login -name so
```
5. Apply the new firmware update by specifying the update file and the file containing the authorization code. If the files are not located in the SafeNet Luna Network HSM Client directory, specify the filepaths.
 

```
lunacm:> hsm updatefw -fuf <filename>.fuf -authcode <filename>.txt
```

## Rolling Back the SafeNet Luna HSM Firmware

When updating the HSM firmware, the SafeNet Luna Network HSM saves the previously-installed firmware version on the HSM. If required, you can roll back to this previously-installed version. Rollback allows you to try firmware without permanently committing to the new version.

Rollback does not create a new rollback target; a single rollback target is preserved when a firmware update is performed. After a rollback operation, no further rollback is possible until the next firmware update saves the pre-update version as the new rollback target.



**CAUTION!** *Update any factory-fresh Network HSM to newer firmware before rolling back.* The firmware rollback feature is intended to return the firmware to the previously installed version. Attempting a firmware rollback on a new appliance received directly from the Thales Group factory can result in RMA (return of product), as the pre-shipment firmware is a factory-test version that does not accept your credentials.

Firmware rollback is destructive; earlier firmware versions might have older mechanisms and security vulnerabilities that a new version does not. Back up any important materials before rolling back the firmware. This procedure zeroizes the HSM and all cryptographic objects are erased.

**NOTE** Firmware rollback is not supported on HSMs that use Functionality Modules. If you have ever enabled **HSM policy 50: Allow Functionality Modules**, even if the policy is currently disabled, you cannot roll back the HSM firmware. See "[FM Deployment Constraints](#)" on page 177 for details.

### To roll back the SafeNet Luna HSM firmware to the previous version

1. Check the previous firmware version that is available on the HSM.  
lunash:> [hsm firmware show](#)
2. Back up any important cryptographic objects currently stored on the HSM (see "[Backup and Restore Using a G5-Based Backup HSM](#)" on page 53).
3. At the LunaSH prompt, login as HSM SO.  
lunash:> [hsm login](#)
4. Roll back the HSM firmware.  
lunash:> [hsm firmware rollback](#)
5. Re-initialize the HSM and restore your partition(s) from backup.

## Upgrading HSM Capabilities and Partition Licenses

The SafeNet Luna Network HSM offers most customers all the capabilities they need. If your needs change, however, Thales Group offers upgrades on some SafeNet Luna Network HSM models. You can select these upgrades when you purchase your HSM, or you can order an upgrade license anytime after purchase and apply it yourself, using the Thales Group Licensing Portal (GLP).

This section provides guidelines and instructions for managing your licenses:

- > "[Purchasing an Upgrade License](#)" on page 403
- > "[Activating a License on the Thales Group Licensing Portal](#)" on page 405
- > "[Managing Your Thales Group Licensing Portal Account](#)" on page 409
- > "[Applying an Upgrade License on the HSM](#)" on page 413
- > "[Upgrade Troubleshooting](#)" on page 415

## Upgrade Options

Thales Group offers multiple options for upgrading your SafeNet Luna Network HSM.

### Factory Upgrades

You can select your desired upgrades at the time you purchase your HSM. Thales Group installs the upgrades at the factory, so that the license is activated when you receive your order. You receive an email from Thales Group's order entry system with the details of your upgrade license. You do not need to take any action; the upgraded HSM is ready for service.

If you plan to use the upgraded HSM as received, you do not need to create a GLP account. If you do create an account, you can use it to transfer upgrade licenses from one SafeNet Luna Network HSM to another as desired.

### Field Upgrades

If you have one of the approved SafeNet Luna Network HSM models, you can order upgrades at any time. After placing an upgrade order, you receive an email from Thales Group's order entry system with instructions on how to obtain your license through the GLP. Attached to the email is an entitlement certificate with an entitlement identifier. You need this number when you create your GLP account.

### Upgradable HSM Models

SafeNet Luna Network HSM comes in three models for your convenience. If you have a SafeNet Luna Network HSM model 750 or 790, you can purchase upgrade licenses and apply them yourself. At this time, the 700 model does not accept upgrades.

### Upgrade Types

Thales Group currently offers three types of HSM upgrade:

- > partition upgrade packs (of 5) to increase the maximum number of application partitions
- > Korea-specific cryptographic algorithms
- > Functionality Modules (allowed on FM-ready HSMs only)

### License Revocation

You may purchase and apply upgrades to any upgradable SafeNet Luna Network HSM appliance you own. If you have already applied an upgrade to an HSM and wish to remove it and apply it to a different HSM, you can revoke the license from one HSM so that it may be activated on the other. Contact Thales Group to revoke an upgrade license from an HSM.

### Return Material Authorization

In the unlikely event that you must return an HSM to Thales Group, the unit that you receive in exchange or receive back will have your purchased upgrades installed, and appearing on the GLP as activated. Thales Group's customer care team will revoke upgrades in GLP on your behalf so that the appliance sent to you has the correct upgrades. If you receive a replacement appliance, you will need to refer to the new serial number when managing your licenses.

## Purchasing an Upgrade License

To place an order for an upgrade, contact your Thales Group sales representative. If you are purchasing a new SafeNet Luna Network HSM, you can opt for factory-installed upgrades or field upgrades that you can install yourself. Thales Group offers the following types of upgrade licenses:

- > partition upgrade packs (of 5) to increase the maximum number of application partitions
- > Korea-specific cryptographic algorithms
- > Functionality Modules (allowed on FM-ready HSMs only)

For example, a SafeNet Luna Network HSM S790 appliance comes with the base maximum number of 10 partitions. To upgrade the maximum to allow 30 partitions, you must order four (4) partition upgrades. After you apply this full entitlement to your HSM, you have the desired maximum 30 partitions. The following table summarizes the upgrade options for different models.

| HSM Model | Factory-Installed Partitions | Maximum Number of Partitions | Maximum Number of 5-Pack Upgrades |
|-----------|------------------------------|------------------------------|-----------------------------------|
| *700      | 5                            | 5                            | N/A                               |
| *750      | 5                            | 20                           | 3                                 |
| *790      | 10                           | 100                          | 18                                |

After you place your order for an upgrade and a Thales Group Customer Care representative has entered the order, you receive an email with detailed instructions on how to obtain and apply your upgrade.

### Entitlement Certificate

Attached to the upgrade email is an entitlement certificate. On this certificate is an entitlement identifier that you need to activate your upgrade. Here is an example of an entitlement certificate and where to find the EID.

### SafeNet Luna Network HSM License Purchase

Thank you for your recent SafeNet Luna Network HSM order. Below please find your Entitlement ID as described in the user guide. Please keep this ID for your records.

We thank you for your business.

| Entitlement ID: c102f5dc-8179-4bec-9373-ffb3e633abe5 |                                              |                                     |          |
|------------------------------------------------------|----------------------------------------------|-------------------------------------|----------|
| <b>Sold To Customer:</b>                             | Customer Name                                |                                     |          |
| <b>End Customer:</b>                                 |                                              |                                     |          |
| <b>Customer Purchase Order:</b>                      | Demo                                         | <b>Gemalto/SafeNet Sales Order:</b> | 11074136 |
| <b>Item Number:</b>                                  | 908-000395-001                               | <b>Quantity:</b>                    | 4        |
| <b>Description:</b>                                  | PARTITION 5-PACK,LUNA HSM 7+ (FIELD UPGRADE) |                                     |          |
| <b>Order Book Date:</b>                              | 05/31/2017                                   |                                     |          |

Next, see ["Activating a License on the Thales Group Licensing Portal"](#) on the next page.

## Activating a License on the Thales Group Licensing Portal

After receiving the entitlement confirmation email, visit the Thales Group Licensing Portal (GLP) and create an account to activate your upgrade license. You need the Entitlement ID from the confirmation email to complete this procedure.

### To activate a license

1. Navigate to the GLP welcome page in your browser, enter the Entitlement ID from the email you received, and click **Activate**.

<https://safenetbelcamp.prod.sentinelcloud.com/ecp/>

Welcome to the Gemalto Licensing Portal (1.46.18.0731) English

**gemalto**

Enter Entitlement ID

Activate

OR

Email Address

Password

[Forgot your password?](#)

Sign in

**gemalto**

© 2006-2018 Gemalto [Privacy Policy](#) [Terms & Conditions](#) [Contact Gemalto](#) [gemalto.com](#)

2. If you do not already have an account, complete the mandatory user registration process by entering your email address and selecting a password and security questions, and click **Next**.

If you already have an account and are activating a new entitlement, click **Login** and enter your email address and password.

gemalto<sup>®</sup> Licensing Portal Asterisk (\*) indicates a required field English Aug 14, 2018 2:36:22 PM

Please take some time to register with us. **Already registered? Login**

Enter Your Account Information

Email Address\* Password\*

Confirm Email Address\* Confirm Password\*

Set Your Security Preferences

Security Question 1\* Security Question 2\*

Security Question 1 Answer\* Security Question 2 Answer\*

Enter Your Personal Information

Name\* Company Name United States

Cancel Next

© 2006-2018 Gemalto Privacy Policy Terms & Conditions Contact Gemalto gemalto.com

**NOTE** The GLP is arranged as a company account. Accounts with email addresses associated with a company are able to see all of that company's purchases. The association between a license and your company is created by registration and login using the Entitlement ID.

Multiple email addresses can be associated with your company. There is no limit.

If a registered GLP user leaves the company, contact Thales Group Customer Support to make the adjustment.

3. On the **License Activation** screen, enter the number of licenses from the entitlement that you wish to activate, and click **Next**.

License Activation Aug 14, 2018 12:28:59 PM

Step 1 - Select License    Step 2 - Select HSM    Step 3 - Finish

Company: Luna Team    Order #: Luna ECP screenshot    Order Date: 08/02/2018  
 Entitlement ID: 88065104-fbd1-458d-b9e8-XXXXXX

| Number | Product Name                                                                              | Activated | Available | Quantity To Activate |                                     |
|--------|-------------------------------------------------------------------------------------------|-----------|-----------|----------------------|-------------------------------------|
| 1      | PARTITION 5-PACK, LUNA HSM7+ (FIELD UPGRADE) 3.0<br>Part# 908-000395-001 Expiration: None | 1         | 14        | 3                    | <input checked="" type="checkbox"/> |

Cancel    Next

© 2006- 2018 Gemalto    Privacy Policy    Terms & Conditions    Contact Gemalto    gemalto.com

4. Specify the HSM that will use this license by clicking **Enter New HSM SN** and entering the serial number. If you previously entered the HSM's serial number, click **Use Existing HSM SN** and select it from the drop-down menu. Click **Next**.

License Activation Aug 14, 2018 12:33:55 PM

Step 1 - Select License    Step 2 - Select HSM    Step 3 - Finish

Company: Luna Team    Order #: Luna ECP screenshot    Order Date: 08/02/2018  
 Entitlement ID: 88065104-fbd1-458d-b9e8-XXXXXX

| Product                                                                                              | Apply to                                                                                                      |
|------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------|
| PARTITION 5-PACK, LUNA HSM7+ (FIELD UPGRADE) 3.0<br>Part# 908-000395-001    Quantity To Activate : 3 | <input checked="" type="radio"/> Enter New HSM SN <input type="radio"/> Use Existing HSM SN<br>HSM SN: 532989 |

Enter comments

Cancel    Previous    Next

© 2006- 2018 Gemalto    Privacy Policy    Terms & Conditions    Contact Gemalto    gemalto.com

5. Your activation is now complete. GLP generates a license string that the SafeNet Luna Network HSM will use to validate an upgrade and apply it. Click **Download License File** to download a ZIP file containing this string. If you do not wish to install the upgrade at this time, click **Done**.

The screenshot shows the Gemalto License Activation interface. At the top, there is a navigation bar with the Gemalto logo, a language dropdown set to 'English', and a user profile section with 'Home / Welcome' and a user icon. Below this, the page title is 'License Activation' and the date/time is 'Aug 14, 2018 12:34:17 PM'. A progress bar shows three steps: 'Step 1 - Select License', 'Step 2 - Select HSM', and 'Step 3 - Finish'. Below the progress bar, there is a summary box with the following information: Company: Luna Team, Order #: Luna ECP screenshot, Order Date: 08/02/2018, and Entitlement ID: 88065104-fbd1-458d-b9e8. A large green banner reads 'Activation Complete'. Below this, a table shows the product name and activation status:

| Product Name                                                                              | Activated |
|-------------------------------------------------------------------------------------------|-----------|
| PARTITION 5-PACK, LUNA HSM7+ (FIELD UPGRADE) 3.0<br>Part# 908-000395-001 Expiration: None | 3         |

At the bottom of the table, there are two buttons: 'Download License File' (highlighted with a red arrow) and 'Done'.

© 2008-2018 Gemalto Privacy Policy Terms & Conditions Contact Gemalto gemalto.com

6. Extract the license string file (default filename: **lserverc**) from the ZIP file. Thales Group recommends that you rename this file to something more distinctive, especially if you have multiple upgrades to manage. If you are managing upgrades for multiple HSMs, it is a good idea to include the HSM serial number, as in the example below.



A screenshot of a Notepad window titled '532989\_15\_partitions - Notepad'. The window contains the following license string:

```
16 LUNA_PARTITIONS_5PACK 1.0 LONG NORMAL STANDALONE ADD 3_KEYS INFINITE_KEYS 14 AUG 2018 16
37 NEVER NiL SLM_CODE CL_ND_LCK NiL *1RAJFAJ86KCKCPL0400 NiL NiL NiL INFINITE_MINS NiL 0
:GE9X00:sVQWvrSsHei0favqw55tUmUqmzrSZWWG10fzZ5WFY:A0IMaUI,28gfKGLuR3473OMxLhFHmdgmqqAr3WRTe
Ln4EH8JC0zKd7viMT3vhzNpQtgDJ0VbK3046,Acf1#
```

Next, see ["Applying an Upgrade License on the HSM"](#) on page 413.

For more information about navigating the GLP, see ["Managing Your Thales Group Licensing Portal Account"](#) on the next page.



## Managing Your Thales Group Licensing Portal Account

Once you have created your account, you can return to it at any time to manage and get information about your purchased licenses. The **My Assets** page is the home for this information. From this page, you can find the following information:

- > "View Licenses by Product" below
- > "Activate New Entitlements" below
- > "Products" on the next page
- > "Orders" on page 411
- > "Activations" on page 411
- > "Devices" on page 412

### View Licenses by Product

To sort license information by product, choose the Thales Group product from the drop-down menu at the top left:

The screenshot shows the Gemalto licensing portal interface. At the top left, the Gemalto logo is displayed. To its right, there is a language dropdown menu set to "English" and a user profile section with a home icon, the text "Home / Welcome", and a user profile picture. A dropdown menu for "All Products" is open, showing a list of product categories: All Products, CCC, SAM, SAC, IDGo 800, Luna, and SMC. The "Luna" option is highlighted. In the top right corner, the date and time "Aug 14, 2018 5:27:51 PM" are displayed. Below the dropdown menu, an instruction reads: "Instruction: The following list displays all products that are available to your company. To view the list of orders for a given product, click the View button for that product. To activate a given order, click the associated Activate button from the list of orders." Below the instruction, there is a "Products" tab and an "Export CSV" button. A table with the following data is shown:

| Product Name                                                             | Activated | Available | View                 |
|--------------------------------------------------------------------------|-----------|-----------|----------------------|
| PARTITION 5-PACK, LUNA HSM7+ (FIELD UPGRADE) 3.0<br>Part# 908-000395-001 | 7         | 8         | <a href="#">View</a> |

Below the table, there is a link to "Orders (1)". At the bottom of the page, there is a footer with the copyright notice "© 2006-2018 Gemalto" on the left, and links for "Privacy Policy", "Terms & Conditions", "Contact Gemalto", and "gemalto.com" on the right.

### Activate New Entitlements

After you select the product type from the drop-down menu, you can activate any new licenses by entering the Entitlement ID in the upper right corner.

The screenshot shows the Gemalto Licensing Portal interface. At the top, there is a navigation bar with the Gemalto logo, a language dropdown set to 'English', and a home button. Below this is a search bar with 'Luna' selected. A red box highlights the 'Entitlement ID' search field, which contains the text 'Enter' and a 'GO' button. A red arrow points from the search bar area towards the highlighted field. Below the search bar, the page title is 'Licensing Portal' and the date is 'Aug 14, 2018 5:35:10 PM'. The main content area is titled 'My Assets' and includes a section for 'Products (1)'. An instruction states: 'The following list displays all products that are available to your company. To view the list of orders for a given product, click the View button for that product. To activate a given order, click the associated Activate button from the list of orders.' Below this is a table with columns for 'Product Name', 'Activated', 'Available', and 'View'. The table contains one row for 'PARTITION 5-PACK, LUNA HSM7+ (FIELD UPGRADE) 3.0' with 7 activated and 8 available licenses. A 'View' button is next to the product name. Below the table are sections for 'Orders (1)' and 'Activations (3)'. The footer contains copyright information and links for Privacy Policy, Terms & Conditions, and Contact Gemalto.

## Products

To see the licenses you have purchased, expand the **Products** view. This page is a summary of upgrades, and shows the quantity available and how many are activated. Click **View** next to a product to see details.

This screenshot is identical to the one above, showing the Gemalto Licensing Portal. The 'View' button for the product 'PARTITION 5-PACK, LUNA HSM7+ (FIELD UPGRADE) 3.0' is highlighted with a red box. The rest of the interface, including the search bar, navigation, and table, is the same as in the previous screenshot.

## Orders

The **Orders** view provides details of each order you purchased. Click **Activate** next to an order to activate available licenses.

Licensing Portal Aug 14, 2018 5:43:15 PM

My Assets ⓘ

Products (1)

Orders (1)

**Instruction :** The following list displays all orders for your company. Click **Activate** for an order to initiate an activation.

**Orders** Export CSV

| Order Date | Order Number        | PO Number           | Product Name                                                                             | Entitlement ID                     | Activated | Available | Activate        |
|------------|---------------------|---------------------|------------------------------------------------------------------------------------------|------------------------------------|-----------|-----------|-----------------|
| 8/2/2018   | Luna ECP screenshot | Luna ECP screenshot | PARTITION 5-PACK, LUNA HSM7+ (FIELD UPGRADE) 3.0<br>Part# 908-000395-001 Expiration:None | 88065104-fbd1-458d-b9e8-██████████ | 7         | 8         | <b>Activate</b> |

Activations (3)

© 2006-2018 Gemalto Privacy Policy Terms & Conditions Contact Gemalto gemalto.com

## Activations

The **Activations** view lists the entitlements you have previously activated. Click **Download** next to an activation to download the corresponding license string in a ZIP file.

gemalto English Home / Welcome [User]

Activations (3)

Instruction :The following list displays all activations for your company.

| Activations     |                                     |                                     |                   |                    |                                                                                             |              | Export CSV |
|-----------------|-------------------------------------|-------------------------------------|-------------------|--------------------|---------------------------------------------------------------------------------------------|--------------|------------|
| Activation Date | Activation ID                       | Entitlement ID                      | HSM Serial Number | Locking Code       | Product Activated                                                                           | License File | Activated  |
| 8/3/2018        | a464cca0-714f-4492-a626- [Redacted] | 88065104-fbd1-458d-b9e8- [Redacted] | 180802            | *1DGG7C [Redacted] | PARTITION 5-PACK, LUNA HSM7+ (FIELD UPGRADE) 3.0<br>Part#908-000395-001<br>Expiration: None | Download     | 1          |
| 8/14/2018       | 9fb2eae0-4d35-4ca3-a260- [Redacted] | 88065104-fbd1-458d-b9e8- [Redacted] | 532989            | *19CF9Z [Redacted] | PARTITION 5-PACK, LUNA HSM7+ (FIELD UPGRADE) 3.0<br>Part#908-000395-001<br>Expiration: None | Download     | 3          |
| 8/14/2018       | 1e8342a5-e5d4-41a6-b6c7- [Redacted] | 88065104-fbd1-458d-b9e8- [Redacted] | 532018            | *1RAJFA [Redacted] | PARTITION 5-PACK, LUNA HSM7+ (FIELD UPGRADE) 3.0<br>Part#908-000395-001<br>Expiration: None | Download     | 3          |

Devices (3)

© 2006- 2018 Gemalto Privacy Policy Terms & Conditions Contact Gemalto gemalto.com

## Devices

The **Devices** view shows all the HSMs you have registered on the portal. Click **View** next to a specific device to see more details (what features were activated and when, and the corresponding license string in a ZIP file).

gemalto English Home / Welcome [User]

Products (1)

Orders (1)

Activations (3)

Devices (3)

Instruction : The following list displays all devices that have an associated activation for your company.

| Devices           |                    |                                                                                     |           |      | Export CSV |
|-------------------|--------------------|-------------------------------------------------------------------------------------|-----------|------|------------|
| HSM Serial Number | Locking Code       | Product Activated                                                                   | Activated | View |            |
| [Redacted]        | *1DGG7C [Redacted] | PARTITION 5-PACK, LUNA HSM7+ (FIELD UPGRADE)<br>Part#908-000395-001 Expiration:None | 1         | View |            |
| [Redacted]        | *1RAJFA [Redacted] | PARTITION 5-PACK, LUNA HSM7+ (FIELD UPGRADE)<br>Part#908-000395-001 Expiration:None | 3         | View |            |
| 532989            | *19CF9Z [Redacted] | PARTITION 5-PACK, LUNA HSM7+ (FIELD UPGRADE)<br>Part#908-000395-001 Expiration:None | 3         | View |            |

© 2006- 2018 Gemalto Privacy Policy Terms & Conditions Contact Gemalto gemalto.com

## Applying an Upgrade License on the HSM

The license string file you downloaded from the GLP (see ["Activating a License on the Thales Group Licensing Portal" on page 405](#)) is used to apply your HSM upgrade. The HSM Security Officer must complete this procedure.

### Prerequisites

- > Ensure that you have the license string file that is registered to the correct HSM serial number.
- > If you are installing partition upgrades, ensure that you have space available on the HSM. By default, partitions are created at a size that will utilize the entire HSM space based on the number of partition licenses at the time. If your existing partitions use all available space on the HSM, the new license application may fail with an error (LUNA\_RET\_RM\_CONFIG\_CHANGE\_FAILS\_DEPENDENCIES). To prevent this, reclaim space on the HSM by resizing the existing partitions (see ["Customizing Partition Sizes" on page 18](#)) before you apply the upgrade license.

### To apply an upgrade license on the HSM

1. Open a command prompt, navigate to the directory containing the license string file, and use **scp/pscp** to transfer it to an **admin**-level account on the SafeNet Luna Network HSM appliance (see [SCP and PSCP](#)).

- Windows: **pscp** [options] <license\_file> **admin@**<host/IP>:
- Linux/UNIX: **scp** [options] <license\_file> **admin@**<host/IP>:

2. Connect to the appliance via SSH or a serial connection, and log in to LunaSH using the **admin**-level account that received the file (see ["Logging In to LunaSH" on page 421](#)).
3. Log in as HSM SO (see ["Logging In as HSM Security Officer" on page 431](#)).

```
lunash:> hsm login
```

4. [Optional] Confirm that the HSM fingerprint matches the one in the license string. If this string does not match, the upgrade will not be applied.

```
lunash:> sysconf fingerprint license
```

```
Fingerprint for Use With Entitlement Management System
```

```

```

```
HSM serial #532018 : *1RAJFAJ86KCKCPL
```

```
License string:
```

```
16 LUNA_PARTITIONS_5PACK 1.0 LONG NORMAL STANDALONE ADD 3_KEYS INFINITE_KEYS 14 AUG 2018 16 37
NEVER NiL SLM_CODE CL_ND_LCK NiL *1RAJFAJ86KCKCPL0400 NiL NiL NiL INFINITE_MINS NiL 0
:GE9X00:sVQWvrSsHei0favqw55tUmUqmzrSZWWG10fzZ5WFY:A0IMaUI,28gfKGLuR3473OMxLhFHmdgmgqAr3WRTEln4E
H8JC0zKd7viMT3vhzNpQtgDJ0VbK3046,Acf1#
```

5. Apply the upgrade to the HSM.

```
lunash:> sysconf license apply -filename <license_file>
```

6. [Optional] Verify that the license has been applied.

```
lunash:> sysconf license list
```

**NOTE** The **QUANTITY** column represents the total number of additional partitions associated with a specific license. This column does not apply to other types of license upgrades.

## Upgrade Troubleshooting

If you are unable to apply an upgrade license from the Thales Group Licensing Portal (GLP), the table below provides descriptions of possible failure messages (lunash:> [sysconf license apply](#)).

| Message                                                       | Description                                                                                                                                                                |
|---------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Cannot find <filename>                                        | The file that you specified containing the license string cannot be found on the HSM appliance. Use lunash:> <a href="#">my file list</a> to see what files are available. |
| Cannot find lserverc                                          | You should not encounter this message. If you do, please contact Thales Group Technical Support for assistance.                                                            |
| Invalid licensed feature                                      | The license string is corrupted in the feature attribute. Confirm that you saved the license string without modification after activating the upgrade in the GLP.          |
| Invalid licensed feature version                              | The license string is corrupted in the feature version attribute. Confirm that you saved the license string without modification after activating the upgrade in the GLP.  |
| Invalid licensed HSM serial number                            | The license string is for an HSM with a different serial number. Ensure that you transferred the correct license string file to the appliance.                             |
| <feature> not licensed for this appliance                     | The license string is for an HSM with a different serial number. Ensure that you transferred the correct license string file to the appliance.                             |
| License is already applied                                    | The license string matches an entitlement already applied on this HSM appliance.                                                                                           |
| LUNA_RET_HSM_TAMPERED                                         | The HSM is in a tampered state and must be cleared of the tampered state before the upgrade can be applied.                                                                |
| Update Result : 12 (Error detecting HSM)                      | The HSM Security Officer is not logged in.                                                                                                                                 |
| License is unknown/not available (feature)                    | The HSM appliance software needs to be updated to support a newer feature.                                                                                                 |
| Upgrades not available for this model of HSM                  | Only 750 and 790 models of HSM support upgrades.                                                                                                                           |
| Upgrade to <#> partitions not available for this model of HSM | Applying the upgrade would exceed the upper limit for the maximum number of partitions on the HSM.                                                                         |
| Unable to determine model of HSM                              | You should not encounter this message. If you do, please contact Thales Group Technical Support for assistance.                                                            |

# CHAPTER 24: Users and 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.

Access to SafeNet Luna Network HSM is controlled through an enhanced version of the PKCS#11 hierarchy of roles, assigned to different users in your organization. Each role allows its user to execute a different set of commands to perform specialized tasks at one of the following levels:

- > ["Appliance Users and Roles" on page 418](#)
- > ["HSM Roles" on page 430](#)
- > ["Partition Roles" on page 433](#)

## Appliance-Level Users and Roles

SafeNet Luna Network HSM consists of an HSM inside a secure appliance with a hardened operating system (accessed via the LunaSH command-line interface). Administration of the appliance (including network setup, file management, and system logging) is considered separate from administration of the HSM and its cryptographic functions. This separation of duties is essential to a secure environment and it allows you to easily delegate responsibilities to personnel.

Although appliance-level roles are not security roles as defined in the PKCS#11 standard, they do provide an additional level of security by requiring that the user be logged in to the appliance before they can log in to the HSM.

When one of the default appliance roles is logged in to LunaSH on the appliance, only the commands available to that role are visible. A user with **admin**-level access can create custom user roles to limit access to specified commands and operations. See ["Appliance Users and Roles" on page 418](#) for details.

**Table 1: Default Appliance Roles**

| Role         | Function                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|--------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>admin</b> | <ul style="list-style-type: none"><li>&gt; Can perform all administrative and configuration tasks on the appliance</li><li>&gt; With the HSM Security Officer credential, can perform all HSM administrative tasks</li><li>&gt; Activates other optional appliance roles and sets/resets their passwords</li><li>&gt; Creates custom users and roles with access to a specified subset of commands</li><li>&gt; Creates NTLS connections between the SafeNet Luna Network HSM appliance and SafeNet Luna HSM Clients</li></ul> |



| Role            | Function                                                                                                                                                                                                                                                                                                                                 |
|-----------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>operator</b> | <ul style="list-style-type: none"> <li>&gt; Can perform administrative tasks on the appliance, except for some configuration tasks</li> <li>&gt; With the HSM Security Officer credential, can perform some basic HSM administration tasks</li> <li>&gt; Cannot execute any commands that affect other roles on the appliance</li> </ul> |
| <b>monitor</b>  | <ul style="list-style-type: none"> <li>&gt; Executes commands that present information about the appliance and HSM</li> <li>&gt; Cannot affect the state or contents of the appliance or HSM</li> </ul>                                                                                                                                  |
| <b>audit</b>    | <ul style="list-style-type: none"> <li>&gt; Initializes the Auditor role on the HSM</li> <li>&gt; With the Auditor credential, manages HSM audit logging</li> </ul>                                                                                                                                                                      |

## HSM-Level Roles

HSM roles are responsible for administration, configuration, and auditing of the HSM within the SafeNet Luna Network HSM appliance. After logging in to LunaSH with the appropriate appliance-level role, you can access commands available to the HSM roles. HSM-level roles cannot perform cryptographic operations on the application partition. See ["HSM Roles" on page 430](#) for details.

**Table 2: HSM Roles**

|                                                          |                                                                                                                                                                                                                                                                                                                                                                                   |
|----------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>HSM Security Officer (SO)</b><br><b>PED Key: Blue</b> | <ul style="list-style-type: none"> <li>&gt; Initializes the HSM, creating the SO credential</li> <li>&gt; Creates/deletes the application partition</li> <li>&gt; Configures global HSM policies</li> <li>&gt; Performs updates of the HSM firmware and appliance software</li> <li>&gt; Must have <b>admin</b>-level access to the appliance to perform all HSM tasks</li> </ul> |
| <b>Auditor (AU)</b><br><b>PED Key: White</b>             | <ul style="list-style-type: none"> <li>&gt; Manages HSM audit logging</li> <li>&gt; Must have <b>audit</b>-level access to the appliance to perform auditing tasks</li> </ul>                                                                                                                                                                                                     |

## Partition-Level Roles

Partition-level roles are responsible for administration and configuration of the application partition, and using the partition to perform cryptographic functions. Partition roles log in using LunaCM, or supply their credentials via crypto applications. An application partition acts as its own virtual HSM, and has its own set of roles. See ["Partition Roles" on page 433](#) for details.

**Table 3: Partition Roles**

|                                                                |                                                                                                                                                                                                                                                                                                        |
|----------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Partition Security Officer (PO)</b><br><b>PED Key: Blue</b> | <ul style="list-style-type: none"> <li>&gt; Initializes the partition, creating the PO credential and setting the cloning domain</li> <li>&gt; Initializes the Crypto Officer role and can reset the CO credential (if permitted by HSM policy)</li> <li>&gt; Configures partition policies</li> </ul> |
|----------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

|                                                     |                                                                                                                                                                                                                                                                                                                                                                                             |
|-----------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Crypto Officer (CO)</b><br><b>PED Key: Black</b> | <ul style="list-style-type: none"> <li>&gt; Creates and modifies cryptographic objects on the partition</li> <li>&gt; Manages backup and restore operations for the partition</li> <li>&gt; Performs cryptographic functions via user applications</li> <li>&gt; Creates and configures HA groups</li> <li>&gt; Initializes the Crypto User role and can reset the CU credential</li> </ul> |
| <b>Crypto User (CU)</b><br><b>PED Key: Gray</b>     | <ul style="list-style-type: none"> <li>&gt; Performs cryptographic functions via user applications (optional read-only role)</li> <li>&gt; Can create public objects only</li> <li>&gt; Can perform backup/restore of public objects on the partition</li> </ul>                                                                                                                            |

## Appliance Users and Roles

Configuration and maintenance tasks on the SafeNet Luna Network HSM appliance (including network setup, file management, and system monitoring) are completed by executing commands in the LunaSH command line interface.

When you log in to LunaSH via SSH or a serial connection, the set of available commands depends on the role assigned to your user account. Appliance roles are defined by their associated command privileges. Clear separation of duties is beneficial to a secure production environment and allows you to easily delegate responsibilities according to your organization's needs. For optimal security, assign each user the lowest-level role necessary to fulfill their responsibilities.

### Managing Appliance Users and Roles

Refer to the following procedures to manage appliance roles:

- > ["Logging In to LunaSH" on page 421](#)
- > ["Enabling/Disabling Appliance User Accounts" on page 422](#)
- > ["Changing Appliance User Passwords" on page 423](#)
- > ["Creating Custom Appliance User Accounts" on page 423](#)
- > ["Creating Custom Appliance Roles" on page 424](#)
- > ["Creating a One-Step NTLS Registration Role" on page 425](#)
- > ["Backing Up/Restoring the Appliance User Role Configuration" on page 427](#)
- > ["Recovering the Admin Account Password" on page 428](#)

### Default Appliance Users and Roles

The default SafeNet Luna Network HSM appliance user accounts are named after their respective default roles. You cannot delete the default user accounts. For a comprehensive list of the LunaSH commands available to the default roles, see ["LunaSH Command Summary" on page 1](#).

By default, only the **admin** and **recover** user accounts are active. The default password for all accounts is "PASSWORD" (see ["Logging In to LunaSH" on page 421](#)).

## admin

The **admin** user is the highest-level default user account. This user (or a custom user assigned an **admin** role) has access to the full set of LunaSH commands (except some specialized **audit** commands) and can perform all configuration and maintenance tasks on the SafeNet Luna Network HSM appliance. Users with an **admin** role can also activate or deactivate the other default user accounts, reset their passwords to default, and create custom user accounts and roles.

The **admin** role is required to access LunaSH commands for configuring and maintaining the HSM within the appliance, so the HSM Security Officer must be assigned an **admin** role to fulfill all HSM SO responsibilities (see ["HSM Security Officer \(SO\)" on page 430](#)).

## operator

The **operator** user is a limited-access default user account that can perform most configuration and maintenance tasks on the SafeNet Luna Network HSM appliance. For example, the **operator** cannot perform the following procedures:

- > activating or deactivating other roles on the appliance or resetting passwords
- > backup/restore of the LunaSH user configuration
- > regenerating the NTLS certificate on the appliance
- > setting TLS ciphers

This user (or a custom user assigned an **operator** role) cannot access HSM configuration commands. While it is possible for a user with an **operator** role to log in to the HSM using the HSM SO credential, many of the commands required by the HSM SO are inaccessible. It is therefore not recommended to assign an **operator** role to the HSM SO.

The **operator** user account must be activated by an **admin** user before it can log in to LunaSH (see ["Enabling/Disabling Appliance User Accounts" on page 422](#)).

## monitor

The **monitor** user is an information-only default user account that can observe the appliance and HSM status. This user (or a custom user assigned a **monitor** role) has access to only those LunaSH commands that present information about the SafeNet Luna Network HSM, including current HSM policies, created partitions, registered clients, and appliance settings. The **monitor** role cannot affect the appliance or HSM in any way.

The **monitor** user account must be activated by an **admin** user before it can log in to LunaSH (see ["Enabling/Disabling Appliance User Accounts" on page 422](#)).

## audit

The **audit** user is the account used by the HSM Auditor to log in to the appliance and access the HSM audit logging functions. This user (or a custom user assigned an **audit** role) has access to a unique subset of commands that configure audit logging, as well as some informational commands, and commands to manage the **audit** user's account and files. The Auditor credential is required for some commands, and therefore the Auditor must be assigned an **audit** role on the appliance to fulfill all Auditor responsibilities (see ["Auditor \(AU\)" on page 430](#)).

The **audit** user account must be activated by an **admin** user before it can log in to LunaSH (see ["Enabling/Disabling Appliance User Accounts" on page 422](#)).

## recover

The **recover** user account's only function is to reset the password for the **admin** user. This account cannot access any LunaSH commands, and there is no **recover** role that can be assigned to a custom user. The **recover** account cannot be locked out, and its default password does not expire.

As a security measure, **recover** can log in via the local serial connection only. The **admin** user's account password can be changed remotely by anyone who already knows it, but the **admin** user's password cannot be arbitrarily reset unless the person doing so has physical access to the appliance, to make the serial connection. See ["Recovering the Admin Account Password" on page 428](#).

## Custom Appliance Users and Roles

If the default set of users and roles do not conform to your organization's specific security profile, you can customize the user configuration on your SafeNet Luna Network HSM appliance to fit your needs. This system of users and roles gives you complete control over how your SafeNet Luna Network HSM is accessed.

### Custom User Accounts

LunaSH allows you to create custom, named user accounts. These users are assigned one of the default appliance roles, or a custom role that you create. For example, the following user configuration options are available:

- > Multiple **admin**-level users, each with a different name
- > Multiple **operator**-level users (or none), each with a different name
- > Multiple **monitor**-level users (or none), each with a different name
- > Multiple **audit**-level users (or none), each with a different name
- > Multiple custom users, each with a different name, with custom roles defined by the users' responsibilities

Named user accounts can be useful in distinguishing the actions of different people in the logs. For example, a user named **john** executing the command **syslog tail** in LunaSH would appear in the April 13 log as:

```
Apr 13 14:17:15 172 -lunash: Command: syslog tail : john : 192.20.10.133/3107
```

If you have personnel performing similar functions at physically separate locations, or assigned to teams or shifts for 24-hour coverage, it could be useful (or required by your security auditors) be able to show which specific person performed which actions on the system.

See ["Creating Custom Appliance User Accounts" on page 423](#).

### Custom Roles

You can also create custom roles with access to a specified subset of LunaSH commands. This allows you to delegate specific tasks to personnel according to your organization's security structure. Like the default roles, a custom role is defined by the commands it can access in LunaSH. When a custom role is assigned to any existing user, that user can see and use only those commands associated with the role. This ensures that a given user does not obtain access beyond their security clearance. The **admin** user can create custom roles, assign them to users, or revoke them as required.

See ["Creating Custom Appliance Roles" on page 424](#).

## Security of LunaSH User Accounts

In most cases anticipated by the design and target markets for SafeNet Luna Network HSM, both the SafeNet Luna Network HSM appliance and any computers that make network connections for administrative purposes would reside inside your organization's secure premises, behind well-maintained firewalls. Site-to-site connections would be undertaken via VPN. Therefore, attacks on the shell account(s) would normally not be an issue.

However, if your application requires placing the SafeNet Luna Network HSM appliance in an exposed position (e.g., in a cloud implementation), your shell account(s) may be vulnerable to attackers. It is your responsibility to protect your sensitive data.

Some recommendations for enhancing your security include using strong passwords, changing the SSH port number from its default, or using certificate-based authentication.

## Logging In to LunaSH

When you open a connection to the SafeNet Luna Network HSM appliance (serial or SSH) you are presented with the **login as:** prompt. By default, only the **admin** user is enabled; the other roles must be enabled by an **admin** user before they can log in (see ["Enabling/Disabling Appliance User Accounts" on the next page](#)). After entering the user name and password, you are presented with the **lunash:>** prompt.

### To log in to LunaSH on the SafeNet Luna Network HSM appliance

1. At the **login as:** prompt, enter the name of the account you want to use (**admin**, **operator**, **monitor**, **audit**, or a custom user account) and press **ENTER**.

You are prompted for the password.

2. Enter the account password and press **ENTER**. If you are logging in to this account for the first time, the initial password is "PASSWORD" (uppercase).

**NOTE** You must log in within two minutes of opening an administration session, or the connection will time out. The username and passwords are case-sensitive.

3. For security, you are immediately prompted to change the factory-default password.

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

**NOTE** If you forget the password to any account, an **admin**-level user can set a new password for you (see ["Changing Appliance User Passwords" on page 423](#)).

If you forget the **admin** password, and no other **admin**-level accounts are available, you can use a local serial connection to log in to the **recover** account (see ["Recovering the Admin Account Password" on page 428](#)).

After successful login, the HSM appliance presents a **lunash:>** prompt. Type **?** or **help** and press **Enter** for a summary of the main commands. Type **?** followed by any of the commands, with or without parameters, and press **Enter** to see a summary of sub-commands and parameters for that command.

## Failed Appliance Login Attempts

The response to failed login attempts is the same for **admin**, **operator**, **monitor**, **audit**, and any named users you have created, and is limited by default SSH settings:

- > If you initiate an SSH session against the appliance, and fail to respond to the prompts, the session expires after 120 seconds. You must restart or launch a new session in your SSH terminal tool.
- > If you initiate an SSH session against the appliance, provide a user name, and then provide an incorrect password, the session prompts you to re-attempt the correct password for that user account. If you fail to provide the correct authentication six (6) times, the session is dropped. You must restart or launch a new session in your SSH terminal tool.

The maximum number of simultaneous sessions per channel is the SSH default of 10. These factors help to limit the pace of brute-force attacks, while still allowing timely recovery from mistyping or forgetfulness by an administrative user.

You can configure SafeNet Luna Network HSM to accept administrative connections (SSH) on only one Ethernet LAN port, and client (NTLS) connections on another.

### Why does my new Network HSM appliance report failed logins?

Upon first login to the Network appliance, you might see a system message like the following:

```
Last failed login: Wed Jan 02 14:25:11 EDT 2019 from 192.168.10.105 on ssh:notty
There were 2 failed login attempts since the last successful login.
Last login: Wed Jan 02 14:15:09 from 192.168.10.105
```

This is expected. The manufacturing process uses a temporary password, then resets the default password and verifies that the temporary password is no longer valid. This accounts for the "failed login attempts".

## Enabling/Disabling Appliance User Accounts

By default, **admin** is the only active user account on the SafeNet Luna Network HSM appliance. The other default accounts (**operator**, **monitor**, **audit**) exist and cannot be deleted. The **admin** account (or a custom user account with an **admin** role) must first enable them using the procedure below.

### To enable a default appliance user account

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 the previous page).
2. Enable the desired account.

```
lunash:> user enable -username <account_name>
```

The user of this account can now log in to LunaSH with the account name and default password "PASSWORD". See "[Logging In to LunaSH](#)" on the previous page.

## To disable any appliance user account

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 421](#)).

2. Disable the desired account.

```
lunash:> user disable -username <username>
```

## Changing Appliance User Passwords

From time to time, you will need to change the password for a LunaSH account. This could be due to a password being compromised, or your company's security policy mandates password changes after a specific time interval. Individual users can change the password for their own account at any time. The **admin** or users with **admin** privileges may change the password for other accounts, including other **admin**-level accounts.

### Password Guidelines

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

For more information, see ["Name, Label, and Password Requirements" on page 438](#).

## To change your own appliance user password

1. Connect to the appliance via SSH or a serial connection, and log in to LunaSH using your username and password (see ["Logging In to LunaSH" on page 421](#)).

2. Change your user password.

```
lunash:> my password set
```

## To change the password for a different user

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 421](#)).

2. Change the password for a specified user.

```
lunash:> user password <username>
```

**NOTE** **admin**-level users can also use this command to change their own password.

## Creating Custom Appliance User Accounts

LunaSH allows you to create custom, named user accounts on the SafeNet Luna Network HSM appliance. These users are assigned one of the standard appliance roles, or a custom role that you create (see ["Creating Custom Appliance Roles" on the next page](#)). Use this procedure to create custom user accounts.

## User Naming Guidelines

### To create a custom user account

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 421](#)).
2. Create the custom user account by specifying a name.

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.

```
lunash:> user add -username <username>
```

```
lunash:>user add -username james
```

```
Stopping sshd: [OK]
```

```
Starting sshd: [OK]
```

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

3. Assign a role to the new user account.

```
lunash:> user role add -username <username> -role <rolename>
```

```
lunash:>user role add -username james -role admin
```

```
User james was successfully modified.
```

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

The user of this account can now log in to LunaSH with the account name and default password "PASSWORD". See ["Logging In to LunaSH" on page 421](#).

## Creating Custom Appliance Roles

LunaSH allows you to create custom roles that can be assigned to custom users, to specify exactly which commands that user is able to access. This allows you to delegate specific tasks to personnel according to your organization's security needs. An **admin**-level user can use the following procedure to create custom roles.

See ["LunaSH Command Summary" on page 1](#) in the *LunaSH Command Reference Guide* for a complete list of available commands.

The following commands (refer to the *LunaSH Command Reference Guide*) allow you to import, add, or remove a custom user role to your SafeNet Luna Network HSM appliance:

- > ["user role import" on page 1](#)
- > ["user role add" on page 1](#)
- > ["user role delete" on page 1](#)



## To create a custom appliance role and assign it to a user

1. Create a text file on your local workstation that lists each command that you want the role to be able to access (the role definition file).

For example, if you wanted the user **Alex** to be able to perform backup operations on your HSM but not restore operations, you would create a role definition file including backup commands and not including restore commands.

**NOTE** All lines must end with a UNIX-style linefeed (lf) character. If you create your file in Windows, be sure to convert it to use UNIX line endings before transferring it to an HSM appliance.

2. Transfer the role definition file to the appliance using **pscp** (Windows) or **scp** (Linux/UNIX). You require the SafeNet Luna Network HSM appliance **admin** password (or an account with an **admin** role) to complete this step. The file is automatically placed in the appropriate directory on the appliance; do not specify a target directory (see "[SCP and PSCP](#)" on page 1).
3. Log into LunaSH as **admin** (or the user you specified when transferring the file).
4. Import the role definition file and specify a name for the new role.

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.

```
lunash:> user role import -file <filename> -role <rolename>
```

```
lunash:>user role import -file backuprole -role backup
```

```
"backuprole" was successfully imported.
```

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

5. Create the user account that you want to assign the role to, if it does not already exist.

```
lunash:> user add -username <username>
```

6. Assign the role to the desired user.

```
lunash:> user role add -username <username> -role <rolename>
```

## Creating a One-Step NTLS Registration Role

Creating NTLS links between a client and partition using the one-step method (see "[One-Step NTLS Connection Procedure](#)" on page 130) usually requires administrative access to the SafeNet Luna Network HSM appliance. You can set up a custom role that allows a third party to use only the commands necessary for one-step NTLS.

## To create a one-step NTLS registration role

1. Create a role definition .txt file on your local workstation, listing the following commands:

```
scp
partition list
client list
client register
client assignPartition
```

**NOTE** All lines must end with a UNIX-style linefeed (lf) character. If you create your file in Windows, be sure to convert it to use UNIX line endings before transferring it to an HSM appliance.

These are the commands necessary for creating one-step NTLS links. You can include any other commands for your registration purposes. See [client](#) for the complete set of commands.

- Transfer the role definition file (**registerclient.txt** in the example below) to the appliance using **pscp** (Windows) or **scp** (Linux/UNIX).

|                   |                                                                                                                                                                                                                                |
|-------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Windows</b>    | <pre>pscp registerclient.txt admin@&lt;server_host/IP&gt;: pscp registerclient.txt admin@192.168.0.123: admin@192.168.0.123's password: ***** registerclient.txt                  1 kB   1.1 kB/s   ETA: 00:00:00   100%</pre> |
| <b>Linux/UNIX</b> | <pre>scp registerclient.txt admin@&lt;server_host/IP&gt;: scp registerclient.txt admin@192.168.0.123: admin@192.168.0.123's password: ***** registerclient.txt                  1 kB   1.1 kB/s   ETA: 00:00:00   100%</pre>   |

- Log in to the appliance by SSH as the **admin** user.
- Import the role definition file to create the **registerclient** role.
 

```
lunash:> user role import -file registerclient.txt -role registerclient
```
- Create the **register** user account.
 

```
lunash:> user add -username register
```
- Assign the role to the **register** user.
 

```
lunash:> user role add -username register -role registerclient
```
- Open a new SSH connection to the appliance and log in as **register** with the default password "PASSWORD".

```
login as: register
register@192.168.0.123's password:
```

You will be prompted to set a new password for the **register** user. This will be the password you provide to the third-party client. Ensure it is both secure and distinct from the **admin** user password.

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

- Provide the **register** password and the partition name to the client operator. The client can now establish a one-step NTLS connection by specifying the **register** user and password in LunaCM.

```
lunacm:> clientconfig deploy -server <server_host/IP> -client <client_host/IP> -partition <name> -user register
```

## Backing Up/Restoring the Appliance User Role Configuration

LunaSH allows you to store a snapshot of the administrative user database (the names and status of all named LunaSH users) that can later be restored if desired.

**CAUTION!** Restoring from backup restores the database of user profiles that existed at the time the backup was made. You will lose any user accounts created since the backup; passwords of existing users could be reverted without their knowledge; enabled users might be disabled; disabled users might be enabled; and any user accounts removed since that backup will be restored.

Your records should indicate when user-profile changes were made, and what those changes were. Any time you restore a backup, reconcile the changed statuses and inform anyone who is affected. For example, users need to know to use their previous password, and to change it immediately.

**NOTE** While the built-in **admin**, **operator**, and **monitor** accounts are not deleted or added by a restore operation (those accounts are permanent), both their enabled/disabled status and their passwords are changed to whatever prevailed at the time the backup was originally taken.

### To back up the appliance user role configuration

- 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 421).
- Back up the user role configuration, specifying a description for the backup file.

```
lunash:> sysconf config backup -description <description>
lunash:>sysconf config backup -description "Configuration Backup 17-03-01"

Created configuration backup file: myLuna_Config_20170301_1200.tar.gz

Command Result : 0 (Success)
```

### To restore the appliance user role configuration

- 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 421).
- List the available configuration backup files.

```
lunash:> sysconf config list
```

Configuration backup files in file system:

| Size                | File Name                          | Description          |
|---------------------|------------------------------------|----------------------|
| 34099<br>2018-05-07 | myLuna_Config_20180507_1629.tar.gz | Configuration Backup |

Command Result : 0 (Success)

- Restore the user role configuration. If you only wish to restore the user configuration, excluding other services on the appliance, specify **-service users**.

lunash:> **sysconf config restore -file <filename> [-service users]**

```
lunash:>sysconf config restore -file myLuna_Config_20180507_1629.tar.gz -service users
```

```
WARNING !! This command restores the configuration from the backup file: myLuna_Config_20180507_1629.tar.gz.
```

```
It first creates a backup of the current configuration before restoring: myLuna_Config_20180507_1629.tar.gz.
```

```
If you are sure that you wish to proceed, then type 'proceed', otherwise type 'quit'.
```

```
> proceed
```

```
Proceeding...
```

```
Created configuration backup file: myLuna_Config_20180507_1634.tar.gz
```

```
Restore the users configuration: Succeeded.
```

```
You must either reboot the appliance or restart the service(s) for the changes to take effect. Please check the new configurations BEFORE rebooting or restarting the services.
```

```
You can restore the previous configurations if the new settings are not acceptable.
```

Command Result : 0 (Success)

- Reboot the SafeNet Luna Network HSM appliance.

lunash:> **sysconf appliance reboot**

## Recovering the Admin Account Password

The **recover** account is a limited-purpose account that has the permanent (fixed) password "PASSWORD". The **recover** account's only purpose is to reset the password of the **admin** user, if the **admin** password is lost/forgotten.

**NOTE** The password recovery procedure does not affect the contents of the HSM or its application partitions. If you suspect that the **admin** account has been compromised, you can perform a factory reset of the HSM and appliance after recovery (see ["Resetting to Factory Condition" on page 167](#)).

As a security measure, **recover** can log in via the local serial connection only. The **admin** user's account password can be changed remotely by anyone who already knows it, but the **admin** user's password cannot be arbitrarily reset unless the person doing so has physical access to the appliance, to make the serial connection.

**CAUTION!** The exception to this rule is where you have your appliances connected to a "terminal server" that aggregates serial links and makes them accessible via telnet or similar. This configuration is useful in a test lab, where access control is not critical, and it can be very convenient when setting up and tearing down appliances for various test and verification scenarios. However, connection of your SafeNet appliances to a remotely accessible terminal server could expose an additional avenue of attack, and therefore Thales Group recommends that you avoid allowing this potential security opening in a production environment.

The **recover** account cannot be locked out, and its default password does not expire.

### To reset the admin account password

1. Connect a serial terminal to the serial console connector on the SafeNet Luna Network HSM rear panel.
2. Log in to LunaSH as **recover**, using the fixed password "PASSWORD".

**NOTE** If the HSM is initialized, you are required to present the HSM Security Officer (SO) credential. Therefore, only the SO can perform this operation. If you have not initialized the HSM prior to resetting the **admin** password, then no credential is required.

You are prompted to set a new **admin** password (see "[Do Not Cancel Out](#)" below).

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

If you are confident that your SafeNet Luna Network HSM has not been compromised, you can resume using it as before (taking care to both remember and secure the **admin** password).

## Do Not Cancel Out

Use of the **recover** account sets the password of the **admin** account back to the factory value, and then forces a password change. Do not attempt to bypass the password change.

To prevent the **admin** account being accessible over the network with a known password during the recover procedure, SSH is disabled when the recover process begins. The SSH service is re-enabled only after the password is changed. Interrupting the process and avoiding the password change leaves SSH service off at boot time. If you cancel out partway through the process in order to retain the default password, instead of changing it when prompted, you might find that you no longer have SSH access.

If you encounter the problem, reconnect a local terminal and log into the **recover** account again, this time allowing it to complete the full process, ending with a proper, non-default password. If SSH service is still not available, contact Technical Support.

**CAUTION!** During recovery, the network service is stopped and other services are affected. The minimum-effort resumption would be to reboot the system, which causes all services to restart with current configuration. However, for safety, you should consider manually restarting services from the local (serial) console, until all passwords have been changed from their default values.

## HSM Roles

SafeNet Luna Network HSM divides roles on the HSM according to an enhanced version of the PKCS#11 standard. Configuration, administration, and auditing of the HSM itself is the responsibility of the roles described below. Cryptographic functions take place on the application partition, which has a different set of independent roles (see "[Partition Roles](#)" on page 433).

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

The HSM-level roles are as follows:

### HSM Security Officer (SO)

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

- > Initializing the HSM and setting the SO credential (see "[HSM Initialization](#)" on page 224)
- > Setting and changing global HSM policies (see "[HSM Capabilities and Policies](#)" on page 95)
- > Creating/deleting the application partition (see "[Creating or Deleting an Application Partition](#)" on page 17)
- > Updating the HSM firmware (see "[Updating the SafeNet Luna HSM Firmware](#)" on page 398)

The HSM SO must have **admin**-level user access to the SafeNet Luna Network HSM appliance (see "[Appliance Users and Roles](#)" on page 418).

### Managing the HSM Security Officer Role

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

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

### Auditor (AU)

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

- > Initializing the Auditor role
- > Setting up audit logging on the HSM

- > Configuring the maximum size of audit log files and the time interval for log rotation
- > Archiving the audit logs

The Auditor must have access to the **audit** account on the SafeNet Luna Network HSM appliance (see ["Appliance Users and Roles" on page 418](#)).

### Managing the Auditor Role

Refer to ["Configuring and Using Audit Logging" on page 38](#) for procedures involving the Auditor role. See also:

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

## Logging In as HSM Security Officer

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

### To log in as HSM SO

1. Connect to the appliance via SSH or a serial connection, and log in to LunaSH as **admin** or a custom user with an **admin** role (see ["Logging In to LunaSH" on page 421](#)).
2. Log in to the HSM.

```
lunash:> hsm login
```

You are prompted for the HSM SO credential.

## Failed HSM SO Login Attempts

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

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

## Changing the HSM SO Credential

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

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

## To change the HSM SO credential

1. Connect to the appliance via SSH or a serial connection, and log in to LunaSH as **admin** or a custom user with an **admin** role (see ["Logging In to LunaSH" on page 421](#)).
2. Log in as HSM SO (see ["Logging In as HSM Security Officer" on the previous page](#)).
3. Change the HSM SO credential.

```
lunash:> hsm changepw
```

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

In LunaSH, the HSM SO 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 using the **-password** option, enclose the password in double quotation marks.

## Logging In as Auditor

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

## To log in as Auditor

1. Connect to the appliance via SSH or a serial connection, and log in to LunaSH as **audit** or a custom user with an **audit** role (see ["Logging In to LunaSH" on page 421](#)).
2. Log in to the HSM.

```
lunash:> audit login
```

You are prompted for the Auditor credential.

## Failed Auditor Login Attempts

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

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

## Changing the Auditor Credential

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



## To change the Auditor credential

1. Connect to the appliance via SSH or a serial connection, and log in to LunaSH as **audit** or a custom user with an **audit** role (see ["Logging In to LunaSH" on page 421](#)).
2. Log in as Auditor (see ["Logging In as Auditor" on the previous page](#)).
3. Change the Auditor credential.

```
lunash:> audit changepwd
```

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

## Partition Roles

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" on page 17](#)). 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 SafeNet Luna HSM Client installed. They do not require SSH access to LunaSH on the SafeNet 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 21](#))
- > Configuring partition policies (see ["Partition Capabilities and Policies" on page 106](#))
- > Initializing the Crypto Officer role (see ["Initializing the Crypto Officer Role" on the next page](#))
- > Activating the partition (see ["Activation and Auto-activation on Multi-factor- \(PED-\) Authenticated Partitions" on page 23](#))

### Managing the Partition SO Role

Refer also to the following procedures to manage the PO role:

- > ["Logging In to the Application Partition" on page 435](#)
- > ["Changing a Partition Role Credential" on page 437](#)

### 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 (see ["Backup and Restore Using a G5-Based Backup HSM" on page 53](#))
- > Create and configure HA groups (see ["Setting Up an HA Group" on page 203](#))
- > Initializing the Crypto User role (see ["Initializing the Crypto User Role" on the next page](#))

### Managing the Crypto Officer Role

Refer also to the following procedures to manage the CO role:

- > ["Logging In to the Application Partition" on the next page](#)
- > ["Changing a Partition Role Credential" on page 437](#)

### 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 (see ["Backup and Restore Using a G5-Based Backup HSM" on page 53](#))

### Managing the Crypto User Role

Refer also to the following procedures to manage the CU role:

- > ["Logging In to the Application Partition" on the next page](#)
- > ["Changing a Partition Role Credential" on page 437](#)

### Initializing the Crypto Officer and Crypto User Roles

The following procedures will allow you to initialize the Crypto Officer (CO) and Crypto User (CU) roles and set an initial credential.

#### 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

1. In LunaCM, log in to the partition as Partition SO (see ["Logging In to the Application Partition" on the next page](#)).  
lunacm:> **role login -name po**
2. 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 276](#) for details on creating PED keys.

In LunaCM, passwords and challenge secrets must be 7-255 characters in length. The following characters are allowed:

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

Double quotation marks (") are problematic and should not be used in passwords.

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

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

3. 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 page 437](#).

### 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 ["Logging In to the Application Partition" below](#)).  
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 276](#) for details on creating PED keys.

In LunaCM, passwords and challenge secrets must be 7-255 characters in length. The following characters are allowed:

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

Double quotation marks (") are problematic and should not be used in passwords.

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

lunacm:> **role 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" on page 437](#).

### Logging In to the Application Partition

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 SafeNet Luna Network HSM client workstation.
2. Set the active slot to the desired partition.  
lunacm:> **slot set -slot** <slotnum>
3. Log in by specifying your role on the partition.  
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 106). 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 "[Resetting the Crypto Officer or Crypto User Credential](#)" on the next page).
- > 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 106](#)). The CO must unlock the CU role and reset the credential (see ["Resetting the Crypto Officer or Crypto User 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 ["Logging In to the Application Partition" on page 435](#)).

```
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 276](#) for details on creating PED keys.

In LunaCM, passwords and challenge secrets must be 7-255 characters in length. The following characters are allowed:

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

Double quotation marks (") are problematic and should not be used in passwords.

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

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

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

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

## Resetting the Crypto Officer or Crypto User Credential

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 106](#)).

**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 or Crypto User credential

1. Log in with the appropriate role (see ["Logging In to the Application Partition" on page 435](#)).
2. Reset the desired role's credential.

In LunaCM, passwords and challenge secrets must be 7-255 characters in length. The following characters are allowed:

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

Double quotation marks (") are problematic and should not be used in passwords.

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

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

You are prompted to set a new credential for the role.

3. Provide the new credential to the 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 the previous page](#).

## Name, Label, and Password Requirements

This page describes length and character requirements for setting names, labels, domains, passwords, and challenge secrets on the SafeNet 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" on the next page](#)
- > ["Appliance User Passwords" on the next page](#)
- > ["HSM Labels" on the next page](#)
- > ["Cloning Domains" on the next page](#)
- > ["Partition Names" on the next page](#)
- > ["Partition Labels" on page 440](#)
- > ["HSM/Partition Role Passwords or Challenge Secrets" on page 440](#)

### 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 HSM SO 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 using the **-password** option, enclose the password in double quotation marks.

In LunaCM, passwords and challenge secrets must be 7-255 characters in length. The following characters are allowed:

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

Double quotation marks (") are problematic and should not be used in passwords.

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