THALES

Thales Luna PCIe HSM 7

LUNACM COMMAND REFERENCE

Document Information

Last Updated	2026-09-04 09:50:03 GMT-05:00

Trademarks, Copyrights, and Third-Party Software
Copyright 2001-2026 Thales Group. All rights reserved. Thales and the Thales logo are trademarks and service marks of Thales and/or its subsidiaries and are registered in certain countries. All other trademarks and service marks, whether registered or not in specific countries, are the property of their respective owners.

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

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

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

> The copyright notice, the confidentiality and proprietary legend and this full warning notice appear in all copies.

> This document shall not be posted on any publicly accessible network computer or broadcast in any media, and no modification of any part of this document shall be made.

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

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

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

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

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

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

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

Regulatory Compliance

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

USA, FCC

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

Canada

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

Europe

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

CONTENTS

Preface: About the LunaCM Command Reference 8
Customer Release Notes 8
Audience 8
Document Conventions 8
Support Contacts 11

Chapter 1: Using LunaCM 12
Accessing LunaCM 12
Scripted Use 13
LunaCM Features 14
Case Insensitivity 15
Quotation Marks 15
Operation 15

Chapter 2: LunaCM Commands 16
appid 18
appid close 19
appid info 20
appid open 21
appid set 22
audit 23
audit config 25
audit export 32
audit import 34
audit logmsg 35
audit status 36
audit time 37
audit time get 38
audit time sync 39
audit verify 40
clientconfig 41
clientconfig deleteserver 42
clientconfig deploy 43
clientconfig listservers 45
clientconfig restart 46
clientconfig verify 47
file display 48
hagroup 49
hagroup addmember 51
hagroup addstandby 53

hagroup creategroup 54
hagroup deletegroup 57
hagroup halog 58
hagroup haonly 60
hagroup interval 61
hagroup listgroups 62
hagroup recover 63
hagroup recoverymode 64
hagroup removemember 65
hagroup removestandby 66
hagroup retry 67
hagroup synchronize 68
hsm 70
hsm changehsmpolicy 72
hsm envshow 73
hsm factoryreset 74
hsm init 76
hsm migratepedkey 80
hsm monitor 81
hsm resetUtilization 82
hsm restart 84
hsm rollbackfw 85
hsm showinfo 86
hsm showmechanism 89
hsm showpolicies 91
hsm showUtilization 93
hsm smkclone 95
hsm smkrollover 97
hsm tamperclear 99
hsm tampershow 100
hsm time 100
hsm time get 100
hsm time sync 101
hsm updatecap 103
hsm updatefw 104
hsm zeroize 105
partition 106
partition addsize 109
partition archive 111
partition archive backup 113
partition archive contents 118
partition archive delete 120
partition archive list 121
partition archive restore 123
partition changelabel 126
partition changepolicy 128
partition changepw 132

partition cipherdisable ... 134
partition cipherenable ... 137
partition ciphershow ... 142
partition clear ... 145
partition clone ... 146
partition contents ... 148
partition create ... 149
partition delete ... 152
partition domainadd ... 154
Example - add a password-authenticated domain to a PED-authenticated HSM partition ... 157
Example - add a PED-authentication domain to a password-authenticated HSM partition ... 158
partition domainchangelabel ... 159
partition domaindelete ... 163
partition domainlist ... 165
partition init ... 167
partition login ... 171
partition logout ... 172
partition logoutother ... 172
Syntax ... 172
Example ... 172
partition resize ... 173
partition restoresim3file ... 175
partition setlegacydomain ... 176
partition showinfo ... 177
partition showmechanism ... 181
partition showpolicies ... 183
partition smkclone ... 191
partition smkrollover ... 194
ped ... 196
ped connect ... 197
ped disconnect ... 198
ped get ... 199
ped set ... 200
ped show ... 201
ped vector ... 202
remotebackup start ... 203
role ... 204
role changepw ... 205
role createchallenge ... 208
role deactivate ... 210
role init ... 211
role list ... 213
role login ... 214
role logout ... 216
role recoveryinit ... 217
role recoverylogin ... 218
role resetpw ... 219

role setdomain 221
role show 222
slot 223
slot configset 225
slot configshow 227
slot list 228
slot partitionlist 230
slot set 231
slot showempty 232
srk 233
srk disable 234
srk enable 235
srk generate 236
srk recover 237
srk show 238
srk transport 239
stm 240
stm recover 241
stm show 243
stm transport 244

PREFACE: About the LunaCM Command Reference

This document describes how to access and use the LunaCM command line tool, with detailed syntax descriptions and examples for each available command. It contains the following chapters:

> "Using LunaCM" on page 12

> "LunaCM Commands" on page 16

The preface includes the following information about this document:

> "Customer Release Notes" below

> "Audience" below

> "Document Conventions" below

> "Support Contacts" on page 11

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

Customer Release Notes

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

Audience

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

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

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

Document Conventions

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

Notes

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

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

Cautions

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

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

Warnings

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

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

Command syntax and typeface conventions

Format	Convention
bold	The bold attribute is used to indicate the following: > 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**.)
italics	In type, the italic attribute is used for emphasis or to indicate a related document. (See the *Installation Guide* 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.

 Copyright 2001-2026 Thales Group

Format	Convention
{**a**|**b**|**c**} {<a>|<b>|<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>|<b>|<c>]	Represent optional alternate keywords or variables in a command line description. Choose one command line argument enclosed within the braces, if desired. Choices are separated by vertical (OR) bars.

Support Contacts

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

Customer Support Portal

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

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

Telephone

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

CHAPTER 1: Using LunaCM

> **NOTE** This is a general-purpose tool intended for use across Luna HSM versions. It might reference mechanisms and features that are not available on all Luna products.

This chapter describes how to access and use the LunaCM utility. It contains the following topics:

> "Accessing LunaCM" below
> "LunaCM Features" on page 14

Accessing LunaCM

The LunaCM utility (LunaCM) is the client-side administrative command interface for Luna PCIe HSM 7s.

From a client/host computer, LunaCM can interact with, and perform operations on any, or all, of the following:

> Internally installed Luna PCIe HSM 7s (HSM card)
> Locally USB-connected Luna USB HSM 7s
> Remotely located Luna Network HSM 7 application partitions, made available by an NTLS or STC network link between the distant HSM appliance and partition(s) and the local client computer.

To access LunaCM

1. Open a Command Prompt or console window.
2. Go to the Luna HSM Client software directory and start the LunaCM utility:

Windows	C:\> **cd c:\Program Files\SafeNet\LunaClient** C:\Program Files\SafeNet\LunaClient\> **lunacm**
Linux/AIX	> **cd /usr/safenet/lunaclient/bin** > **./lunacm**
Solaris	> **cd /opt/safenet/lunaclient/bin** > **./lunacm**

   Some preliminary status information is displayed, followed by the lunacm:> command-line prompt.

3. You can now issue any LunaCM utility command to manage your Luna PCIe HSM 7s. For a summary, type "help" and press **Enter**.

> **NOTE** For Luna PCIe HSM 7 andLuna USB HSM 7, LunaCM is used to administer both the HSM as HSM SO, and the application partition. For Luna Network HSM 7, LunaCM is used to manage application partitions (assuming an NTLS or STC link between your Luna HSM Client computer and the Luna Network HSM 7 appliance). LunaCM is not used to perform HSM-wide administration by the HSM SO on Luna Network HSM 7 - for that you must log into a LunaSH session via SSH.

LunaCM depends on the availability of HSM partitions in order to be useful. If no application partition has been created, then only the HSM SO (administrative) partition is available, against which to run commands.

> **CAUTION!** If the **Chrystoki.conf** / **Crystoki.ini** configuration file [Presentation] setting "ShowAdminTokens=" is set to **no**, then the HSM administrative partition/slot for any attached HSMs are not available. If you also have not created any application partitions, LunaCM is not usable. If you know you have a working Luna PCIe HSM 7 attached to your Client computer and LunaCM shows no usable commands, or you cannot see the Admin slots, then verify in your **Chrystoki.conf** or **Crystoki.ini** file that "ShowAdminTokens" is not set to **no**. See Configuration File Summary for more information.

Scripted Use

This document generally describes LunaCM being used via its own persistent interface or shell, where the tool is launched and remains open for administrative users to issue commands at their convenience. However, for headless operation and other administrative scenarios, it is possible to launch LunaCM from a Windows or UNIX/Linux command prompt to execute a single command and immediately close. Similarly, it is possible to invoke LunaCM by referring it to a file that contains a list of commands to execute. Some command-line launch-time flags are provided.

lunacm [**-c** <command>] [**-q** <command>] [**-s** <slot id> <command>] [**-e** <script filename>] [**-f** <script filename>]

Option	Description
Non-repeating, single-instance commands	
. <command>	If no option is specified, LunaCM launches its full, persistent shell interface.
-c <command>	This option displays the banner and runs a single instance of a LunaCM command, and then returns to the operating system command prompt.
-q <command>	This option runs a single instance of a LunaCM command, and then returns to the operating system command prompt. The banner is suppressed.
-s <slot number> <command>	This option runs a single instance of a LunaCM command against the specified slot, and then returns to the operating system command prompt. The banner is suppressed.
Scripting options	

Option	Description
-e <script filename>	Launch LunaCM with this option followed by the name of a file containing a list of LunaCM commands, with one command per line. This option halts when the first error is encountered. Use this option when debugging your scripts.
-f <script filename>	Launch LunaCM with this option followed by the name of a file containing a list of LunaCM commands, with one command per line. This option continues after any command that results in an error (as long as the command concludes by returning control).

NOTE When preparing a script file, any commands with a **-force** option should include that option to suppress prompts (like "Type 'proceed'...") that could halt the progression of scripted commands. If a command requires inputs (like passwords, domains, etc), those parameters must be provided as part of the command.

TIP Change in scripted operation from Luna HSM 6.x to Luna HSM 7.x

When scripting multi-step operations, a common way to provide responses to interactive commands (example, the lunacm **hagroup creategroup** command needs a response of "copy", or "remove", or "quit") is to use "echo" to pipe the response text into the command within your script.

This worked well for Luna 5.x/6.x, in the below example presenting "copy" to resolve the interim prompt.

```
"echo copy | lunacm -q hagroup creategroup -serialNumber <serialNumber> -label
<HAgroupName>  -password <partitionPass>"
```

To accomplish the same result with Luna 7.x.x, do the following:

1. Create a file, in this example, “copy.txt” that contains only the word “copy” as its content.
2. Run the “lunacm” commands as below to create the HA group, and to add a member to the HA group, while inputting the “copy” prompt:
   - In cmd (for .bat script):

     ```
     type copy.txt | lunacm -c hagroup creategroup -label HA -slot 0 -p ********
     type copy.txt | lunacm -c hagroup addmember -group HA -slot 1 -p ********
     ```
   - In Powershell (for powershell script) :

     ```
     Get-Content .\copy.txt | .\lunacm.exe -c hagroup creategroup -label HA -
     slot 0 -p ********
     Get-Content .\copy.txt | .\lunacm.exe -c hagroup addmember -group HA -slot
     1 -p ********
     ```

Use the same technique in similar situations.

LunaCM Features

> Command history is supported, using up/down arrows, **Home**, **End**, **Page Up**, **Page Down**.

> Non-ambiguous command shortnames are supported. You must type the exact shortname that is listed in the syntax help, or else type the full command with no abbreviations.
Additionally, for syntax help, the alias **?** is available.

- Commands and options are case-insensitive.
- Limited scripting is possible.

However, handling of return codes is not fully supported at this time. The utility is not a full-featured shell, so features like command-completion or parsing of partial commands are not supported.

Case Insensitivity

Commands and options entered by the user are not sensitive to case. If a user accidentally leaves the Caps-Lock key on, or by habit capitalizes some commands or options, they should not have to re-enter or edit the command line.

Command parameters, however, are passed to command executables with the same case as entered on the command line. Command executables must deal with case issues as appropriate for the command.

For example, you can type:

lunacm:> **partition login -password <your_unique_password_for_current_partition>**

or

lunacm:> **partition LOGIN -PASSWorD <your_unique_password_for_current_partition>**

and successfully login to your Partition. Note that the command and sub-commands can be any combination of uppercase and lowercase letters. The command parser interprets it correctly. However, the password string itself is passed on to the access-control handler, which is very particular about lettercase. Therefore, an item like a password must be typed letter-perfect with the appropriate case applied.

> **NOTE** For multi-factor authenticated HSM, do not type the password - you are directed to the Luna PED, which prompts for the required PED key.

Quotation Marks

It might happen that a command parameter consists of two or more parts, separated by spaces. This can be misconstrued by the command parser as two (or more) additional parameters. To ensure that a multi-part parameter is parsed as a single entity, enclose it in quotation marks " ".

Operation

LunaCM's cache can become unsynchronized if you access an HSM in more than one application session and make administrative changes.

For example, you might attempt a role login against a connected Luna Network HSM 7 application partition, in a lunacm instance that had been open for a while, and you (or someone else) had just made a partition policy change in lunash, such as changing max bad login attempts from default 10 down to (say) 3. The policy change comes into effect immediately, though any other open sessions might be unaware of the change. A failed attempt in the open lunacm instance might state that you still had nine unsuccessful attempts remaining, when in fact you had only two, because the lunacm instance was not up-to-date with the change made via lunash.

Relaunching lunacm, or using "clientconfig restart" updates the cache and fixes the mismatch.

CHAPTER 2: LunaCM Commands

This chapter describes the commands available in LunaCM. The commands are described in alphabetical order and provide:

- A brief description of the command function
- The command syntax and parameter descriptions
- Usage examples

LunaCM opens with a slot list, showing brief descriptions of the HSM administrative or application partitions that are visible to the library, in the order that they are detected. Those include:

- Luna Network HSM 7 application partitions (if any), network-connected to the host computer via NTLS
- Luna PCIe HSM 7s (if any) installed within the host computer
- Luna Backup HSMs (if any) connected via USB to the host computer

By default, LunaCM shows the lowest-numbered slot first. Local HSMs (Luna PCIe HSM 7 or Luna USB HSM 7) might have an HSM administrative slot (for the HSM SO) or an application partition slot, or both, so LunaCM leaves gaps in the slot numbering to allow for the possible slots on a given HSM.

> **NOTE** Login state of a slot is preserved until explicitly ended (such as with "logout" or "deactivate" or closing the application). Therefore, login state persists when you switch slots in LunaCM. If you were logged into the partition in slot 1, then set current slot to slot 2, then came back to slot 1, the login state for the partition in slot 1 would still be in force, with no need to reinstate it.

The following table provides links to the top-level commands in the hierarchy. Select a link to display the command syntax or to navigate to the sub-command you need. Some of these commands act on the active-slot partition; some have a **-slot** option to direct their action to another partition/slot.

Argument(s)	Shortcut	Description
appid	**a**	Manage Application Ids. See "appid" on page 18.
audit	**au**	Audit commands. These commands are available only on the HSM's administrative partition. See "audit" on page 23
clientconfig	**ccfg**	Client configuration. See "clientconfig" on page 41.
file	**f**	File commands. See "file display" on page 48.
hagroup	**ha**	High Availability Group commands. See "hagroup" on page 49.

Argument(s)	Shortcut	Description
hsm	**hs**	HSM commands. These commands are available only when the active slot is the HSM's administrative partition. See "hsm" on page 70.
partition	**par**	Partition commands. See "partition" on page 106.
ped	**p**	Remote PED commands. See "ped" on page 196.
remotebackup	**rb**	Manage Remote Backup server. See "remotebackup start" on page 203.
role	**ro**	Role management commands. See "role" on page 204.
slot	**s**	Slot management commands. See "slot" on page 223.
srk	**r**	Secure Recovery Commands. These commands are available only when the active slot is set to a Luna Backup HSM. See "srk" on page 233.
stm	**stm**	Secure Transport Mode commands. These commands are available only when the active slot is the HSM's administrative partition. See "stm" on page 240.

appid

Access the **appid**-level commands to manage application IDs on the HSM. For a description of application IDs, see Application IDs.

> **NOTE** This command is not applicable on DPoD Luna Cloud HSM services.

> **NOTE** From HSM firmware version 7.8.4 and newer, Application IDs (APPId) are *encrypted*, with the following effects:
>
> - Whenever firmware is upgraded from a non-APPID encrypted version (before firmware 7.8.4) to an encrypted APPID firmware version, the access ID shown in the audit logs will change.
> - The ID is encrypted for sending *to* the HSM, and when sent *back to* the crypto library, and is *unencrypted* and visible for the application (for example, LUNACM) but appears in *encrypted* form only, in audit logs.
> - The access ID shown also changes after every reset/restart of firmware version 7.8.4 and newer because a new APPID encryption key (AEK) is created each time firmware starts up. The AEK is used by the crypto library of the APP to encrypt the access ID.
> - Also whenever an Application is started it creates a new random access ID each time (unless fixed to a value [set AppId= under the Misc section] in the Configuration file).

Syntax

appid

close
info
open
set

Argument(s)	Shortcut	Description
close	**c**	Close a previously set access ID. See "appid close" on the next page
info	**i**	Display information for the access IDs. See "appid info" on page 20
open	**o**	Open a previously set access ID. See "appid open" on page 21
set	**s**	Set an access ID. See "appid set" on page 22

appid close

Close an application access ID on the HSM to prevent your applications from using it to access the HSM. Application IDs are assigned as a way of sharing login state among multiple processes. AppIDs require two 4-byte/32-bit unsigned integers, one designated "major" and the other designated "minor". For a full description of application IDs, see Application IDs.

> **NOTE** If you are concerned that an unauthorized process might be able to take over a login state, then you can use large, difficult-to-guess numbers for the major and minor appids. If this is not a concern, or for use in a development lab, you can use any arbitrary, conveniently small integers.
>
> This command is not applicable on DPoD Luna Cloud HSM services.

Syntax

appid close -major <value> **-minor** <value>

Argument(s)	Shortcut	Description
-major <value>	**-ma**	The major appid.
-minor <value>	**-mi**	The minor appid.

Example

```
lunacm:> appid close -major 1 -minor 40

Command Result : No Error
```

 Copyright 2001-2026 Thales Group

appid info

Display the currently set application IDs. This list includes all set application IDs, regardless of whether they are open or closed. For a full description of application IDs, see Application IDs.

> **NOTE** This command is not applicable on DPoD Luna Cloud HSM services.

Syntax

appid info

Example

```
lunacm:>appid info
        Using user defined Application ID:


        Application ID Major: 307
        Application ID Minor: 207

Command Result : No Error
```

appid open

Open an application access ID on the HSM to allow your applications to use it to access the HSM. Application IDs are assigned as a way of sharing login state among multiple processes. AppIDs require two 4-byte/32-bit unsigned integers, one designated "major" and the other designated "minor". For a full description of application IDs, see Application IDs.

> **NOTE** If you are concerned that an unauthorized process might be able to take over a login state, then you can use large, difficult-to-guess numbers for the major and minor appids. If this is not a concern, or for use in a development lab, you can use any arbitrary, conveniently small integers.
>
> This command is not applicable on DPoD Luna Cloud HSM services.

Syntax

appid open -major <value> **-minor** <value>

Argument(s)	Shortcut	Description
-major <value>	**-ma**	The major appid.
-minor <value>	**-mi**	The minor appid.

Example

```
lunacm:> appid open -major 1 -minor 40

Command Result : No Error
```

appid set

Set an application access ID on the HSM. Application IDs are assigned as a way of sharing login state among multiple processes. AppIDs require two 4-byte/32-bit unsigned integers, one designated "major" and the other designated "minor". After setting an appid, you must open it using **appid open** to allow your applications to use it to access the HSM. Once you set an appid you can open and close it, as required, to allow or deny application access to the HSM using the appid. For a full description of application IDs, see Application IDs.

> **NOTE** If you are concerned that an unauthorized process might be able to take over a login state, then you can use large, difficult-to-guess numbers for the major and minor appids. If this is not a concern, or for use in a development lab, you can use any arbitrary, conveniently small integers.
>
> This command is not applicable on DPoD Luna Cloud HSM services.

> **NOTE** From HSM firmware version 7.8.4 and newer, Application IDs (APPId) are *encrypted*, with the following effects:
>
> - Whenever firmware is upgraded from a non-APPID encrypted version (before firmware 7.8.4) to an encrypted APPID firmware version, the access ID shown in the audit logs will change.
> - The ID is encrypted for sending *to* the HSM, and when sent *back to* the crypto library, and is *unencrypted* and visible for the application (for example, LUNACM) but appears in *encrypted* form only, in audit logs.
> - The access ID shown also changes after every reset/restart of firmware version 7.8.4 and newer because a new APPID encryption key (AEK) is created each time firmware starts up. The AEK is used by the crypto library of the APP to encrypt the access ID.
> - Also whenever an Application is started it creates a new random access ID each time (unless fixed to a value [set AppId= under the Misc section] in the Configuration file).

Syntax

appid set -major <value> **-minor** <value>

Argument(s)	Shortcut	Description
-major <value>	**-ma**	The major appid.
-minor <value>	**-mi**	The minor appid.

Example

```
lunacm:> appid set -major 1 -minor 40

Command Result : No Error
```

audit

Access the audit-level commands. Audit commands control HSM audit logging, and can be used only by the properly authenticated HSM Audit role, once that role has been initialized.

> **NOTE** The **audit** commands appear only when LunaCM's active slot is set to the administrative partition.
>
> This command is not applicable on DPoD Luna Cloud HSM services.

The LunaCM **hsm** commands available to the **audit** user are restricted to **hsm show**, and all **hsm ped** commands, except **hsm ped vector** commands. The "audit" appliance user is allowed to connect and disconnect remote PED connections, adjust timeout, and view connection information, but is not allowed to create (init) or erase a remote PED vector.

> **NOTE** After initializing the Audit role on a password-authenticated HSM, log in as the Auditor and set the domain (see "role setdomain" on page 221). This step is required before setting logging parameters or the log filepath, or importing/exporting audit logs.

Syntax

audit

config
export
import
logmsg
status
time
verify

Argument(s)	Shortcut	Description
config	**c**	Configure the audit parameters. See "audit config" on page 25.
export	**e**	Read the wrapped log secret from the HSM. See "audit export" on page 32.
import	**m**	Import the wrapped log secret to the HSM. See "audit import" on page 34.
logmsg	**logm**	Write a message to the HSM's log. See "audit logmsg" on page 35.
status	**s**	Show the status of the logging subsystem. See "audit status" on page 36.

 Copyright 2001-2026 Thales Group

Argument(s)	Shortcut	Description
time	**t**	Synchronize the HSM time to the host, or get the HSM time. See "audit time" on page 37.
verify	**v**	Verify a block of log messages. See "audit verify" on page 40.

audit config

Set the audit logging configuration parameters. This command allows you to configure the following:

- Which events are captured in the log
- The log rotation interval

> **NOTE**
> - After initializing the Audit role on a password-authenticated HSM, log in as the Auditor and set the domain (see "role setdomain" on page 221). This step is required before setting logging parameters or the log filepath, or importing/exporting audit logs.
> - The **audit** commands appear only when LunaCM's active slot is set to the administrative partition.
> - This command is not applicable on DPoD Luna Cloud HSM services.
> - To configure the audit log path using "audit config" above **-path** on a Luna PCIe HSM 7 or Luna Backup HSM 7, the PED Client needs to be running. Otherwise, the command will return the CKR_CALLBACK_ERROR.

Syntax

audit config [**get**] [**path** <filepath>] [**evmask** <mask>] [**interval** <interval>] [**size** <integer><k | m>]

Argument(s)	Shortcut	Description
evmask <mask>	**e**	The value you want to configure for the specified parameter. **Valid values for the event parameter:** Enter a comma-separated list of events to log. In addition to specifying an event category, you must also specify the conditions under which those events are to be logged - either 'f' for failures, or 's' for successes, or both. Any or all of the following may be specified: > **[f]ailure**: log command failures > **[s]uccess**: log command successes > **[a]ccess**: log access attempts (logins) > **[m]anage**: log HSM management (init/reset/etc) > **[k]eymanage**: key management events (key create/delete) > **asymmetri[c]**: asymmetric key usage (enc/dec/sig/ver) > **fi[r]st**: first asymmetric key usage only (enc/dec/sig/ver) > **s[y]mmetric**: symmetric key usage (enc/dec/sig/ver) > **symf[i]rst**: first symmetric key usage only (enc/dec/sig/ver) > **e[x]ternal**: log messages from CA_LogExternal > **lo[g]manage**: log events relating to log configuration > **a[l]l**: log everything (user will be warned) > **[n]one**: turn logging off (can be set without a log path) **Note:** When specifying an event class to log, you must specify whether successful or failed events are to be logged. For example, to log all key management events you would use the command "audit config e k,s,f".
force	**f**	Force action without prompting for confirmation.
get	**g**	Get (show) the current configuration.
interval <interval>	**i**	**Valid values for the rotation interval parameter** Enter one of the following options for the log rotation interval: > **hourly [@min]** > **daily [@hour:min]** > **weekly [@day:hour:min]** > **monthly [@date:hour:min]** > **never** (can be set without a log path)

Argument(s)	Shortcut	Description
path <filepath>	**p**	Path on the host to which logs will be written. As usual, any filepath that contains a space should be enclosed in quotation marks, to prevent misreading. The system throws an error if the specified path does not exist. **CAUTION!** Linux only. If you delete the directory specified by the **path** parameter, your cryptographic operations will continue without a warning or error. Logging will continue until the HSM FRAM is full, at which point a CKR_LOG_FULL message is generated.
size <integer><**k** | **m**>	**s**	Size limit of a log, to trigger rotation. **Valid values for the size parameter**: An integer string signifying the size of the log in bytes. The optional modifiers **k** or **m** may be given after the string to specify KB or MB (for example, **s 8388608**, **s 8192k**, and **s 8m** all specify rotation when log size reaches 8MB). **Valid Range**: **4096k - 2097151k** **Default**: **2097151k**

Example

```
     audit config e s                audit all command successes
     audit config e f                audit all command failures
     audit config e u,f,s            audit all key usage requests,
                                     both success and failure
     audit config e n                log nothing


     audit config p /usr/lunapci/log  set path
     audit config i daily@12:05       rotate logs daily at 12:05
     audit config s 4096k             rotate logs when 4MB is exceeded



lunacm:> audit config evmask all,failure,success

        You have chosen to log all successful key usage events. This can result in
        an extremely high volume of log messages, which will significantly degrade
        the overall performance of the HSM.
        Are you sure you wish to continue?

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

Command Result : No Error

lunacm:> audit config get

Current Logging Configuration
-----------------------------
```

```
event mask        : Log everything
rotation interval : daily@0:00
rotation size (MB): 4
path to log       : /var/audit/


Command Result : No Error
```

> **NOTE** In the above example of output from **audit config get**, the configuration rotates the logs daily; "rotation size (KB)" indicates the maximum log size. With this configuration, multiple log files may be produced per day, none larger than 4MB.

Example removing key management actions from items to log

```
lunacm:>audit config get

Current Logging Configuration
-----------------------------
event mask : Log failure+success+access+manage+keymanage
rotation interval : infinite
rotation size : never (2097151 KB max file size)
path to log : /root/logging

Command Result : No Error

lunacm:>audit config e f,s,a,m

Command Result : No Error

lunacm:>audit config get

Current Logging Configuration
-----------------------------
event mask : Log failure+success+access+manage
rotation interval : infinite
rotation size : never (2097151 KB max file size)
path to log : /root/logging

Command Result : No Error
```

Now perform a partition clone in or out with any CPV4 cipher enabled (CPV=0, CPV3 disabled)

```
lunacm:>partition clone -o 0 -slot 27 -p userpinco

Logging in to target slot 27

Checking if objects already exist on target slot 27.

Cloning the objects.
Handle 294 on slot 26 is now handle 70 on slot 27
Handle 293 on slot 26 is now handle 75 on slot 27
Handle 290 on slot 26 is now handle 76 on slot 27
Handle 289 on slot 26 is now handle 79 on slot 27
Handle 286 on slot 26 is now handle 101 on slot 27
Handle 285 on slot 26 is now handle 104 on slot 27
Handle 282 on slot 26 is now handle 105 on slot 27
```

```
Handle 281 on slot 26 is now handle 313 on slot 27
Handle 278 on slot 26 is now handle 314 on slot 27
Handle 277 on slot 26 is now handle 317 on slot 27
Handle 274 on slot 26 is now handle 318 on slot 27
Handle 273 on slot 26 is now handle 321 on slot 27
Handle 270 on slot 26 is now handle 322 on slot 27
Handle 269 on slot 26 is now handle 325 on slot 27
Handle 266 on slot 26 is now handle 326 on slot 27
Handle 265 on slot 26 is now handle 329 on slot 27
Handle 262 on slot 26 is now handle 330 on slot 27
Handle 261 on slot 26 is now handle 333 on slot 27
Handle 258 on slot 26 is now handle 334 on slot 27
Handle 257 on slot 26 is now handle 337 on slot 27
Handle 254 on slot 26 is now handle 338 on slot 27
Handle 253 on slot 26 is now handle 341 on slot 27
Handle 250 on slot 26 is now handle 342 on slot 27
Handle 249 on slot 26 is now handle 345 on slot 27
Handle 246 on slot 26 is now handle 346 on slot 27
Handle 245 on slot 26 is now handle 349 on slot 27
Handle 242 on slot 26 is now handle 350 on slot 27
Handle 241 on slot 26 is now handle 353 on slot 27
Handle 238 on slot 26 is now handle 354 on slot 27
Handle 237 on slot 26 is now handle 357 on slot 27
Handle 234 on slot 26 is now handle 358 on slot 27
Handle 233 on slot 26 is now handle 361 on slot 27
Handle 230 on slot 26 is now handle 362 on slot 27
Handle 229 on slot 26 is now handle 365 on slot 27
Handle 226 on slot 26 is now handle 366 on slot 27
Handle 225 on slot 26 is now handle 369 on slot 27
Handle 222 on slot 26 is now handle 370 on slot 27
Handle 221 on slot 26 is now handle 373 on slot 27
Handle 218 on slot 26 is now handle 374 on slot 27
Handle 217 on slot 26 is now handle 377 on slot 27
Handle 214 on slot 26 is now handle 378 on slot 27
Handle 213 on slot 26 is now handle 381 on slot 27
Handle 210 on slot 26 is now handle 382 on slot 27
Handle 209 on slot 26 is now handle 385 on slot 27
Handle 206 on slot 26 is now handle 386 on slot 27
Handle 205 on slot 26 is now handle 389 on slot 27
Handle 202 on slot 26 is now handle 390 on slot 27
Handle 201 on slot 26 is now handle 393 on slot 27
Handle 198 on slot 26 is now handle 394 on slot 27
Handle 197 on slot 26 is now handle 397 on slot 27
Handle 194 on slot 26 is now handle 398 on slot 27
Handle 193 on slot 26 is now handle 401 on slot 27
Handle 190 on slot 26 is now handle 402 on slot 27
Handle 189 on slot 26 is now handle 405 on slot 27
Handle 186 on slot 26 is now handle 406 on slot 27
Handle 185 on slot 26 is now handle 409 on slot 27
Handle 182 on slot 26 is now handle 410 on slot 27
Handle 181 on slot 26 is now handle 413 on slot 27
Handle 178 on slot 26 is now handle 414 on slot 27
Handle 177 on slot 26 is now handle 417 on slot 27
Handle 174 on slot 26 is now handle 418 on slot 27
Handle 173 on slot 26 is now handle 421 on slot 27
Handle 170 on slot 26 is now handle 422 on slot 27
Handle 169 on slot 26 is now handle 425 on slot 27
Handle 166 on slot 26 is now handle 426 on slot 27
```

```
Handle 165 on slot 26 is now handle 429 on slot 27
Handle 162 on slot 26 is now handle 430 on slot 27
Handle 161 on slot 26 is now handle 433 on slot 27
Handle 158 on slot 26 is now handle 434 on slot 27
Handle 157 on slot 26 is now handle 437 on slot 27
Handle 154 on slot 26 is now handle 438 on slot 27
Handle 153 on slot 26 is now handle 441 on slot 27
Handle 150 on slot 26 is now handle 442 on slot 27
Handle 149 on slot 26 is now handle 445 on slot 27
Handle 146 on slot 26 is now handle 446 on slot 27
Handle 145 on slot 26 is now handle 449 on slot 27
Handle 142 on slot 26 is now handle 450 on slot 27
Handle 141 on slot 26 is now handle 453 on slot 27
Handle 138 on slot 26 is now handle 454 on slot 27
Handle 137 on slot 26 is now handle 457 on slot 27
Handle 134 on slot 26 is now handle 458 on slot 27
Handle 133 on slot 26 is now handle 461 on slot 27
Handle 130 on slot 26 is now handle 462 on slot 27
Handle 129 on slot 26 is now handle 465 on slot 27
Handle 126 on slot 26 is now handle 466 on slot 27
Handle 125 on slot 26 is now handle 469 on slot 27
Handle 122 on slot 26 is now handle 470 on slot 27
Handle 121 on slot 26 is now handle 473 on slot 27
Handle 118 on slot 26 is now handle 474 on slot 27
Handle 117 on slot 26 is now handle 477 on slot 27
Handle 114 on slot 26 is now handle 478 on slot 27
Handle 113 on slot 26 is now handle 481 on slot 27
Handle 110 on slot 26 is now handle 482 on slot 27
Handle 109 on slot 26 is now handle 485 on slot 27
Handle 97 on slot 26 is now handle 486 on slot 27
Handle 85 on slot 26 is now handle 489 on slot 27
Handle 94 on slot 26 is now handle 490 on slot 27
Handle 93 on slot 26 is now handle 493 on slot 27
Handle 89 on slot 26 is now handle 494 on slot 27
Handle 86 on slot 26 is now handle 497 on slot 27

Migrated 100 objects

Command Result : No Error

lunacm:>
```

Scroll back through the last hundred or so lines of Secure Log output, and see no mention of migration or insert/extract commands

```
9925517,22/01/14 20:38:13,S/N 18373207469733 session 5 Access 9b24f87f487d51eb operation LUNA_
OPEN_SESSION returned RC_OK(0x00000000) session handle 5
,60DABCE85788BEDFD0C7857D4330034EEDD747DB706547472E6DE707EB986940,8D7397408260240035DFE16100000
0009B24F87F487D51EBA52E81D8B5100000050000000000000000000000000000000000000000
9925518,22/01/14 20:38:13,S/N 18373207469733 session 5 Access 9b24f87f487d51eb operation LUNA_
CLOSE_SESSION returned RC_OK(0x00000000) session handle 5
,50AEBF8088ADF075AE9455A5112F3AACA09AB5E1CCE1D412D8BF357D31C1B87C,8E7397400260260035DFE16100000
0009B24F87F487D51EBA52E81D8B5100000050000000000000000000000000000000000000000
9925519,22/01/14 20:38:23,S/N 18373207469732 session 5 Access 9b24f87f487d51eb operation LUNA_
OPEN_SESSION returned RC_OK(0x00000000) session handle 5
,49CD7DFC8D0B287E2AA3489D7E187379253AA4D68B82388DC8955810A995DC3B,8F739740826024003FDFE16100000
0009B24F87F487D51EBA42E81D8B5100000050000000000000000000000000000000000000000
9925520,22/01/14 20:38:23,S/N 18373207469732 session 5 Access 9b24f87f487d51eb operation LUNA_
```

```
LOGIN returned RC_OK(0x00000000) roleID=0 container=6
,D9659DCEECFCD6052879937A937E4B3A92074E03A823CC93889F191FC66E0655,9073974002600D003FDFE16100000
0009B24F87F487D51EBA42E81D8B5100000050000000600000007000000000000000000000000
9925521,22/01/14 20:39:38,S/N 18373207469732 session 6 Access 9b24f87f487d51eb operation LUNA_
OPEN_SESSION returned RC_OK(0x00000000) session handle 6
,4C4F730BB22262F55140F142EB27670F64D3B9393722CE278A95FA6FC3DE1816,91739740826024008ADFE16100000
0009B24F87F487D51EBA42E81D8B5100000060000000000000000000000000000000000000000
9925522,22/01/14 20:39:38,S/N 18373207469733 session 7 Access 9b24f87f487d51eb operation LUNA_
OPEN_SESSION returned RC_OK(0x00000000) session handle 7
,FFB17D3BCFDE980AC91EBB09D62FD415A3341BB9A1211023B0FF4570F0030AA9,92739740826024008ADFE16100000
0009B24F87F487D51EBA52E81D8B5100000070000000000000000000000000000000000000000
9925523,22/01/14 20:39:38,S/N 18373207469733 session 7 Access 9b24f87f487d51eb operation LUNA_
LOGIN returned RC_OK(0x00000000) roleID=0 container=63
,DAC77E99B544B1F9A475106F90B456AB3A1829C1C356AE7B94A7B4E0A346437B,9373974002600D008ADFE16100000
0009B24F87F487D51EBA52E81D8B5100000070000003F000000070000000000000000000000
9925524,22/01/14 20:39:38,S/N 18373207469732 session 6 Access 9b24f87f487d51eb operation LUNA_
CLOSE_SESSION returned RC_OK(0x00000000) session handle 6
,1586983CA033CF8C8AB9A8E638ED971021D1D4B991945F9BB10E59FF15BCF8B2,94739740026026008ADFE16100000
0009B24F87F487D51EBA42E81D8B5100000060000000000000000000000000000000000000000
9925525,22/01/14 20:39:38,S/N 18373207469733 session 7 Access 9b24f87f487d51eb operation LUNA_
LOGOUT returned RC_OK(0x00000000) roleID=0 container=63
,A961ED9AAC4011288D8D9BDB4595FF67C28DF64D7B7D883C0003D523F526E43F,9573974002600E008ADFE16100000
0009B24F87F487D51EBA52E81D8B5100000070000003F000000000000000000000000000000
9925526,22/01/14 20:39:38,S/N 18373207469733 session 7 Access 9b24f87f487d51eb operation LUNA_
CLOSE_SESSION returned RC_OK(0x00000000) session handle 7
,0284B1730007D473C9FC37DA8221F636592E0B35B351FF5D4E5C16D87F9DE1F4,96739740026026008ADFE16100000
0009B24F87F487D51EBA52E81D8B5100000070000000000000000000000000000000000000000
9925527,22/01/14 20:40:18,S/N 18373207469732 session 5 Access 9b24f87f487d51eb operation LUNA_
CLOSE_SESSION returned RC_OK(0x00000000) session handle 5
,8212A73324B5EEC5E2AA7DA2BBBE04F17A5E7F0D0F978B34BB7298A5B4EA0F66,97739740026026008B2DFE16100000
0009B24F87F487D51EBA42E81D8B5100000050000000000000000000000000000000000000000
```

audit export

Export the audit logging secret to the user local directory for import to another HSM. The **audit export** command reads the log secret from the HSM, wrapped with the KCV which was used when the audit container was initialized. The blob of data is then stored in a file on the HOST. The audit officer then imports this wrapped secret into another HSM in the same domain, where it is unwrapped. This allows one HSM to verify logs that have been generated on another.

> **NOTE** After initializing the Audit role on a password-authenticated HSM, log in as the Auditor and set the domain (see "role setdomain" on page 221). This step is required before setting logging parameters or the log filepath, or importing/exporting audit logs.
>
> The **audit** commands appear only when LunaCM's active slot is set to the administrative partition.
>
> This command is not applicable on DPoD Luna Cloud HSM services.

Syntax

audit export [**file** <filename>] [**overwrite**] [**list**]

Argument(s)	Shortcut	Description
file <filename>	**f**	Enter this parameter followed by an optional filename for the file to receive wrapped log secret. If a file name is not specified, the file will be given a default name with the following structure: LogSecret_YYMMDDhhmmss_N.lws where YYMMDD = year/month/date hhmmss = hours/mins/secs N = HSM serial number This file will be written to the subdirectory which was set by a previous **audit config p [path]** command. If this path does not exist, or the configuration was not set for any reason, an error will be returned. If name was specified, it is examined to see if it contains subdirectories. If it does, then the path is treated as a fully qualified path name. If not the file is stored in the default log path.
overwrite	**o**	Overwrite the file if it already exists.
list	**l**	List the files which reside in the log path.

Example

```
lunacm:>audit export

        Successfully exported wrapped log secret to file '/var/audit/LogSecret_170222131119_
```

```
532018.lws'.

Command Result : No Error
```

audit import

Import an audit log secret that was exported using the **audit export** command. The Import command reads a wrapped log secret from a file, and sends it to the HSM where it will be unwrapped using that HSM's KCV If the second HSM is in the same domain, it can then be used to verify logs that were generated on the first one.

> **NOTE** After initializing the Audit role on a password-authenticated HSM, log in as the Auditor and set the domain (see "role setdomain" on page 221). This step is required before setting logging parameters or the log filepath, or importing/exporting audit logs.
>
> The **audit** commands appear only when LunaCM's active slot is set to the administrative partition.
>
> This command is not applicable on DPoD Luna Cloud HSM services.

Syntax

audit import [**file** <filename>] [**list**]

Argument(s)	Shortcut	Description
file <filename>	**f**	Name of file containing the wrapped log secret. If a file name is not specified, the user will be given a list of files in the directory which was set by a previous **audit config p [path]** If this path does not exist, or the configuration was not set for any reason, an error will be returned. If name was specified, it is examined to see if it contains subdirectories. If it does, then the path is treated as a fully qualified path name. If not the file is retrieved from the default log path.
list	**l**	Display a list of the files which reside in the log path.

Example

```
lunacm:>audit import file 150718.lws

Command Result : No Error
```

audit logmsg

Logs a message to the audit log file. If the message includes spaces, it must be enclosed in double quotes.

> **NOTE** The **audit** commands appear only when LunaCM's active slot is set to the administrative partition.
>
> This command is not applicable on DPoD Luna Cloud HSM services.

Syntax

audit logmsg "<message>"

Example

```
lunacm:> audit logmsg "Sample log message"

Command Result : No Error
```

audit status

Displays the Audit logging info for the indicated HSM.

> **NOTE** The **audit** commands appear only when LunaCM's active slot is set to the administrative partition.
>
> This command is not applicable on DPoD Luna Cloud HSM services.

Syntax

audit status [**-serial** <serialnum>]

Argument(s)	Shortcut	Description
-serial	**-s**	Specifies the serial number of the HSM for which you want to display the HSM Audit configuration. This can be the Luna PCIe HSM 7, or a USB-connected Luna Backup HSM.

Example

```
lunacm:>audit status

        HSM Auditor: initialized

        HSM Logging:
                HSM found logging daemon
                Logging has been configured
                HSM is currently storing 16 log records.


Command Result : No Error
```

audit time

Audit time commands allow you to check if the HSM time and the Host time match - which ensures that the log times of HSM events coincide with file creation and update events in the host file system - and to synchronize those times if needed.

> **NOTE** The **audit** commands appear only when LunaCM's active slot is set to the administrative partition.
>
> This command is not applicable on DPoD Luna Cloud HSM services.

Syntax

audit

get
sync

Argument(s)	Shortcut	Description
get	**g**	Show the current HSM and Host computer times, to see if they differ. See "audit time get" on the next page.
sync	**s**	Synchronize the HSM time to the Host computer system time to maintain alignment of HSM event log times with file creation and update events. See "audit time sync" on page 39.

 Copyright 2001-2026 Thales Group

audit time get

Compare the HSM time to the host time. The host computer might be synchronized by NTP, or by local drift correction. It is desirable that the log times of HSM events coincide with file creation and update events in the host file system. This command shows any discrepancies between the two time settings, alerting you to use the "audit time sync" on the next page command if needed.

> **NOTE** The **audit** commands appear only when LunaCM's active slot is set to the administrative partition.
>
> This command is not applicable on DPoD Luna Cloud HSM services.

Syntax

audit time get

Example

```
lunacm:>audit time get

System time from HSM : Fri Feb 24 17:00:42 2017
System time from HOST: Fri Feb 24 17:00:33 2017
Difference           : 9 sec

Command Result : No Error
```

audit time sync

Synchronize the HSM time to the host time. Use this command to have the HSM adjust its time to match that of the host computer. This is especially useful when the host computer is synchronized by NTP, or by local drift correction. Among other benefits, this ensures that the log times of HSM events coincide with file creation and update events in the host file system. Use the "audit time get" on the previous page command to determine whether a 'sync' is needed.

> **NOTE** The **audit** commands appear only when LunaCM's active slot is set to the administrative partition.
>
> This command is not applicable on DPoD Luna Cloud HSM services.

Syntax

audit time sync [**-force**]

Argument(s)	Shortcut	Description
-force	**-f**	Forces the action, bypassing prompts; useful for scripting.

Example

```
lunacm:>audit time sync

        The HSM clock will be synchronized with the HOST clock.
        Are you sure you wish to continue?

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

HSM time was synchronized to HOST

Command Result : No Error
```

Example with "force" option

```
lunacm:>audit time sync -force

HSM time was synchronized to HOST

Command Result : No Error
```

audit verify

Verify the audit log records. This command displays details for the indicated file, or verifies records in the specified range from the named file.

> **NOTE** If the log file is archived (tar or tgz) it must be untarred/unzipped before **audit verify** can work on records in that log. You cannot verify a ".tgz" file directly. The audit verify command is not able to verify a log that was in-progress when it was archived. Only logs from the ready_for_archive folder, logs that have been completed and closed, can be verified. This usually means that if you cannot verify the most recent log entry in an archive, then that same entry is probably the first log entry in the next archive, where it was properly closed and can be verified.
>
> The **audit** commands appear only when LunaCM's active slot is set to the administrative partition.
>
> This command is not applicable on DPoD Luna Cloud HSM services.

Syntax

audit verify [**start** <start record>] [**end** <end record>] **file** <fully_qualified_filename> [**details**]

Argument(s)	Shortcut	Description
start	**s**	The index of the first record in file to verify. If this parameter is omitted, the first record in file is assumed.
end	**e**	The index of the last record in file to verify. If this parameter is omitted, the last record in file is assumed.
file	**f**	The fully-qualified name of file containing data to verify. This is the only mandatory parameter.
details	**d**	Show details for file. This includes the first and last timestamps, first and last record sequence numbers, and total number of records in the file. It does not verify the contents of the file. To do so, run **audit verify file <filename>** without the **details** parameter.

Example

```
lunacm:>audit verify file hsm_66331_00000001.log details start 1 end 46
file /var/audit/66331/hsm_66331_00000001.log: 270541 records
first record: sequence number          1, timestamp       NO HSM TIME
last record:  sequence number     270540, timestamp 17/02/27 14:33:21

        Verified messages 1 to 46

Command Result : No Error
```

 Copyright 2001-2026 Thales Group

clientconfig

Access the clientconfig-level commands to configure your client to connect to a Luna Network HSM 7.

Syntax

clientconfig

deleteserver
deploy
listservers
restart
verify

Argument(s)	Shortcut	Description
deleteserver	**d**	Delete a Luna Network HSM 7 server. See "clientconfig deleteserver" on the next page.
deploy	**dp**	Create a network Trust Link (NTL) between the client and the Luna Network HSM 7 in one step. See "clientconfig deploy" on page 43.
listservers	**ls**	List the Luna Network HSM 7 appliances that are registered to the client. See "clientconfig listservers" on page 45.
restart	**rest**	Restart LunaCM. See "clientconfig restart" on page 46.
verify	**v**	Verify the Luna Network HSM 7 slots/partitions that are visible to the client. See "clientconfig verify" on page 47.

 Copyright 2001-2026 Thales Group

clientconfig deleteserver

Delete a Luna Network HSM 7 server from the client.

Syntax

clientconfig deleteserver -server <server_name>

Argument(s)	Shortcut	Description
-server <server_name>	**-n**	The name of the server to be deleted.

Example

```
lunacm:> clientconfig deleteserver -server 192.20.11.78

Server 192.20.11.78 successfully removed from server list.


Command Result : No Error
```

clientconfig deploy

Creates a Network Trust Link between the client and a Luna Network HSM 7 appliance. This command creates a client Private Key and Certificate, and uses **pscp** or **sftp** to transfer the client and server certificates to each other.

> **NOTE** If **pscp** or **sftp** is blocked by a firewall, this command will fail and the certificates must be transferred by other secure means and registered manually.

Syntax

clientconfig deploy -server <server_IP> **-client** <client_IP> **-partition** <partition_name> [**-password** <your_unique_password_for_partitiono>] [**-hsmPassword** <your_unique_password_for_hsmsoo>] [**-user** <username>] [**-regen**] [**-verbose**] [**-force**]

Argument(s)	Shortcut	Description
-client <client_IP>	**-c**	The client hostname or IP.
-hsmPassword <HSMSO_password>	**-hsmpw**	The HSM SO password. This option is required only if HSM SO login enforcement is enabled on Luna Network HSM 7.
-force	**-f**	Force the action without prompting for confirmation.
-partition <partition_name>	**-par**	The name of the partition to be assigned to the client. This partition must be created in advance using LunaSH.
-password <password>	**-pw**	Password of the Luna Network HSM appliance's admin-capable user that is running this command. Default is admin, or can be a custom-defined user having requisite admin privileges.
-regen	**-rg**	Including this option will regenerate and replace any current client certificate with the default 2048-bit RSA certificate. This may disrupt connections to other Luna Network HSM 7 servers. If you need your client to use larger RSA keysizes, then generate via the **vtl** utility instead.
-server <server_IP>	**-n**	The server hostname or IP.
-verbose	**-v**	Show more detailed logs during the procedure.
-user <username>	**-ur**	Username of the Luna Network HSM appliance user running this command – can be admin or can be a custom user with admin privileges, if you have created one for the target appliance. **Default: admin**

Example

```
lunacm:> clientconfig deploy -server 192.20.11.78 -client 192.20.11.129 -partition par1 -
password <your_unique_password_for_appliance admin> -user admin
Please wait while we set up the connection to the HSM. This may take several minutes...

Last login: Wed Feb 22 10:06:59 2020 from 192.20.11.129

Luna Network HSM 7.7.0 Command Line Shell - Copyright (c) 2001-2020 SafeNet, Inc. All rights
reserved.


Private Key created and written to: C:\Program
Files\SafeNet\LunaClient\cert\client\192.20.11.129Key.pem
Certificate created and written to: C:\Program
Files\SafeNet\LunaClient\cert\client\192.20.11.129.pem



New server 192.20.11.78 successfully added to server list.



The following Luna Network HSM Slots/Partitions were found:


Slot    Serial #               Label
====    ================       =====
   0       1238700701510       par0
   1        154438865312


Command Result : No Error
```

clientconfig listservers

List the Luna Network HSM 7 appliances that are registered to the client.

Syntax

clientconfig listservers

Example

```
lunacm:> clientconfig listservers

 Server ID  Server                          Channel
 ____________________________________________________________________

 0          192.20.11.40                    STC

 1          192.20.11.78                    NTLS


Command Result : No Error
```

clientconfig restart

Restart LunaCM. This command refreshes the LunaCM display to show any changes.

Syntax

clientconfig restart [**-force**]

Argument(s)	Shortcut	Description
-force	**-f**	Force the action without prompting for confirmation.

Example

```
lunacm:> clientconfig restart

        You are about to restart this application.
        All current login sessions and remote PED connections will be terminated.
        Are you sure you wish to continue?

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

Command Result : No Error



LunaCM v7.0.0. Copyright (c) 2006-2017 SafeNet, Inc.

        Available HSMs:

        Slot Id ->              0
        Label ->                par0
        Serial Number ->        1238700701510
        Model ->                LunaSA
        Firmware Version ->     7.0.1
        Configuration ->        Luna User Partition With SO (PED) Signing With Cloning Mode
        Slot Description ->     Net Token Slot

        Slot Id ->              1
        Label ->                par1
        Serial Number ->        154438865312
        Model ->                LunaSA 7.0.0
        Firmware Version ->     7.0.1
        Configuration ->        Luna User Partition With SO (PW) Signing With Cloning Mode
        Slot Description ->     Net Token Slot


        Current Slot Id: 0
```

clientconfig verify

Generates a list of Luna Network HSM 7 slots/partitions that are visible to the client.

Syntax

clientconfig verify

Example

```
lunacm:> clientconfig verify

The following Luna SA Slots/Partitions were found:

Slot    Serial #               Label
====    ================       =====
   0       1238700701510       par0
   1        154438865312       par1


Command Result : No Error
```

file display

> **NOTE** This command is deprecated and will be removed in a future release. It was used with backup files generated by, and compatible with firmware versions that were end-of-life long ago.

Display the contents of a backup file.

Syntax

file display -filename <filename>

Argument(s)	Shortcut	Description
-filename <filename>	**-f**	Specify the name of the backup file to display. Enter this keyword followed by the name of an existing backup file.

Example

```
lunacm:> file display -filename somepartfile

File Name:              somepartfile
File Version:           0
SIM Form:               CKA_SIM_PORTABLE_NO_AUTHORIZATION
Object Count:           3
Source Serial Number:   321312 (0x4e720)

Object: 1
Attribute Count: 23
CKA_CLASS: CKO_SECRET_KEY
CKA_TOKEN: True
CKA_PRIVATE: True
CKA_LABEL:
47 65 6E 65 72 61 74 65 64 20 44 45 53 33 20 4B
65 79
CKA_KEY_TYPE: CKK_DES3
CKA_SENSITIVE: True
CKA_ENCRYPT: True
CKA_DECRYPT: True
CKA_WRAP: True
CKA_UNWRAP: True
CKA_SIGN: True
CKA_VERIFY: True
CKA_DERIVE: True
CKA_LOCAL: True
CKA_MODIFIABLE: True
CKA_EXTRACTABLE: True
CKA_ALWAYS_SENSITIVE: True
CKA_NEVER_EXTRACTABLE: False
CKA_CCM_PRIVATE: False
CKA_FINGERPRINT_SHA1:
E2 EB 1B 86 58 BB 6C EF 07 87 4C 59 D4 06 73 7D
5E 4D 3A 65
```

hagroup

Access the **hagroup**-level commands. The **hagroup** commands are used to manage and administer HA (high availability) groups of Luna HSM partitions for redundancy and load balancing.

Syntax

hagroup

- **addmember**
- **addstandby**
- **creategroup**
- **deletegroup**
- **halog**
- **haonly**
- **interval**
- **listgroups**
- **recover**
- **recoverymode**
- **removemember**
- **removestandby**
- **retry**
- **synchronize**

Argument(s)	Shortcut	Description
addmember	**am**	Add a member to an HA group. See "hagroup addmember" on page 51.
addstandby	**as**	Convert an HA group member to a standby member. See "hagroup addstandby" on page 53.
creategroup	**c**	Create an HA group. See "hagroup creategroup" on page 54.
deletegroup	**d**	Delete an HA group . See "hagroup deletegroup" on page 57.
halog	**hl**	Configure the HA log file. See "hagroup halog" on page 58.
haonly	**ho**	Enable "HA Only" mode. See "hagroup haonly" on page 60.
interval	**i**	Set the HA recover retry interval. See "hagroup interval" on page 61
listgroups	**l**	List the currently-configured HA groups. See "hagroup listgroups" on page 62.
recover	**re**	Recover a failed HA member. See "hagroup recover" on page 63.

Argument(s)	Shortcut	Description
recoverymode	**m**	Set HA recovery mode to "activeBasic" or "activeEnhanced". See "hagroup recoverymode" on page 64.
removemember	**rm**	Remove a member from an HA group. See "hagroup removemember" on page 65.
removestandby	**rs**	Convert a standby member to an active member of the HA group. See "hagroup removestandby" on page 66.
retry	**rt**	Set the HA recover retry count. See "hagroup retry" on page 67
synchronize	**s**	Synchronize an HA group. See "hagroup synchronize" on page 68

TIP Change in scripted operation from Luna HSM 6.x to Luna HSM 7.x

When scripting multi-step operations, a common way to provide responses to interactive commands (example, the lunacm **hagroup creategroup** command needs a response of "copy", or "remove", or "quit") is to use "echo" to pipe the response text into the command within your script.

This worked well for Luna 5.x/6.x, in the below example presenting "copy" to resolve the interim prompt.

```
"echo copy | lunacm -q hagroup creategroup -serialNumber <serialNumber> -label
<HAgroupName>  -password <partitionPass>"
```

To accomplish the same result with Luna 7.x.x, do the following:

1. Create a file, in this example, “copy.txt” that contains only the word “copy” as its content.
2. Run the “lunacm” commands as below to create the HA group, and to add a member to the HA group, while inputting the “copy” prompt:
   - In cmd (for .bat script):

     ```
     type copy.txt | lunacm -c hagroup creategroup -label HA -slot 0 -p ********
     type copy.txt | lunacm -c hagroup addmember -group HA -slot 1 -p ********
     ```
   - In Powershell (for powershell script) :

     ```
     Get-Content .\copy.txt | .\lunacm.exe -c hagroup creategroup -label HA -
     slot 0 -p ********
     Get-Content .\copy.txt | .\lunacm.exe -c hagroup addmember -group HA -slot
     1 -p ********
     ```

Use the same technique in similar situations.

hagroup addmember

Add a member to an HA group. Use the **-slot** option or the **-serialnumber** option to specify which HSM to add to the group.

All password-authenticated HA group members must have the same password.

All multifactor quorum-authenticated HA group members must have a challenge created, and activation turned on, and all challenges must be the same. See Activation on Multifactor Quorum-Authenticated Partitions for more information.

If you intend to add a standby member to the group, you must first use this command to add the member to the group, then use the LunaCM **hagroup addstandby** command to convert the member to standby status. By default, Luna Cloud HSM services are added as standby members.

> **NOTE V1 partitions:** If you add an application partition with an existing SMK to an HA group, the primary member's SMK overwrites the existing SMK of the joining partition.
>
> If a partition's SMK has ever been used to encrypt important SKS objects, save a backup of the SMK before adding that partition to any HA group.

> **NOTE** If you are planning or setting up an HA group, note the following:
>
> - A partition at Luna HSM Firmware 7.7.0 or newer cannot be a primary for an HA group where a secondary member firmware version is older than 7.7.0.
> - Luna HSM Client 10.4.0 allows creation of groups with a mix of FIPS and non-FIPS member partitions.

Syntax

hagroup addmember {**-serialnumber** <serialnum> | **-slot** <slotnumber>} **-group** <label> **-password** <password>

Argument(s)	Shortcut	Description
-serialnumber <serialnum>	**-se**	Serial number of the member to add. This option is mandatory if **-slot** is not used. The serial number that identifies the partition being added to the HA group.
-slot <slotnumber>	**-sl**	Slot number of the member to add. This option is mandatory if **-serialnumber** is not used. A slot number to identify the partition being added to the HA group.
-group <label>	**-g**	Label for the group being joined.
-password <password>	**-p**	Crypto Officer password or challenge secret for the partition. This password must be the same for all HA group member partitions.

Example

```
lunacm:> hagroup addmember -serialnumber 1238700701515 -group myHAgroup

        Enter the password: ********
        Member 1238700701515 successfully added to group myHAgroup. New group
        configuration is:

         HA Group Label:  myHAgroup
        HA Group Number:  1154438865288
       HA Group Slot ID:  5
       Synchronization: enabled
          Group Members:  154438865288, 1238700701515
              Needs sync:  yes
        Standby Members:  <none>


Slot #    Member S/N                      Member Label    Status
======    ==========                      ============    ======
     0  154438865288                           sa78-2     alive
     1  1238700701515                           sa40-2     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
```

hagroup addstandby

Make an existing member of the HA group a standby member. Use the **-serialnumber** option to specify which HSM to make a standby member. You must add a member before you can make it a standby member.

Syntax

hagroup addstandby -serialnumber <serialnum> **-group** <label>

Argument(s)	Shortcut	Description
-serialnumber <serialnum>	**-s**	Serial number of the member being made standby.
-group <label>	**-g**	Label or serial number for the existing member's group.

Example

```
lunacm:> hagroup addstandby -serialnumber 1238700701515 -group myHAgroup

        The member 1238700701515 was successfully added to the standby list for the HA Group
myHAgroup.


Command Result : No Error
```

hagroup creategroup

Create an HA group. Use the **-slot** or **-serialnumber** options to specify the primary member for the group. All password-authenticated HA group members must have the same password. All multifactor quorum-authenticated HA group members must have a challenge created, and activation turned on, and all challenges must be the same. See Activation on Multifactor Quorum-Authenticated Partitions for more information. By default, you cannot create a group using a Luna Cloud HSM service as the primary member; it must be added to an existing group.

However, if you prefer to use the Luna Cloud HSM service as an active HA member, you must first edit the following toggle in the **Chrystoki.conf/crystoki.ini** configuration file (see Configuration File Summary):

```
[Toggles]
lunacm_cv_ha_ui = 0
```

> **CAUTION!** Failover to Luna Cloud HSM is supported in an HA group with password-authenticated Luna partitions only. When configured in an HA group with multifactor quorum-authenticated Luna partitions, Luna Cloud HSM functions as a backup only.

> **NOTE** Using Luna HSM Client 10.9.4 or older, apply labels no longer than 31 characters to a new HA group. The creation of an HA group, in client versions up to this point, allows *input* of as many as 32 characters for the group label, but *incorrectly trims* the 32nd character. For any label with fewer than 32 characters, that is not an issue. For a previously input 32-character label, the **hagroup deletegroup** command fails to recognize the label and does not delete the group.
>
> Further, an attempt to create a second HA group with a label that differed from the first by only the 32nd character, would cause lunacm to see that as a duplicate and present an error saying the label is already being used.
>
> **WORKAROUND:** When using the **deletegroup** command against an HA group with a label that was nominally 32 characters, provide just the first 31 characters for your group label. The deletion proceeds properly.
> When *creating* an HA group using Luna HSM Client 10.9.4 or older, restrict labels to maximum 31 characters.

For a more in-depth look at HA groups and their options please see High-Availability Groups.

Syntax

hagroup creategroup {**-serialnumber** <serialnum> | **-slot** <slotnumber>} **-label** <label> **-password** <password>

Argument(s)	Shortcut	Description
-serialnumber <serialnum>	**-se**	Serial number of the partition selected to be the primary member of the HA group.

Argument(s)	Shortcut	Description
-slot <slotnumber>	**-sl**	Slot number of the partition selected to be the primary member of the HA group.
-label <label>	**-l**	Label for the HA group being created.
-password <password>	**-p**	Crypto Officer password or challenge secret for the primary partition. This password must be the same for all HA group member partitions.

Example

```
lunacm:> hagroup creategroup -serialnumber 154438865288 -label myHAgroup

        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


        New group with label "myHAgroup" created with group number 1154438865288.
        Group configuration is:

         HA Group Label:  myHAgroup
        HA Group Number:  1154438865288
       HA Group Slot ID:  Not Available
        Synchronization: enabled
          Group Members:  154438865288
              Needs sync:  no
        Standby Members:  <none>

Slot #    Member S/N                    Member Label    Status
======    ==========                    ============    ======
     0  154438865288                          sa78-2     alive


Command Result : No Error



LunaCM v7.0.0. Copyright (c) 2006-2017 SafeNet.

        Available HSMs:

        Slot Id ->              0
        Label ->                sa78-2
        Serial Number ->        154438865288
        Model ->                LunaSA 7.0.0
```

```
Firmware Version ->     7.0.1
Configuration ->        Luna User Partition With SO (PW) Signing With Cloning Mode
Slot Description ->     Net Token Slot

Slot Id ->              1
Label ->                sa40-2
Serial Number ->        1238700701515
Model ->                LunaSA 7.0.0
Firmware Version ->     7.0.1
Configuration ->        Luna User Partition With SO (PW) Signing With Cloning Mode
Slot Description ->     Net Token Slot

Slot Id ->              5
HSM Label ->            myHAgroup
HSM Serial Number ->    1154438865288
HSM Model ->            LunaVirtual
HSM Firmware Version -> 7.0.1
HSM Configuration ->    Luna Virtual HSM (PW) Signing With Cloning Mode
HSM Status ->           N/A - HA Group



Current Slot Id: 0
```

hagroup deletegroup

Delete an HA group. Use the **-label** option to specify the group to be deleted.

Syntax

hagroup deletegroup -label <label>

Argument(s)	Short	Description
-label <label>	**-l**	Label of the group being deleted.

Example

```
lunacm:> hagroup deletegroup -label myHAgroup

        The HA group myHAgroup was successfully deleted.

Command Result : No Error
```

> **NOTE** Using Luna HSM Client 10.9.4 or older, apply labels no longer than 31 characters to a new HA group. The creation of an HA group, in client versions up to this point, allows *input* of as many as 32 characters for the group label, but *incorrectly trims* the 32nd character. For any label with fewer than 32 characters, that is not an issue. For a previously input 32-character label, the **hagroup deletegroup** command fails to recognize the label and does not delete the group.
>
> Further, an attempt to create a second HA group with a label that differed from the first by only the 32nd character, would cause lunacm to see that as a duplicate and present an error saying the label is already being used.
>
> **WORKAROUND:** When using the **deletegroup** command against an HA group with a label that was nominally 32 characters, provide just the first 31 characters for your group label. The deletion proceeds properly.
> When *creating* an HA group using Luna HSM Client 10.9.4 or older, restrict labels to maximum 31 characters.

hagroup halog

Configure the HA log.

Syntax

hagroup halog {**-disable** | **-enable** | **-maxlength** <max_file_length> | **-path** <filepath> | **-show**}

Argument(s)	Shortcut	Description
-disable	**-d**	Disable HA logging.
-enable	**-e**	Enable HA logging.
-maxlength <max_file_length>	**-m**	Set the maximum length for the HA log file. The default and minimum size is 40000 bytes. Any proposed number from 0-through-39999 results in an error message. A failure due to an out-of-bounds -maxlength results in the current value remaining unchanged (either the default or a larger number that was previously set).
-path <filepath>	**-p**	Set the location for the HA log file. You must enclose the path specification in quotes if it contains spaces.
-show	**-s**	Display the HA log configuration.

Example

```
lunacm:> hagroup halog -maxlength 500000

        HA Log maximum file size was successfully set to 500000.

Command Result : No Error


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


lunacm:> hagroup halog -enable

        HA Log was successfully enabled.

Command Result : No Error
```

```
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



lunacm:> hagroup halog -disable

        HA Log was successfully disabled.

Command Result : No Error
```

hagroup haonly

Enable, disable, or display the HA-only mode configuration for the group.

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).

> **NOTE** Individual partition slots remain 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.

Syntax

hagroup haonly {**-enable** | **-disable** | **-show**}

Argument(s)	Shortcut	Description
-enable	**-e**	Enable HA Only mode for the current group.
-disable	**-d**	Disable HA Only mode for the current group.
-show	**-s**	Show the status of HA Only mode for the current group.

Example

```
lunacm:> hagroup haonly -enable

        "HA Only" has been enabled.

Command Result : No Error


lunacm:> hagroup haonly -show

        This system is configured to show only HA slots.  (HA Only is enabled)

Command Result : No Error
```

hagroup interval

Modify the HA Recover retry interval.

For HA recovery attempts:

- The default retry interval is 60 seconds.
- The default number of retries is 0, which means that automatic recovery is disabled.
- The HA configuration section in the **Chrystoki.conf/crystoki.ini** file is created and populated when either the interval or the number of retries is specified in the LunaCM commands "hagroup retry" on page 67 and "hagroup interval" above.

Syntax

hagroup interval -interval <seconds>

Argument(s)	Shortcut	Description
-interval <seconds>	**-i**	Sets the number of seconds between attempts to recover a failed HA group member. **Default:** 60 seconds **Range:** 60 to 1200 seconds

Example

```
lunacm:> hagroup interval -interval 120

        HA Auto Recovery Interval has been set to 120 seconds.

Command Result : No Error
```

hagroup listgroups

List all configured HA groups and all of their members, and show their synchronization status.

> **NOTE** Changes that are initiated from the appliance (for example, revoking the client's access to a partition with lunash:> client revokePartition) may not be reported correctly until a new LunaCM session is opened.

Syntax

hagroup listgroups

Example

```
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:  1154438865288
       HA Group Slot ID:  7
       Synchronization: enabled
          Group Members:  154438865288, 1238700701515, 154438865289, 1238700701516
             Needs sync:  yes
        Standby Members:  1238700701516

Slot #    Member S/N                    Member Label    Status
======    ==========                    ============    ======
     0  154438865288                          sa78-2     alive
     2  1238700701515                          sa40-2     alive
     1  154438865289                          sa78-3     alive
     3  1238700701516                          sa40-3     alive

Command Result : No Error
```

hagroup recover

Recover any failed members of an HA group. Use the **-group** option to specify which HA group to recover.

Syntax

hagroup recover -group <label>

Argument(s)	Shortcut	Description
-group <label>	**-g**	Specifies the label for the group to recover.

Example

```
lunacm:> hagroup recover -group myHAgroup

        Signal sent to HA Group "myHAgroup" to recover.

Command Result : No Error
```

 Copyright 2001-2026 Thales Group

hagroup recoverymode

Set HA recovery mode to active basic or active enhanced automatic recovery.

Syntax

hagroup recoverymode -mode {**activeBasic** | **activeEnhanced**}

Argument(s)	Shortcut	Description
-mode <mode>	**-m**	Specifies method of HA automatic recovery. **Valid values:** **activeBasic** - uses a separate Active Recovery Thread to perform background checks of HA member presence and runs synchronization if a member fails/leaves and then returns to availability; attempts to reconnect with the members if all members were simultaneously unavailable. Does not restore existing sessions. Luna Network HSM 7 appliances do not have to restart, login is manual. **activeEnhanced** - works like activeBasic, but additionally restores all sessions and their login states

Example

```
lunacm:> hagroup recoveryMode -mode activeBasic

        HA Auto Recovery Mode has been set to activeBasic mode.

Command Result : No Error
```

hagroup removemember

Remove a member partition from an existing HA group. Use the **-slot** option or the **-serialnumber** option to specify which partition to remove from the group specified by the **-group** option.

Syntax

hagroup removemember {**-serialnumber** <serialnum> | **-slot** <slotnumber>} **-group** <label>

Argument(s)	Shortcut	Description
-serialNumber <serialnum>	**-se**	Serial number of the member to remove from the HA group.
-slot <slotnumber>	**-sl**	Slot number of the member to remove from the HA group.
-group <label>	**-g**	Label for the existing HA group to which the member belongs.

Example

```
lunacm:> hagroup removemember -serialnumber 1238700701515 -group myHAgroup

        Member 1238700701515 successfully removed from group myHAgroup.


Command Result : No Error
```

hagroup removestandby

Convert a standby member of an HA group to an active member. The member must be online to remove it from standby. If the standby member is offline, wait for it to come back online or remove it from the HA group using lunacm:> **"hagroup removemember" on the previous page**.

By default, a Luna Cloud HSM service cannot be removed from standby. It can only be removed from the HA group using lunacm:> **"hagroup removemember" on the previous page**.

Syntax

hagroup removestandby -serialnumber <serialnum> **-group** <label>

Argument(s)	Shortcut	Description
-serialnumber <serialnum>	**-se**	Serial number of the standby member to change to active in the named HA group.
-group <label>	**-g**	Label for the HA group being modified.

Example

```
lunacm:> hagroup removestandby -serialnumber 1238700701515 -group myHAgroup

        The member 1238700701515 was successfully removed from the standby list for the HA
Group myHAgroup.


Command Result : No Error
```

hagroup retry

Modify the HA recovery retry count. The retry count specifies the number of times the system attempts to recover a failed member. The interval between retries is specified by the command "hagroup interval" on page 61.

For HA recovery attempts:

- The default retry interval is 60 seconds.
- The default number of retries is 0, which means that automatic recovery is disabled.
- The HA configuration section in the **Chrystoki.conf/crystoki.ini** file is created and populated when either the interval or the number of retries is specified in the LunaCM commands "hagroup retry" above and "hagroup interval" on page 61.

Syntax

hagroup retry -count <retries>

Argument(s)	Shortcut	Description
-count <retries>	**-c**	Sets the number of times the HA controller attempts to recover a member that fails. Enter a value of **-1** to specify unlimited retries. Enter a value of **0** to disable HA auto-recovery. **Default:** 0 **Range:** -1 to 500

Example

```
lunacm:> hagroup retry -count -1

        HA Auto Recovery Count has been set to -1

Command Result : No Error
```

hagroup synchronize

Synchronize an HA group or enable/disable key synchronization for key export applications. This command is only required if you have declined to use auto-recovery with your HA group.

> **NOTE** If you are using Luna HSM Client 10.4.0 or newer and run this command to synchronize an HA group with a mix of FIPS and non-FIPS partitions as members, any non-FIPS keys will fail to replicate to the FIPS member(s). An error is returned when this occurs, but lunaCM synchronizes everything else.

Syntax

hagroup synchronize -group <label_or_serialnum> [**-password** <password>] [**-enable** | **-disable**]

Argument(s)	Shortcut	Description
-disable	**-d**	Disable synchronization for this HA group. This option allows you to disable synchronization on HA groups that use HSMs configured for key export (KE) to wrap asymmetric private RSA keys. In this model, you create your symmetric wrapping keys, which are synchronized to each member of the HA group. After synchronizing the symmetric wrapping keys, you disable synchronization and begin creating your asymmetric RSA keys. If one of the HA members fails, the remaining members are still able to generate and wrap asymmetric private RSA keys using the synchronized symmetric wrapping key.
-enable	**-e**	Enable synchronization for this HA group. Synchronization is enabled by default. You require this setting only if you wish to re-enable synchronization on an HA group where synchronization was previously disabled. For example, to create and synchronize a new symmetric wrapping key.
-group <label_or_serialnum>	**-g**	Label or serial number for the HA group being synchronized.
-password <password>	**-p**	Password for the group.

Example

```
lunacm:> hagroup synchronize -group myHAgroup

        Enter the password: ********

        Synchronization completed.

Command Result : No Error


lunacm:> hagroup synchronize -group myHAgroup -disable
```

```
        HA synchronization disabled

        No synchronization performed/needed.

Command Result : No Error
```

hsm

Access the HSM-level commands.

> **NOTE** The "hsm" above commands appear only when LunaCM's active slot is set to the administrative partition.

Syntax

hsm

changehsmpolicy
envshow
factoryreset
init
migratepedkey
monitor
resetUtilization
restart
rollbackfw
showinfo
showmechanism
showpolicies
showUtilization
smkclone
smkrollover
tamperclear
tampershow
time
updatecap
updatefw
zeroize

Argument(s)	Shortcut	Description
changehsmpolicy	**changehp**	Change the HSM Policy value. See "hsm changehsmpolicy" on page 72.
envshow	**es**	Display environmental status information for the card. See "hsm envshow" on page 73.
factoryreset	**f**	Factory reset the HSM. See "hsm factoryreset" on page 74.
init	**i**	Initialize the HSM. See "hsm init" on page 76.
migratepedkey	**mig**	Migrate a PED Key from a legacy HSM. See "hsm migratepedkey" on page 80.

 Copyright 2001-2026 Thales Group

Argument(s)	Shortcut	Description
monitor	**mon**	Get HSM utilization information. See "hsm monitor" on page 81.
resetUtilization	**ru**	Reset utilization metrics. See "hsm resetUtilization" on page 82.
restart	**rs**	Restart the HSM. See "hsm restart" on page 84.
rollbackfw	**rb**	Rollback the HSM firmware. See "hsm rollbackfw" on page 85.
showinfo	**si**	Get HSM information. See "hsm showinfo" on page 86.
showmechanism	**showm**	Show all mechanisms. See "hsm showmechanism" on page 89.
showpolicies	**sp**	Get HSM policy information. See "hsm showpolicies" on page 91.
showUtilization	**su**	Show Utilization Metrics. See "hsm showUtilization" on page 93.
smkclone	**smkc**	Clone the SKS Master Key. See "hsm smkclone" on page 95.
smkrollover	**smkr**	Rollover the SKS Master Key. See "hsm smkrollover" on page 97.
tamperclear	**tc**	Unlock the HSM following a tamper event. See "hsm tamperclear" on page 99
tampershow	**ts**	Display the current tamper state for the HSM. See "hsm tampershow" on page 100
time	**t**	Display the current HSM time, and synchronize HSM time with host time. See "hsm time" on page 100
updatecap	**uc**	Update the HSM capabilities. See "hsm updatecap" on page 103.
updatefw	**uf**	Update the HSM firmware. See "hsm updatefw" on page 104.
zeroize	**z**	Put the HSM in a zeroized state. See "hsm zeroize" on page 105.

 Copyright 2001-2026 Thales Group

hsm changehsmpolicy

Change HSM-level policies. This command changes the specified HSM Policy from the current value to the new, specified value, if the corresponding HSM capability setting permits the change.

> **NOTE** The "hsm" on page 70 commands appear only when LunaCM's active slot is set to the administrative partition.

Syntax

hsm changehsmpolicy -policy <number> **-value** <value> [**-force**]

Argument(s)	Shortcut	Description
-force	**-f**	Force the change without further prompting.
-policy <number>	**-p**	The number identifying the HSM policy that you want to change. Use the **hsm show** command to find the number of the policy you want to change.
-value <value>	**-v**	The new setting to be applied to the indicated HSM policy. Use the **hsm show** command to find the current setting of the policy you want to change.

Example

```
lunacm:>hsm changehsmpolicy -policy 12 -value 0

        You are about to change a destructive HSM policy.
        All partitions of the HSM will be destroyed.

        Are you sure you wish to continue?

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

Command Result : No Error
```

hsm envshow

Display environmental status information for the card. The following information is displayed:

- the card temperature.
- the card temperature warning threshold. If the card reaches this temperature, a warning is displayed in the output and logged.
- the status of the fans.
- the battery voltage.
- the battery voltage warning threshold. If the battery voltage falls below this level, a warning is displayed in the output and logged.

> **NOTE** The "hsm" on page 70 commands appear only when LunaCM's active slot is set to the administrative partition.

Syntax

hsm envshow

Example

Normal conditions

```
lunacm:>hsm envshow

        Environmental:
                Fan 1 Status                            : standby
                Fan 2 Status                            : active
                Battery Voltage                         : 3.093 V
                Battery Warning Threshold Voltage       : 2.750 V
                System Temp                             : 35 deg. C
                System Temperature Warning Threshold    : 75 deg. C

Command Result : No Error
```

Temperature/voltage outside warning threshold

```
lunacm:> hsm envshow

        Environmental:
                Fan 1 Status                            : failed
                Fan 2 Status                            : active
                Battery Voltage                         : 2.615 V
                Battery Warning Threshold Voltage       : 2.750 V
WARNING: Battery Voltage below warning threshold!!
                System Temp                             : 77 deg. C
                System Temperature Warning Threshold    : 75 deg. C
WARNING: System Temperature above warning threshold!!

Command Result : No Error
```

hsm factoryreset

Reset the HSM to its factory configuration. Use this command to set the HSM back to factory default settings, clearing all contents (puts HSM in zeroized state). Because this is a destructive command, the user is asked to “proceed” unless the **-force** switch is provided at the command line. This command resets settings and configuration, but does not perform firmware rollback or uninstall new capabilities installed since the HSM came from the factory.

> **NOTE** The "hsm" on page 70 commands appear only when LunaCM's active slot is set to the administrative partition.

For eIDAS compliance, **hsmrecover** function is added to factoryreset commands - see Stored Data Integrity.

The standalone **hsmrecover** tool in the tools folder performs the same action, but can present additional messages that might be useful to Support engineers.

Syntax

hsm factoryreset [**-force**]

Argument(s)	Shortcut	Description
-force	**-f**	Force the action without prompts. If this option is included in the list, the HSM will be zeroized without prompting the user for a confirmation of this destructive command.

Example

```
lunacm:>hsm factoryreset

        Error communicating with the HSM.

        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.

        Are you sure you wish to continue?

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

        Resetting HSM


 Command Result : No Error
```

Example output showing extended hsmrecover attempts

```
lunacm:>hsm factoryreset

        Error communicating with the HSM.
```

```
        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.

        Are you sure you wish to continue?

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

        Resetting HSM
        lunaserver: cannot reset token: Input/output error

        HSM Firmware not responding. Trying factory reset again.
        This operation may take several minutes . . . . . .

Command Result : No Error
```

hsm init

Initialize the Luna HSM. Initializing the HSM erases all existing data, including any HSM Partition and its data. The HSM Partition then must be recreated with the **partition create** command. Because this is a destructive command, the user is asked to “proceed” unless the **-force** switch is provided at the command line.

> **NOTE** To *change* the authentication type of a Luna USB HSM 7 between Password auth and Multifactor Quorum auth, or the reverse, (with the `-ipwd` option or the `-iped` option of the `hsm init command`) requires a factory reset first ("hsm factoryreset" on page 74).
>
> The factory reset is *not* needed if you are initializing the HSM to the same mode of authentication as is currently configured.

> **NOTE** The "hsm" on page 70 commands appear only when LunaCM's active slot is set to the administrative partition.

Syntax

hsm init -label <label> [**-password** <your_unique_password_for_hsmso>] [**-domain** <domain> | **-defaultdomain**] [**-initwithped** | **-initwithpwd**] [**-applytemplate** <filepath/filename>] [**-auth**] [**-force**]

Argument(s)	Shortcut	Description
-applytemplate <filepath/filename>	**-at**	Apply a policy template located in the specified directory. This feature requires minimum Luna HSM Firmware 7.1.0 and Luna HSM Client 7.1.0.
-auth	**-a**	Log in after the initialization.
-domain <domain>	**-d**	Specifies the key cloning domain string for the HSM Admin partition. It applies to password-authenticated HSMs only. This string is not required for any key cloning or crypto operations on application partitions. The HSM domain is a legacy feature that must be set, but has no practical function on Luna 7 HSMs. **NOTE** This is distinct from the domain on an application partition, which is a critical component required for key cloning, backup/restore, and high availability groups. Refer to Domain Planning for more information.
-defaultdomain	**-def**	This option is deprecated. It applies to password-authenticated HSMs only. It allows you to set a default domain that is compatible with certain legacy HSMs, instead of specifying a unique domain string with **-domain**.
-force	**-f**	Force the action - no prompts. Useful for scripting.

Argument(s)	Shortcut	Description
-initwithped	**-iped**	Initialize a Backup or USB HSM with multifactor quorum authentication. This option is supported only when initializing an HSM that is in a zeroized state. This option is mutually exclusive with the **-initwithpwd** option.
-initwithpwd	**-ipwd**	Initialize a Backup or USB HSM with password authentication. This option is supported only when initializing an HSM that is in a zeroized state. This option is mutually exclusive with the **-initwithped** option.
-label <label>	**-l**	Specifies the label to assign to the HSM. The HSM label created during initialization must be 1-32 characters in length. If you specify a longer label, it will automatically be truncated to 32 characters. The following characters are allowed: `abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789 !@#$%^&*()-_=+[]{}|/;:'",.<>?`~` Spaces are allowed; enclose the label in double quotes if it includes spaces. Including both spaces and quotation marks in a label may cause unexpected labeling behavior.
-password	**-p**	HSM SO password. This option is required for a password authenticated HSM. If you do not provide the password string in the command, you are prompted for it, and the characters that you type are obscured by asterisks (*). This option is ignored for multifactor quorum-authenticated HSMs. Passwords and activation challenge secrets must be 8-255 characters in length. Spaces are allowed; to specify a password with spaces using command-line options, enclose the password in double quotation marks. The space character may not be used as the first character in a password. The following characters are allowed: `!#$%'()*+,-./0123456789:=? @ABCDEFGHIJKLMNOPQRSTUVWXYZ[]^_ abcdefghijklmnopqrstuvwxyz{}~` This character set is enforced when using Luna HSM Client 10.8.0 or newer, and recommended for all previous versions. Previously-set passwords and challenge secrets are unaffected, but the new character set is enforced when these passwords are changed.

Example

Soft init (no factory reset)

```
lunacm:>hsm init -label myLuna

        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.

        Are you sure you wish to continue?

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

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

Command Result : No Error
```

Hard init (with factory reset first)

```
lunacm:>hsm init -label myLuna

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

        Are you sure you wish to continue?

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

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

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

        Option -domain was not specified.  It is required.

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

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

Command Result : No Error
```

HSM init on Luna Backup HSM

```
lunacm:>hsm init -label mybackuphsm -password <your_unique_password_for_backup_hsmso> -domain
<your_secure_domain> -force -auth -initwithpwd

        Initialization was successful and "-auth" was specified.
        Performing an SO login.

Command Result : No Error

lunacm:>hsm si

        HSM Label -> mybackupHSM Manufacturer -> Safenet, Inc.
        HSM Model -> G5Backup
        HSM Serial Number -> 7000013
        HSM Status -> OK
        Token Flags ->
                CKF_RNG
                CKF_LOGIN_REQUIRED
                CKF_RESTORE_KEY_NOT_NEEDED
                CKF_TOKEN_INITIALIZED
        Firmware Version -> 6.10.1
        Rollback Firmware Version -> Not Available

......[output snipped for space]....

        License Count -> 4
                1. 621000028-000 Luna Backup HSM base configuration
                1. 621000048-001 621-000048-001SCU,G5,BU,Partitions100
                2. 621000006-001 Enabled for 15.5 megabytes of object storage
```

```
                2. 621000008-001 Enable remote PED capability

Command Result : No Error
```

hsm migratepedkey

Migrate the PED key contents. Use this command to copy the contents of a Version 1.x Luna PED key to a Version 2.x PED key. This operation requires both a version 1.14 Luna PED (no earlier version will work - contact Thales Customer Support) and a Version 2.x Luna PED. A G4/K5 HSM or token with firmware 4.6.1 must be connected, in order to run this command.

> **NOTE** The "hsm" on page 70 commands appear only when LunaCM's active slot is set to the administrative partition.

Syntax

hsm migratepedkey

Example

```
lunacm:> hsm migratepedkey

                Make sure a Version 1 PED is connected.

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

        Please attend to the PED.

                Make sure a Version 2 PED is connected.

        Please attend to the PED.

Command Result : No Error
```

hsm monitor

Query the HSM for performance monitoring statistics, such as HSM up time, command counts, and utilization. You can display the information or save it to a file.

> **NOTE** The "hsm" on page 70 commands appear only when LunaCM's active slot is set to the administrative partition.

Syntax

hsm monitor [**-slot** <slot number>] [**-interval** <seconds>] [**-rounds** <number>] [**-noheader**] [**-file** <filename>]

Argument(s)	Shortcut	Description
-file<filename>	**-f**	Save the output to the specified file. The output is also displayed to the terminal window.
-interval <seconds>	**-i**	Specifies the polling interval, in seconds. **Default:** 5 **Range:** 5 to 999
-noheader	**-n**	Omit the header and footer from the output. This option is typically used in conjunction with the **-file** parameter.
-rounds <number>	**-r**	Specifies the number of samples to collect during the HSM polling. The default is a single round, which includes a first sample at the time the command is launched, followed by the interval (either the default 5 seconds, or the interval that you specified), followed by a second sample which is compared with the first, to complete the round. The command exits after the specified number of rounds are displayed. **Default**: 1 **Range**: 1 to 65535
-slot	**-s**	The target slot.

Example

Without arguments

```
lunacm:>hsm monitor

------------------|---------------------------------|---------------------------------
                  |       HSM Command Counts        |        HSM Utilization (%)
 HSM Uptime (Secs) |-----------------|---------------|-----------------|---------------
                  | Since HSM Reset | Last   5 Secs | Since HSM Reset | Last   5 Secs
------------------|-----------------|---------------|-----------------|---------------
            97,856 |       1,543,834 |             1 |            1.36 |          0.01
```

```
------------------|-----------------|---------------|-----------------|---------------

    Average HSM Utilization In This Period  :  0.21%

    HSM Last Reset       :  Tue Feb 21 10:53:44 2017
    HSM Has Been Up For  :  1 day(s), 03:10:56


Command Result : 0 (Success)
```

With arguments

```
lunacm:>hsm monitor -interval 6 -rounds 6

------------------|---------------------------------|---------------------------------
                  |       HSM Command Counts        |        HSM Utilization (%)
 HSM Uptime (Secs) |-----------------|---------------|-----------------|---------------
                  | Since HSM Reset | Last   6 Secs | Since HSM Reset | Last   6 Secs
------------------|-----------------|---------------|-----------------|---------------
            98,048 |       1,546,866 |             1 |            1.36 |          0.07
            98,054 |       1,547,119 |           253 |            1.36 |          3.58
            98,060 |       1,547,120 |             1 |            1.36 |          0.01
            98,066 |       1,547,121 |             1 |            1.36 |          0.00
            98,072 |       1,547,374 |           253 |            1.36 |          3.58
            98,078 |       1,547,375 |             1 |            1.36 |          0.00
------------------|-----------------|---------------|-----------------|---------------

    Average HSM Utilization In This Period  :  1.21%

    HSM Last Reset       :  Tue Feb 21 10:53:44 2017
    HSM Has Been Up For  :  1 day(s), 03:14:38

Command Result : No Error
```

hsm resetUtilization

Display and then reset utilization metrics about the HSM.

> **NOTE** This feature requires minimum Luna HSM Firmware 7.3.0 and Luna HSM Client 7.3.0.

> **NOTE** The "hsm" on page 70 commands appear only when LunaCM's active slot is set to the administrative partition.

User Privileges

This command requires that the HSM SO be logged in.

Syntax

hsm resetUtilization

There are no options/arguments for this command.

Example

```
lunacm:>hsm resetUtilization


SN# 1230507392694:myPCIe7hsm
        [            SIGN:REQUESTS        ] = 0
        [          VERIFY:REQUESTS        ] = 0
        [         ENCRYPT:REQUESTS        ] = 0
        [         DECRYPT:REQUESTS        ] = 0
        [  KEY_GENERATION:REQUESTS        ] = 0
        [  KEY_DERIVATION:REQUESTS        ] = 0

SN# 1230507392696:mypar1
        [            SIGN:REQUESTS        ] = 0
        [          VERIFY:REQUESTS        ] = 0
        [         ENCRYPT:REQUESTS        ] = 0
        [         DECRYPT:REQUESTS        ] = 0
        [  KEY_GENERATION:REQUESTS        ] = 134
        [  KEY_DERIVATION:REQUESTS        ] = 1200
-----------------------------------
All Utilization Metrics are reset!

Command Result : 0 (Success)
```

hsm restart

Restart the Luna HSM. Use this command to restart the Luna HSM if it has stopped responding, but your computer is still responsive. This command closes out any login status and open sessions.

If you are a developer, trace what you were doing at the time the problem occurred and try to find another way to program the task that does not put the module in an unresponsive state. If that is not possible, then contact Thales Customer Support with details of the problem and how to reproduce it.

If you are an end-user customer, using an application developed by a supplier other than Thales, contact that company for a resolution of the problem. They know how their application is programmed to accomplish tasks that use the Luna HSM, and they can determine possible workarounds or fixes. If the third-party supplier determines that there is an actual implementation fault with the Luna, they will contact Thales after gathering the relevant information.

> **NOTE** The "hsm" on page 70 commands appear only when LunaCM's active slot is set to the administrative partition.

Syntax

hsm restart [**-force**]

Argument(s)	Shortcut	Description
-force	**-f**	Force the action without prompting for confirmation (useful for scripting).

Example

```
lunacm:> hsm restart

        You are about to restart the HSM. You will lose all volatile data.
        Are you sure you wish to continue?

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


Command Result : No Error
```

hsm rollbackfw

Roll back the HSM firmware to the previously installed version. Only the previously installed version is available for rollback. Rollback allows you to try a new firmware version without permanently committing to the new version.

> **CAUTION!** Firmware rollback is a destructive action; earlier firmware versions may have fewer or older mechanisms and might have security vulnerabilities that a newer version does not. Back up any important materials before running this command.

You must be logged in as HSM SO to use this command. The HSM must be re-initialized after a firmware rollback.

LunaCM performs an automatic restart following a firmware rollback.

> **NOTE** The "hsm" on page 70 commands appear only when LunaCM's active slot is set to the administrative partition.

Syntax

hsm rollbackfw

Example

```
lunacm:>role login -n so

        Please attend to the PED.

Command Result : No Error



lunacm:>hsm rollbackfw
        You are about to rollback the firmware to version 7.0.1.

        All objects will be destroyed.
        The User will be destroyed.
        The HSM will be reset.

        Are you sure you wish to continue?

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

Rolling back firmware. This may take several minutes.

Firmware rollback passed. Resetting HSM

Command Result : No Error
```

 Copyright 2001-2026 Thales Group

hsm showinfo

Display HSM-level information.

> **NOTE** The "hsm" on page 70 commands appear only when LunaCM's active slot is set to the administrative partition.

Syntax

hsm showinfo

Luna PCIe HSM 7 Example

```
lunacm:> hsm showinfo

        Partition Label -> myPCIeHSM
        Partition Manufacturer -> SafeNet
        Partition Model -> Luna K7
        Partition Serial Number -> 67842
        Partition Status -> L3 Device
        HSM Part Number -> 808-000048-002
        HSM Serial Number -> 67842
        Token Flags ->
                CKF_RNG
                CKF_RESTORE_KEY_NOT_NEEDED
                CKF_TOKEN_INITIALIZED
        RPV Initialized -> No
        Slot Id -> 16
        Session State -> CKS_RW_SO_FUNCTIONS
        Role Status ->   SO logged in

        Partition SMK OUIDs:
                SMK-FW4: Not Initialized
                SMK-FW6: Not Initialized
                SMK-FW7-FM: Not Initialized
                SMK-FW7-Rollover: Not Initialized
                SMK-FW7-Primary: 2a0000003a00000102090100

        Extended Token Flags ->
                TOKEN_KCV_CREATED
        Partition OUID -> 00000000000000002090100

        Partition Storage:
                Total Storage Space:  655360
                Used Storage Space:   0
                Free Storage Space:   655360
                Object Count:         0
                Overhead:             16192

        *** The HSM is NOT in FIPS approved operation mode. ***

        FM HW Status -> FM Ready
        Firmware Version -> 7.8.4
        Bootloader Version ->  1.1.5
        Rollback Firmware Version -> 7.4.2
```

 Copyright 2001-2026 Thales Group

```
        System Times:
                HSM  : Wed Nov 27 20:20:21 UTC 2024
                Host : Wed Nov 27 20:20:21 UTC 2024
                Difference: 0 sec

        Environmental:
                Fan 1 Status                            : active
                Fan 2 Status                            : active
                Battery Voltage                         : 3.093 V
                Battery Warning Threshold Voltage       : 2.750 V
                System Temp                             : 64 deg. C
                System Temperature Warning Threshold    : 75 deg. C

        HSM Storage:
                Total Storage Space:  67108864
                Used Storage Space:   7315283
                Free Storage Space:   59793581
                Allowed Partitions:   1
                Number of Partitions: 1

        License Count:
                1. 621000068-000 Test Cert : K7 Base
                2. 621010185-003 Key backup via cloning protocol
                3. 621000138-001 Controlled tamper recovery
                4. 621000134-002 Enable 64 megabytes of object storage
                5. 621000021-002 Maximum performance
                6. 621000135-002 Enable allow decommissioning
                7. 621000154-001 Enable decommission on tamper with policy off


Command Result : No Error
```

NOTE

- The **System Times** field does not appear until the HSM time has been synchronized with the host system using lunacm:> "hsm time sync" on page 101.
- Starting with Luna HSM Firmware 7.7.0, this command reports 671120 bytes of overhead under HSM Storage after initialization.
- If you are migrating a Secure Master Key (SMK) from a Luna 6 HSM to a Luna 7 HSM, in addition to the SMK-FW6, the SMK-FW4 on the Luna 7 HSM is also overwritten by a new one (even if you have *not* initialized an SMK-FW4 on the Luna 6 HSM by a prior migration) and this command reports the presence of an SMK-FW4 on the Luna 7 HSM.

Luna Backup HSM 7 Example

```
lunacm:> hsm showinfo

        Slot Id -> 126
        Partition Label -> myG7pwd
        Partition Serial Number -> 596426
        Partition Model -> Luna G7
        Partition Manufacturer -> SafeNet
        Partition Status -> L3 Device, OK
        Session State -> CKS_RW_PUBLIC_SESSION
```

```
        Role Status ->   none logged in
        RPV Initialized -> No

        Partition Cloning Version -> 1
        Partition FM Status -> FM Disabled

        Partition SMK OUIDs:
                SMK-FW4: Not Initialized
                SMK-FW6: Not Initialized
                SMK-FW7-FM: Not Initialized
                SMK-FW7-Rollover: Not Initialized
                SMK-FW7-Primary: Not Initialized


        Partition Storage:
                Total Storage Space:  655360
                Used Storage Space:   0
                Free Storage Space:   655360
                Object Count:         0
                Overhead:             24224

        Firmware Version -> 7.7.1
        Bootloader Version ->  1.3.0
        Rollback Firmware Version -> 7.3.2
        HSM Part Number -> 808-000064-005

        HSM Storage:
                Total Storage Space:  33816576
                Used Storage Space:   761724
                Free Storage Space:   33054852
                Allowed Partitions:   100
                Number of Partitions: 3

        Environmental:
                System Temperature :  46 deg. C

        License Count:
                1. 621000121-000 G7 BU 32M Base CUF December 7 2018

        *** The HSM is NOT in FIPS 140-2 approved operation mode. ***

Command Result : No Error
```

NOTE

- Starting with Luna Backup HSM 7 Firmware 7.7.1, this command reports 679584 bytes of overhead under HSM Storage after initialization.
- If you are migrating a Secure Master Key (SMK) from a Luna 6 HSM to a Luna 7 HSM, in addition to the SMK-FW6, the SMK-FW4 on the Luna 7 HSM is also overwritten by a new one (even if you have *not* initialized an SMK-FW4 on the Luna 6 HSM by a prior migration) and this command reports the presence of an SMK-FW4 on the Luna 7 HSM.

 Copyright 2001-2026 Thales Group

hsm showmechanism

Displays a list of the cryptographic mechanisms supported on the HSM.

> **NOTE** The "hsm" on page 70 commands appear only when LunaCM's active slot is set to the administrative partition.

Syntax

hsm showmechanism [**-m** <number>]

Argument(s)	Short	Description
.	.	With no arguments/options, lists all available mechanisms
-m <number>	**-m**	Show expanded information for the indicated mechanism (optional). Include just the number, without the "0x" prefix.

Example

```
lunacm:> hsm showmechanism


Mechanisms Supported:
        0x00000000 - CKM_RSA_PKCS_KEY_PAIR_GEN
        0x00000001 - CKM_RSA_PKCS
        0x00000003 - CKM_RSA_X_509
        0x00000006 - CKM_SHA1_RSA_PKCS
        0x00000009 - CKM_RSA_PKCS_OAEP
        0x0000000a - CKM_RSA_X9_31_KEY_PAIR_GEN
        0x0000000c - CKM_SHA1_RSA_X9_31
        0x0000000d - CKM_RSA_PKCS_PSS
        0x0000000e - CKM_SHA1_RSA_PKCS_PSS
        0x00000010 - CKM_DSA_KEY_PAIR_GEN
        0x00000011 - CKM_DSA
        0x00000012 - CKM_DSA_SHA1


....(clip)...


        0x80000140 - CKM_DSA_SHA224
        0x80000141 - CKM_DSA_SHA256
        0x80000a02 - CKM_NIST_PRF_KDF
        0x80000a03 - CKM_PRF_KDF

Command Result : No Error



lunacm:> hsm showmechanism -m 00000003

(0x3 - 3) CKM_RSA_X_509
```

```
         Min Key Size 256
         Max Key Size 8192
         Flags 0x301
Command Result : No Error
```

hsm showpolicies

Displays the HSM-level capability and policy settings for the HSM. Include the **-exporttemplate** option to export the current state of all HSM policies to a policy template. Only policies that the HSM SO can change (the corresponding capability is not set to **0**) are included in the output. For a complete list of HSM capabilities and policies, refer to HSM Capabilities and Policies.

> **NOTE** Some mechanisms (such as KCDSA) are not enabled unless you have purchased and installed the required Secure Capability Update package. If you require a particular mechanism, and do not see it listed when you generate a mechanism list, contact Thales Customer Support.
>
> The "hsm" on page 70 commands appear only when LunaCM's active slot is set to the administrative partition.

Syntax

hsm showpolicies [**-exporttemplate** <filepath/filename>]

Argument(s)	Short	Description
-exporttemplate <filepath/filename>	**-et**	Export the current state of all HSM policies to a policy template in the specified location. This feature requires minimum Luna HSM Firmware 7.1.0 and Luna HSM Client 7.1.0.

Examples

```
lunacm:> hsm showpolicies
        HSM Capabilities
                 0: Enable PIN-based authentication : 1
                 1: Enable PED-based authentication : 0
                 2: Performance level : 15
                 4: Enable domestic mechanisms & key sizes : 1
                 6: Enable masking : 0
                 7: Enable cloning : 1
                 9: Enable full (non-backup) functionality : 1
                12: Enable non-FIPS algorithms : 1
                15: Enable SO reset of partition PIN : 1
                16: Enable network replication : 1
                17: Enable Korean Algorithms : 0
                18: FIPS evaluated : 0
                19: Manufacturing Token : 0
                21: Enable forcing user PIN change : 1
                22: Enable offboard storage : 1
                23: Enable partition groups : 0
                25: Enable remote PED usage : 0
                27: HSM non-volatile storage space : 33554432
                30: Enable unmasking : 1
                33: Maximum number of partitions : 100
                35: Enable Single Domain : 0
                36: Enable Unified PED Key : 0
                37: Enable MofN : 0
                38: Enable small form factor backup/restore : 0
```

```
                39: Enable Secure Trusted Channel : 1
                40: Enable decommission on tamper : 1
                42: Enable partition re-initialize : 0
                43: Enable low level math acceleration : 1
                46: Allow Disabling Decommission : 1
                47: Enable Tunnel Slot : 0
                48: Enable Controlled Tamper Recovery : 1
                49: Enable Partition Utilization Metrics : 1
                50: Enable Functionality Modules : 1
                51: Enable SMFS Auto Activation : 1
                52: Enable Disabling FM Privilege Level : 1
                53: Enable FM Cipher Engine Key Encryption : 1
                56: Enable User Defined ECC Curves : 1


        HSM Policies
                 0: PIN-based authentication : 1
                 7: Allow cloning : 1
                12: Allow non-FIPS algorithms : 1
                15: SO can reset partition PIN : 0
                16: Allow network replication : 1
                21: Force user PIN change after set/reset : 1
                22: Allow offboard storage : 1
                30: Allow unmasking : 1
                33: Current maximum number of partitions : 100
                39: Allow Secure Trusted Channel : 0
                40: Decommission on tamper : 0
                43: Allow low level math acceleration : 1
                46: Disable Decommission : 0
                48: Do Controlled Tamper Recovery : 1
                49: Allow Partition Utilization Metrics : 1
                50: Allow Functionality Modules : 1
                51: Allow SMFS Auto Activation : 0
                52: Disable FM Privilege Level : 0
                53: Do FM Cipher Engine Key Encryption : 0
                56: Allow User Defined ECC Curves : 1


Command Result : No Error
```

Example with Luna PCIe HSM or Network HSM firmware >= 7.7.0 and Client >= 10.3.0

```
lunacm (64-bit) v10.3.0. Copyright (c) 2020 SafeNet. All rights reserved.

lunacm:>hsm sp
        HSM Capabilities
                 0: Enable PIN-based authentication : 1
                 1: Enable PED-based authentication : 0
                 2: Performance level : 15
                 4: Enable domestic mechanisms & key sizes : 1
                 6: Enable masking : 1
                 7: Enable cloning : 1
                 9: Enable full (non-backup) functionality : 1
                12: Enable non-FIPS algorithms : 1
                15: Enable SO reset of partition PIN : 1
                16: Enable network replication : 1
```

```
            17: Enable Korean Algorithms : 0
            19: Manufacturing Token : 0
            21: Enable forcing user PIN change : 1
            22: Enable offboard storage : 1
            23: Enable partition groups : 0
            25: Enable remote PED usage : 0
            27: HSM non-volatile storage space : 67108864
            30: Enable unmasking : 1
            33: Maximum number of partitions : 20
            35: Enable Single Domain : 0
            36: Enable Unified PED Key : 0
            37: Enable MofN : 0
            38: Enable small form factor backup/restore : 0
            40: Enable decommission on tamper : 1
            42: Enable partition re-initialize : 0
            43: Enable low level math acceleration : 1
            46: Allow Disabling Decommission : 1
            48: Enable Controlled Tamper Recovery : 1
            49: Enable Partition Utilization Metrics : 1
            50: Enable Functionality Modules : 0
            51: Enable SMFS Auto Activation : 0
            52: Allow Restricting FM Privilege Level : 0
            53: Allow encrypting of keys from FM to HSM : 0

      HSM Policies
             0: PIN-based authentication : 1
             6: Allow masking : 1
             7: Allow cloning : 1
            12: Allow non-FIPS algorithms : 1
            15: SO can reset partition PIN : 0
            16: Allow network replication : 1
            21: Force user PIN change after set/reset : 1
            22: Allow offboard storage : 1
            30: Allow unmasking : 1
            33: Current maximum number of partitions : 20
            40: Decommission on tamper : 0
            43: Allow low level math acceleration : 1
            46: Disable Decommission : 0
            48: Do Controlled Tamper Recovery : 1
            49: Allow Partition Utilization Metrics : 1


Command Result : No Error
```

hsm showUtilization

Display the partition utilization metrics.

> **NOTE** This feature requires minimum Luna HSM Firmware 7.3.0 and Luna HSM Client 7.3.0.

> **NOTE** The "hsm" on page 70 commands appear only when LunaCM's active slot is set to the administrative partition.

User Privileges

This command requires that the HSM SO be logged in.

Syntax

hsm showUtilization [**-serial** <partition_serial_number>]

Argument(s)	Shortcut	Description
-serial <partition_serial_number>	**-s**	Optionally, show only the metrics for the partition with this serial number. Otherwise, show metrics for the whole HSM.

Example

With no arguments (output to terminal):

```
lunacm:>hsm showUtilization


SN# 1230507392694:myPCIe7hsm
        [            SIGN:REQUESTS        ] = 0
        [          VERIFY:REQUESTS        ] = 0
        [         ENCRYPT:REQUESTS        ] = 0
        [         DECRYPT:REQUESTS        ] = 0
        [  KEY_GENERATION:REQUESTS        ] = 0
        [  KEY_DERIVATION:REQUESTS        ] = 0

SN# 1230507392696:mypar1
        [            SIGN:REQUESTS        ] = 0
        [          VERIFY:REQUESTS        ] = 0
        [         ENCRYPT:REQUESTS        ] = 0
        [         DECRYPT:REQUESTS        ] = 0
        [  KEY_GENERATION:REQUESTS        ] = 134
        [  KEY_DERIVATION:REQUESTS        ] = 1200

Command Result : 0 (Success)
```

With partition serial number (output to terminal):

```
lunacm:>hsm showUtilization -serial 1230507392696

SN# 1230507392696:mypar1
        [            SIGN:REQUESTS        ] = 0
        [          VERIFY:REQUESTS        ] = 0
        [         ENCRYPT:REQUESTS        ] = 0
        [         DECRYPT:REQUESTS        ] = 0
        [  KEY_GENERATION:REQUESTS        ] = 134
        [  KEY_DERIVATION:REQUESTS        ] = 1200

Command Result : 0 (Success)
```

hsm smkclone

Clone the Scalable Key Storage Masking Key (SMK) from the current slot to the target slot.

Always back up any SMK that you have created (with partition archive backup to an SKS Backup HSM), before performing an action that would overwrite that SMK, like hsm smkClone or like partition archive restore from an SKS partition on an SKS Backup HSM. Failure to do so risks permanently losing any objects that are encrypted with that original SMK.

> **CAUTION!** This command overwrites the SMK in the target partition with the SMK from the source. If you have exported any objects using a particular SMK, that SMK must be backed up to a Backup HSM before you overwrite it with smkclone, or those exported objects become unusable and can never be recovered.

An SMK secret that is cloned from a source V1 HSM partition to a target V1 partition overwrites any pre-existing V1 SMK on the target partition. SMK secrets cloned from V0 partitions do not overwrite V1 SMK secrets, but are stored separately.

On a Luna PCIe HSM 7 or Luna USB HSM 7 the Admin partition defaults to V1, so it has an SMK.

> **NOTE** The "hsm" on page 70 commands appear only when LunaCM's active slot is set to the administrative partition.

Syntax

hsm smkClone -slot <slot number> **[-force] -password** <password>

Argument	Shortcut	Description
-force	**-f**	Force the action without prompting for confirmation (useful when scripting commands).
-password <password>	**-p**	Password of the target slot.
-slot <number>	**-sl**	Target slot to which the source SMK is to be cloned (overwriting any SMK that might already be in the target slot).

Example

```
lunacm (64-bit) v10.7.1-62. Copyright (c) 2024 Thales Group. All rights reserved.


        Available HSMs:

        Slot Id ->              3
        Label ->                MyPar
        Serial Number ->        1292468271971
        Model ->                Luna K7
        Firmware Version ->     7.8.4
        Bootloader Version ->   1.1.5
```

```
        Configuration ->        Luna User Partition With SO (PW) Signing With Cloning Mode
        Slot Description ->     User Token Slot
        FM HW Status ->         FM Ready

        Slot Id ->              103
        Label ->                card1
        Serial Number ->        555111
        Model ->                Luna K7
        Firmware Version ->     7.8.4
        Bootloader Version ->   1.1.5
        Configuration ->        Luna HSM Admin Partition (PW) Signing With Cloning Mode
        Slot Description ->     Admin Token Slot
        FM HW Status ->         FM Ready
        HSM Configuration ->    Luna HSM Admin Partition (PW)
        HSM Status ->           L3 Device
        HSM Certificates ->


        Slot Id ->              104
        Label ->                G7Par
        Serial Number ->        1434611353268
        Model ->                Luna G7
        Firmware Version ->     7.7.3
        Bootloader Version ->   1.6.0
        Configuration ->        Luna User Partition With SO (PW) Key Export With Cloning Mode
        Slot Description ->     User Token Slot


        Slot Id ->              105
        Label ->                G7HSM
        Serial Number ->        616161
        Model ->                Luna G7
        Firmware Version ->     7.7.3
        Bootloader Version ->   1.6.0
        Configuration ->        Luna HSM Admin Partition (PW) Key Export With Cloning Mode
        Slot Description ->     Admin Token Slot
        HSM Status ->           L3 Device, OK
        HSM Certificates ->


        Current Slot Id: 3


lunacm:>s s s 103

        Current Slot Id:  103     (Luna Admin Slot 7.8.4 (PW) Signing With Cloning Mode)

Command Result : No Error


lunacm:>role login -n so -p so-password

Command Result : No Error


lunacm:>hsm smkclone -slot 105 -password so-password

        Logging in to target slot 105
```

```
        Cloning the SMK.

                The SMK was cloned successfully.

Command Result : No Error


lunacm:>
```

hsm smkrollover

This is a two-part command that creates a new secret (**S**KS **m**aster **k**ey or SMK) to encrypt objects for extraction in encrypted blobs. It is issued twice to perform the full rollover task:

- once with the **-start** option, and then
- a second time, with the **-end** option, to finish the sequence.

This command, with the **-start** option, moves the current primary SMK to the Rollover location, and generates a new Primary SMK.

- If you just wanted to generate a fresh SMK, and no external SKS blobs are encrypted with the previous SMK, then you can issue the command again with the **-end** option, and the task is finished.
- If you are performing a rollover of an active SMK that was used to encrypt extracted keys and objects (as you might do, in compliance with your organization's key-rotation policy), then immediately after **hsm smkrollover -start**, you must
  - *insert* sequentially any SKS blobs that are encrypted by the old SMK, and
  - *re-extract* each key or object encrypted by the new SMK, forming new encrypted blobs (**b**inary **l**arge **ob**jects).

  The HSM recognizes which SMK was used to encrypt a blob, and if it is the rollover SMK (or if it is an SMK from a previous HSM generation, currently in the appropriate 'legacy' SMK location), it uses that prior SMK for the insertion. [Re-]extraction always uses the Primary SMK, which would be the new one.

When all desired keys and objects have been re-extracted into newly encrypted blobs, the **hsm smkrollover -end** command finishes the process.

> **CAUTION!** The **hsm smkrollover -end** command deletes the SMK from the Rollover space of the current partition, leaving only the new SMK in the Primary space. If you have exported any SKS blobs using the old SMK, that you have not re-extracted with the new Primary SMK, then those blobs can never be inserted again, unless you have retained a backup of the old SMK.

> **NOTE** The "hsm" on page 70 commands appear only when LunaCM's active slot is set to the administrative partition.

Syntax

hsm smkrollover {[**-start**] | [**-end**]} [**-force**]

Argument	Shortcut	Description
-end	**-e**	End SMK rollover and delete the Rollover SMK.
-force	**-f**	Force the action without prompting for confirmation (useful when scripting commands).
-start	**-s**	Start SMK rollover, moving the pre-existing SMK to the Rollover space, and creating a new SMK in the Primary SMK space.

Example

```
lunacm:> hsm smkrollover -start

        You are about to rollover the SMK.
        Are you sure you wish to continue?

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

Command Result : No Error
```

Between issuing the **-start** and **-end** commands, insert and re-extract any SKS blobs that were encrypted/extracted with the old SMK, so that they are now encrypted with the new (Primary) SMK and stored externally to the cryptographic module.

```
lunacm:> hsm smkrollover -end

        You are about to rollover the SMK.
        Are you sure you wish to continue?

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

Command Result : No Error
```

hsm tamperclear

Unlock the HSM following a tamper event.

The type of tamper event is indicated by the **HSM Status** line in the output of the command "slot list" on page 228. Use the command "hsm tampershow" on the next page to display detailed information for the tamper.

> **NOTE** The "hsm" on page 70 commands appear only when LunaCM's active slot is set to the administrative partition.

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

Syntax

hsm tamperclear

Example

```
lunacm:>hsm tamperclear

Command Result : No Error
```

hsm tampershow

Display the current tamper state for the HSM card. If the card has been tampered (tamper event, card removal, opened chassis, etc.), detailed information regarding the tamper is displayed.

> **NOTE** The "hsm" on page 70 commands appear only when LunaCM's active slot is set to the administrative partition.

Syntax

hsm tampershow

Example

```
lunacm:>hsm tampershow
        No active tampers.

Command Result : No Error
```

hsm time

Display the current HSM time, and synchronize the HSM time to the host time.

> **NOTE** The "hsm" on page 70 commands appear only when LunaCM's active slot is set to the administrative partition.
>
> The "hsm time" above commands are available for HSMs with Luna HSM Firmware 7.8.0 or newer and Luna HSM Client 10.3.0 or newer.

Syntax

hsm time

get
sync

Argument(s)	Shortcut	Description
get	**g**	Display the current HSM time. See "hsm time get" below.
sync	**s**	Synchronize the HSM time with the host time. See "hsm time sync" on the next page.

hsm time get

Display the current HSM time, the current host time, and the difference between the two, in a block called **System Times**.

Once "hsm time sync" below has been executed, the **System Times** information also appears in the command output for:

- lunacm:> "hsm showinfo" on page 86
- lunacm:> "partition showinfo" on page 177

> **NOTE** The "hsm" on page 70 commands appear only when LunaCM's active slot is set to the administrative partition. The "hsm time" on the previous page commands are available for HSMs with Luna HSM Firmware 7.8.0 or newer and Luna HSM Client 10.3.0 or newer.
>
> This command returns an error (`LUNA_RET_TIME_NOT_INITIALIZED`) until lunacm:> "hsm time sync" below has been executed for the first time.

The HSM SO is not required to be logged in, to run this command.

Syntax

hsm time get

Example

```
lunacm:>hsm time get

System Times:
HSM  :   Mon May 16 15:26:12 UTC 2022
Host :   Mon May 16 15:22:53 UTC 2022
Difference:  199 sec

Command Result : 0 (Success)
```

hsm time sync

Synchronize the current HSM time with the current host time.

Automatic HSM time synchronization depends on the HSM and Host clocks being no more than 3 seconds out-of-sync. If the difference is greater, you can use this command to 'manually' synchronize the two, after which daily automatic synchronization can carry on.

> **NOTE** The "hsm" on page 70 commands appear only when LunaCM's active slot is set to the administrative partition. The "hsm time" on the previous page commands are available for HSMs with Luna HSM Firmware 7.8.0 or newer and Luna HSM Client 10.3.0 or newer.
>
> Once "hsm time sync" above has been executed, the **System Times** information also appears in the command output for:
>
> - lunacm:> "hsm showinfo" on page 86
> - lunacm:> "partition showinfo" on page 177

The HSM SO must be logged in, to use this command.

Syntax

hsm time sync

Example

```
lunacm:> hsm time sync

HSM time was synchronized to Host

Command Result : No Error
```

hsm updatecap

Update the capabilities of the Luna HSM. When new features and capabilities are made available from Thales, this command allows you to apply them to your Luna HSM.

> **NOTE** The "hsm" on page 70 commands appear only when LunaCM's active slot is set to the administrative partition.

On Luna Network HSM, these upgrades are obtained via the Thales Licensing Portal (GLP).

Syntax

hsm updatecap -cuf <filename> **-authcode** <filename> [**-force**]

Argument(s)	Shortcut	Description
-cuf <filename>	**-u**	Specifies the capability update file that you want to apply.
-authcode <filename>	**-a**	Specifies the file containing the authorization code for the capability update.
-force	**-f**	Force the change without further prompting.

Example

```
lunacm:> hsm updatecap -cuf 621-000100-001_RC4_G5PPSO.CUF -authcode G5PPSO-RC6.txt

 You are about to apply a destructive update.
 All contents of the HSM will be destroyed.

 Are you sure you wish to continue?

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

Command Result : No Error
```

> **NOTE** The filenames shown above are only examples for the purpose of demonstration.

hsm updatefw

Update the firmware on the Luna HSM. LunaCM performs an automatic restart following a firmware update.

> **NOTE** The "hsm" on page 70 commands appear only when LunaCM's active slot is set to the administrative partition.

Syntax

hsm updatefw -fuf <filename> [**-authcode** <filename>] [**-show**] [**-force**]

Argument(s)	Shortcut	Description
-authcode <filename>	**-a**	Specifies the file containing the authorization code for the firmware update.
-fuf <filename>	**-u**	Specifies the firmware update file.
-force	**-f**	Force the action without prompting.
-show	**-s**	Show the firmware update file contents.

Example

```
lunacm:>hsm updatefw -fuf fwupdateK7_testCert_7.0.1_RC327.fuf -authcode fwupdateK7_testCert_
7.0.1_RC327.fuf.txt
        You are about to update the firmware.
        The HSM will be reset.
        Are you sure you wish to continue?

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

        Updating firmware. This may take several minutes.

        Firmware update passed. Resetting HSM

Command Result : No Error
```

hsm zeroize

Puts the HSM in a zeroized state. All partitions and cryptographic contents of the HSM will be destroyed. Because this is a destructive command, the user is prompted to "proceed" unless the **-force** option is included. This action does not affect HSM policies, remote PED settings, or Auditor settings.

> **NOTE** The "hsm" on page 70 commands appear only when LunaCM's active slot is set to the administrative partition.

Syntax

hsm zeroize [**-force**]

Argument(s)	Shortcut	Description
-force	**-f**	Force the action without prompts. If this option is included in the list, the HSM will be zeroized without prompting the user for a confirmation of this destructive command.

Example

```
lunacm:>hsm zeroize

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

        HSM policies, remote PED vector and Auditor left unchanged.

        Are you sure you wish to continue?

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

Command Result : No Error
```

 Copyright 2001-2026 Thales Group

partition

Access the partition-level commands. Different commands are available depending on whether the current slot is the HSM administrative partition or a user partition. As well, some commands, or some command options, might be available or usable only:

- when you are using the most recent Luna HSM Client version (with lunacm that supports more recently developed commands, or additions to older commands)
  and
- when the current slot is on an HSM with recent firmware that supports the particular command.

For the Luna Network HSM 7, 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 Luna Network HSM 7 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.

Syntax

This version of the partition command set includes an **init** command for the application partition. These are the commands you see if the current-slot application partition was created using the **-slot** option.

partition

addsize
archive
changelabel
changepolicy
changepw
cipherdisable
cipherenable
ciphershow
clear
clone
contents
create
delete
domainadd
domainchangelabel
domaindelete
domainlist
init
login
logout
logoutother
resize
restoresim3
setlegacydomain
showinfo
showmechanism

 Copyright 2001-2026 Thales Group

showpolicies
smkclone
smkrollover

Argument(s)	Shortcut	Description
addsize	**as**	Increase the size of a partition by a specific number of bytes. See "partition addsize" on page 109.
archive	**ar**	Partition archive management commands. See "partition archive" on page 111.
changelabel	**changel**	Change the specified partition's label. See "partition changelabel" on page 126.
changepolicy	**changepo**	Change the Partition Policy value. See "partition changepolicy" on page 128
changepw	**changepw**	Change the Partition Password for all members of an HA group. See "partition changepw" on page 132
cipherdisable	**cid**	Disable the indicated cipher suite for cloning. See "partition cipherdisable" on page 134
cipherenable	**cie**	Enable the indicated cipher suite for cloning. See "partition cipherenable" on page 137
ciphershow	**cish**	Show available cipher suites for cloning, and their status. See "partition ciphershow" on page 142
clear	**clr**	Delete all of the user's token objects. See "partition clear" on page 145.
clone	**clo**	Clone user objects. See "partition clone" on page 146.
contents	**con**	Show the contents of the user partition. See "partition contents" on page 148.
create	**crp**	Create a user partition. See "partition create" on page 149.
delete	**del**	Delete a user partition. See "partition delete" on page 152.
domainadd	**da**	Add a cloning domain to the partition. See "partition domainadd" on page 154.
domainchangelabel	**dc**	Change a cloning domain label. See "partition domainchangelabel" on page 159.

Argument(s)	Shortcut	Description
domaindelete	**de**	Delete a cloning domain from the partition. See "partition domaindelete" on page 163.
domainlist	**dl**	List a cloning domains in the partition. See "partition domainlist" on page 165.
init	**in**	Initialize an application partition. See "partition init" on page 167.
login	**logi**	Log in to an HA group using the common Crypto Officer password or challenge secret. See "partition login" on page 171.
logout	**logo**	Log out of an HA group. See "partition logout" on page 172.
logoutother	**lo**	Log a user out of all sessions other than the current one. See "partition logoutother" on page 172.
resize	**res**	Resize a user partition. See "partition resize" on page 173.
restoresim3file	**rsim3f**	Restore user objects (using SIM3). See "partition restoresim3file" on page 175.
setlegacydomain	**sld**	Set the legacy domain. "partition setlegacydomain" on page 176.
showinfo	**si**	Display partition information. See "partition showinfo" on page 177.
showmechanism	**showm**	Show all available mechanisms. See "partition showmechanism" on page 181.
showpolicies	**sp**	Get partition policy information. See "partition showpolicies" on page 183.
smkclone	**smkc**	Clone the SKS Master Key (SMK). See "partition smkclone" on page 191.
smkrollover	**smkr**	Moves the current primary SKS Master Key (SMK) to the SMK Rollover location and generates a new primary SMK. See "partition smkrollover" on page 194.

partition addsize

Increase the size of a backup partition by a specific number of bytes.

This command is applicable to Luna Backup HSM partitions only, and appears in LunaCM only when a Backup HSM is connected. You must be logged in to the Backup HSM as HSM SO to use this command.

Syntax

partition addsize -slot <number> **-size** <bytes> {**-partition** <name> | **-all**} [**-force**]

Argument(s)	Shortcut	Description
-all	**-a**	Increase the size of all partitions on the slot by a specified number of bytes.
-force	**-f**	Force the action without prompting for confirmation.
-partition <name>	**-par**	The name of the affected partition.
-size <bytes>	**-si**	The storage space (in bytes) to be added to the partition.
-slot <number>	**-sl**	The slot where the partition is located.

Example

```
lunacm:>partition archive list -slot 2

        HSM Storage Information for slot 2:

          Total HSM Storage Space: 16252928
          Used HSM Storage Space:  606468
          Free HSM Storage Space:  15646460
          Allowed Partitions:      20
          Number Of Partitions:    3

        Partition list for slot 2

          Number of partition: 2

          Name: bk1
          Total Storage Size:        200000
          Used Storage Size:         0
          Free Storage Size:         200000
          Number Of Objects:         0


          Name: bk2
          Total Storage Size:        200000
          Used Storage Size:         0
          Free Storage Size:         200000
          Number Of Objects:         0

Command Result : No Error
```

```
lunacm:>hsm login

        Please attend to the PED.


Command Result : No Error


lunacm:>partition addsize -slot 2 -size 999 -partition bk2

        This command will increase the user partition's storage size.
        Are you sure you wish to continue?

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

Command Result : No Error



lunacm:>partition archive list -slot 2

        HSM Storage Information for slot 2:

          Total HSM Storage Space: 16252928
          Used HSM Storage Space:  607467
          Free HSM Storage Space:  15645461
          Allowed Partitions:      20
          Number Of Partitions:    3

        Partition list for slot 2

          Number of partition: 2

          Name: bk1
          Total Storage Size:        200000
          Used Storage Size:         0
          Free Storage Size:         200000
          Number Of Objects:         0

          Name: bk2
          Total Storage Size:        200999
          Used Storage Size:         0
          Free Storage Size:         200999
          Number Of Objects:         0

Command Result : No Error
```

partition archive

Access the partition archive commands.

An archive (backup) device can be one of the following:

- An HSM in another slot in the current system
- A backup HSM connected to a remote workstation
- A USB-attached HSM connected directly to a Luna PCIe HSM 7

Device configuration

In each scenario, the HSM that is being used as a backup device should be configured as a backup device; the HSM capability **Enable full (non-backup) functionality (9)** is disabled.

If the HSM is not configured as a backup device then you will not be able to create new backup partitions on the HSM. You will only be able to backup/restore to/from any existing partitions.

> **NOTE** If the domains of your source and target HSMs do not match or the policy settings do not permit backup, the partition archive backup command fails. No objects are cloned to the target HSM but the command creates an empty backup partition. In this circumstance, you must manually delete the empty backup partition.

Specifying the backup device

To specify a backup device in another slot in the current system, use the **-s** option and give the actual slot number (for example, **-s 4**).

To specify a backup device in a remote work station, use the **-s** option and include the keyword **remote** (for example, **-s remote**). When specifying a remote device, you must also provide a hostname and port number using the **-hostname** and **-port** options. (The **-hostname** option also accepts an IP address.)

To specify a USB attached backup device directly connected to the HSM in the current slot, use the **-s** option and include the keyword **direct** (for example, **-s direct**). If you know the slot number that contains the USB attached HSM, you can specify that slot number explicitly (for example, **-s 5**).

Password-authenticated Luna Backup HSM

When using a password-authenticated Luna Backup HSM, the SO password, partition password, and domain values cannot be specified with the command. This is because the network connection is not secured and the passwords should not be transferred across the network in the clear. If these values are required, they are prompted on the remote workstation console.

Device initialization

Before a backup HSM can be used, it must be initialized. To initialize a backup HSM, you must set your backup HSM as your current slot and use the **hsm init** command. If your backup HSM is in a remote workstation, then you must initialize it locally at that workstation, or remotely using remote PED if it is supported.

Appending objects to an existing backup partition

When backing up, the **append** option can be used to add objects to the existing backup partition. If the specified partition does not exist, then this option cannot be used. If the partition does exist and this option is not used, the existing partition is deleted and a new partition is created. If the **append** option is not used and the specified partition does not exist, it is created. If the partition must be created or resized, the SO password for the backup HSM is required.

Remote backups

To perform remote backup (**-s remote**), a remote backup server must be running on the remote work station. To start a remote backup server, run LunaCM on the remote workstation, select the slot you wish to use as a remote backup HSM, and use the command **remotebackup start**. The remote backup server will accept commands and execute them against the current slot.

Syntax

partition archive

backup
contents
delete
list
restore

Argument(s)	Shortcut	Description
backup	**b**	Back up objects from the current slot to a backup partition in a backup device in a specified slot. See "partition archive backup" on the next page.
contents	**c**	List the contents of a backup partition in a backup device in a specified slot. See "partition archive contents" on page 118.
delete	**d**	Delete the specified backup partition in a backup device in a specified slot. See "partition archive delete" on page 120.
list	**l**	List the backup partitions on a backup device in a specified slot. See "partition archive list" on page 121.
restore	**r**	Restore objects from the specified backup partition in a backup device in a specified slot to the current user partition. See "partition archive restore" on page 123.

partition archive backup

Backup partition objects. Use this command to backup objects from the current user partition to a partition on a backup device. You must be logged in as the Crypto Officer to backup the partition.

> **NOTE** If the domains of your source and target HSMs do not match or the policy settings do not permit backup, the **partition archive backup** command fails. No objects are cloned to the target HSM but the command creates an empty backup partition. In this circumstance, you must manually delete the empty backup partition.

When you call for a cloning operation (such as backup or restore), the source HSM transfers each object one at a time, encrypted with the source domain. If the source is a V0 or pre-7.7.0 partition, the target HSM then decrypts and verifies each received blob. If the source is a V1 partition, the blob remains encrypted on the Backup HSM. See Behavior of Pre-Firmware 7.7, V0, and V1 Partitions for more information.

If the verification is successful, the object is stored at its destination – the domains are a match. If the verification fails, then the blob is discarded and the target HSM reports the failure. If the domain string or the domain PED key used to create the target partition did not match the domain of the source HSM partition, the operation fails with the error CKR_CERTIFICATE_INVALID. If the source is a partition using firmware older than Luna HSM Firmware 7.7.0, the source HSM moves to the next item in the object list and attempts to clone again, until the end of the list is reached. If the source is a V0 or V1 partition, the backup operation ends when the first object fails.

> **NOTE** To perform backup operations on Luna HSM Firmware 7.7.0 or newer (V0 or V1 partitions) you require at minimum:
>
> > Luna Backup HSM 7 Firmware 7.7.1
>
> > Luna Backup HSM G5 Firmware 6.28.0
>
> You can use a Luna Backup HSM with older firmware to restore objects to a V0 or V1 partition, but this is supported for purposes of getting your objects from the older partitions onto the newer V0 or V1 partitions only. V0 and V1 partitions are considered more secure than partitions at earlier firmware versions - any attempt to restore from a higher-security status to lower-security status fails gracefully.

Backup partition sizing

When you run the **partition archive backup** command, it compares the size of the source partition with the remaining free space on the backup HSM to ensure that there is enough space on the backup HSM to accommodate the backup. If there is not enough space, the backup operation is canceled, and an appropriate error message is displayed.

Luna Backup HSM 7 partition re-sizing

On Luna Backup HSM 7s, when you create a new backup, all of the available free space on the backup HSM is assigned to the new backup partition. Once all of the objects have been successfully cloned to the new backup partition, the new backup partition is automatically re-sized to the minimum size required to accommodate the backup objects, and any free space is reallocated.

> **NOTE** If this re-sizing operation should fail, all the free space on the Backup HSM will be occupied and no new backups can be made. In this unlikely event, you must delete the backup using lunacm:> **"partition archive delete" on page 120** and re-attempt the backup operation.

If the backup partition becomes full before all of the objects have been successfully cloned, the backup is canceled and an error message is displayed. The new backup partition and all of the objects cloned to that point are deleted from the backup HSM and it reverts to the state it was in prior to the backup operation. In this case you will need to free up some space on the backup HSM or use another backup HSM with more available free space.

Syntax

partition archive backup -slot <backup_slot> [**-partition** <backup_partition>] **-password** <your_unique_password_for_backup-partition> [**-sopassword** <your_unique_password_for_so>] [**-domain** <domain> | **-defaultdomain**] [**-append**] [**-replace**] [**-objects** <object_handles>] [**-smkonly**] [**-debug**] [**-force**]

Argument(s)	Shortcut	Description
-append	**-a**	Append new objects to the existing partition. Do not overwrite existing objects that have the same OUID, even if their attributes differ (see **-replace**). **NOTE** When backing up objects from an HSM with firmware older than 7.7.0 to a Luna Backup HSM 7 with firmware 7.7.1 or newer, objects with the same OUID as those already stored on the backup may be identified as having a different fingerprint: `Target Object handle 3596 has same OUID as Source Object handle 358 (different finger print).` Use both **-append** and **-replace** to overwrite these backup objects with the versions on the source partition.
-debug	**-deb**	Turn on additional error information (optional).
-defaultdomain	**-def**	Default domain for the specified partition.
-domain <domain>	**-do**	Domain for the specified partition.
-force	**-f**	Force action with no prompting.

Argument(s)	Shortcut	Description
-objects <object_handles>	**-o**	Select specific individual objects to back up by specifying their object handles using any of the following methods: > a single object handle > **0** or **all**, to indicate that all objects are to be extracted > a list of handles, separated by commas. For example: **-objects 3,4,6** This option requires Luna HSM Client 10.3.0 or newer, and gives the capability to backup selected objects to a backup HSM.
-partition <backup_partition>	**-par**	Backup partition name (maximum length of 32 characters). **NOTE** Optional on the Luna Backup HSM 7. If you omit this option, the partition is assigned a default name (<source_partition_name>_<YYYYMMDD>).
-password <password>	**-pas**	Password for the specified partition.
-replace	**-rep**	Replace the entire backup with a new one. Since a new backup partition is created, you must present a new PO credential for the backup.
-slot <see description>	**-s**	Target slot containing the backup device. It can be specified by any of the following: > <slot number>, if the backup slot is in the current system. > **direct** to specify a USB-attached backup device. If you know the slot number that contains the USB-attached HSM, you can specify that slot number explicitly (for example, **-s 5**).
-smkonly	**-smk**	Back up the SKS Master Key (SMK) without objects. This option applies to Luna HSM Firmware 7.7.0 and newer.
-sopassword <sopassword>	**-sop**	SO password for the backup device.

Example

```
lunacm:> partition archive backup -slot 2 -partition sa78backup -domain clientdomain -password
<your_unique_password_for_backup-partition> -sopassword <your_unique_password_for_backuphsmso>
        Logging in as the SO on slot 2.

        Creating partition sa78backup on slot 2.

        Logging into the container sa78backup on slot 2 as the user.

        Creating Domain for the partition sa78backup on slot 2.

        Verifying that all objects can be backed up...

        6 objects will be backed up.
```

```
        Backing up objects...
        Cloned object 70 to partition sa78backup (new handle 14).
        Cloned object 69 to partition sa78backup (new handle 18).
        Cloned object 53 to partition sa78backup (new handle 19).
        Cloned object 54 to partition sa78backup (new handle 23).
        Cloned object 52 to partition sa78backup (new handle 24).
        Cloned object 47 to partition sa78backup (new handle 28).

        Backup Complete.

        6 objects have been backed up to partition sa78backup
        on slot 2.

Command Result : No Error
```

Example - SKS Backup

Backup the SMK from the current slot to the indicated SKS Backup HSM. This does not backup crypto objects. The target must be an SKS Backup HSM.

> **NOTE** Do not name the target partition to be created on the Backup HSM, because SKS backup creates the name from the label of the source partition, combined with a timestamp.

> **CAUTION!** Always be careful when restoring a backed-up SMK, because that operation overwrites the SMK on the target partition. If you do not have a backup of that overwritten SMK, any objects encrypted by that SMK can never be decrypted.

```
lunacm:>partition archive backup -slot 5 -smkonly

You are backing up a SKS partition.
Only the SKS master key (SMK) will be backed up.
No other objects will be cloned.

Are you sure you wish to continue?

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

Logging in as the SO on slot 5.

Please attend to the PED.

Creating partition 358628973182_2019:03:09-16:52:47 on slot 5.

Please attend to the PED.

Logging into the container 358628973182_2017:03:09-16:52:47 on slot 5 as the user.

Please attend to the PED.

Creating Domain for the partition 358628973182_2019:03:09-16:52:47 on slot 5.

Please attend to the PED.
```

```
The SMK was cloned successfully.

Command Result : No Error
```

partition archive contents

Display the contents of a specified backup partition on the backup device in the specified slot.

Syntax

partition archive contents -slot <backup_device> **-partition** <backup_partition> **-password** <password> [**-debug**]

Argument(s)	Shortcut	Description
-debug	**-deb**	Turn on additional error information (optional).
-partition <backup_partition>	**-par**	Partition on the backup device (maximum length of 64 characters).
-password	**-pas**	User password for the specified partition.
-slot <backup_device>	**-s**	Target slot containing the backup device. It can be specified by any of the following: > <slot number>, if the backup slot is in the current system. > **direct** to specify a USB-attached backup device. If you know the slot number that contains the USB-attached HSM, you can specify that slot number explicitly (for example, **-s 5**)

Example

```
lunacm:> partition archive contents -slot 2 -partition sa78backup

        Option -password was not supplied.  It is required.

        Enter the user password for the backup container: ********

        Logging in as the user on slot 2.

        Contents of partition sa78backup on slot 2 :

        Object list:

        Label:         MT RSA 4096-bit Private KeyGen
        Handle:        14
        Object Type:   Private Key
        Object UID:    26000000050000071b030100

        Label:         MT RSA 4096-bit Public KeyGen
        Handle:        18
        Object Type:   Public Key
        Object UID:    25000000050000071b030100

        Label:         MT RSA 4096-bit Private KeyGen
        Handle:        19
        Object Type:   Private Key
```

```
        Object UID:    24000000050000071b030100

        Label:         MT RSA 4096-bit Public KeyGen
        Handle:        23
        Object Type:   Public Key
        Object UID:    23000000050000071b030100

        Label:         MT RSA 4096-bit Private KeyGen
        Handle:        24
        Object Type:   Private Key
        Object UID:    22000000050000071b030100

        Label:         MT RSA 4096-bit Public KeyGen
        Handle:        28
        Object Type:   Public Key
        Object UID:    21000000050000071b030100


        Number of objects:  6


Command Result : No Error
```

partition archive delete

Delete the specified partition on the backup device in the specified slot.

Syntax

partition archive delete -slot <backup_slot> **-partition** <backup_partition> **-password** <password> [**-debug**]

Argument(s)	Shortcut	Description
-debug	**-deb**	Turn on additional error information. (optional)
-partition <backup_partition>	**-par**	Partition to delete on the backup device. (maximum length of 64 characters) .
-password <password>	**-pas**	User password for the specified partition.
-slot <see description>	**-s**	Target slot containing the backup device. It can be specified by any of the following: > <slot number>, if the backup slot is in the current system. > **direct** to specify a USB attached backup device. If you know the slot number that contains the USB attached HSM, you can specify that slot number explicitly (for example, **-s 5**)

Example

> **NOTE** The **partition archive delete** command cannot be issued while the currently selected slot is the Luna Backup HSM. Set your lunacm slot to any other slot, to allow **partition archive delete** to work.

```
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 archive delete -slot 2 -partition sa40backup

        Option -password was not supplied.  It is required.

        Enter the SO password for the backup device: ********

        Logging in as the SO on slot 2.

        Partition sa40backup was successfully deleted on slot 2.

Command Result : No Error
```

 Copyright 2001-2026 Thales Group

partition archive list

Display a list of the backup partitions on a backup device in a specified slot. The description of each backup includes information about the version of cloning protocol used, and the OUID of each SMK type stored on the backup. See Behavior of Pre-Firmware 7.7, V0, and V1 Partitions for more information.

Syntax

partition archive list -slot <backup_slot> [**-debug**]

Argument(s)	Shortcut	Description
-debug	**-de**	Turn on additional error information (optional).
-slot <see description>	**-s**	Target slot containing the backup device. It can be specified by any of the following: > <slot number>, if the backup slot is in the current system. > **direct** to specify a USB attached backup device. If you know the slot number that contains the USB attached HSM, you can specify that slot number explicitly (for example, **-s 5**)

Example

```
lunacm:> partition archive list -slot 105

        HSM Storage Information for slot 105:

           Total HSM Storage Space: 33816576
           Used HSM Storage Space:  862832
           Free HSM Storage Space:  32953744
           Allowed Partitions:      100
           Number Of Partitions:    2

        Partition list for slot 105

           Number of partitions: 2
           Label:                     myLunaPar_20200805153131
           Total Storage Size:        56984
           Used Storage Size:         56984
           Free Storage Size:         0
           Number Of Objects:         34

           Partition Cloning Version: 3
           Partition FM Status:       FM Disabled

           Partition SMK OUIDs:
                   SMK-FW4: Not Initialized
                   SMK-FW6: Not Initialized
                   SMK-FW7-FM: Not Initialized
                   SMK-FW7-Rollover: Not Initialized
                   SMK-FW7-Primary: Not Initialized
```

```
Label:                      myLunaPar_20200805153614
Total Storage Size:         78200
Used Storage Size:          78200
Free Storage Size:          0
Number Of Objects:          34

Partition Cloning Version: 3
Partition FM Status:       FM Disabled

Partition SMK OUIDs:
        SMK-FW4: Not Initialized
        SMK-FW6: Not Initialized
        SMK-FW7-FM: Not Initialized
        SMK-FW7-Rollover: Not Initialized
        SMK-FW7-Primary: 40000000360000140209010O
```

```
Command Result : No Error
```

> **NOTE** If you are migrating a Secure Master Key (SMK) from a Luna 6 HSM to a Luna 7 HSM, in addition to the SMK-FW6, the SMK-FW4 on the Luna 7 HSM is also overwritten by a new one (even if you have *not* initialized an SMK-FW4 on the Luna 6 HSM by a prior migration) and this command reports the presence of an SMK-FW4 on the Luna 7 HSM.

partition archive restore

Restore partition objects from a backup. Use this command to restore objects from the specified backup partition, in a backup HSM, in a specified slot, to the current user partition.

Cloning is a repeating atomic action

When you call for a cloning operation (such as backup or restore), the source HSM transfers each object one at a time, encrypted with the source domain. If the source is a V0 or pre-7.7.0 partition, the target HSM then decrypts and verifies each received blob. If the source is a V1 partition, the blob remains encrypted on the Backup HSM. See Behavior of Pre-Firmware 7.7, V0, and V1 Partitions for more information.

If the verification is successful, the object is stored at its destination – the domains are a match. If the verification fails, then the blob is discarded and the target HSM reports the failure. If the domain string or the domain PED key used to create the target partition did not match the domain of the source HSM partition, the operation fails with the error CKR_CERTIFICATE_INVALID. If the source is a partition using firmware older than Luna HSM Firmware 7.7.0, the source HSM moves to the next item in the object list and attempts to clone again, until the end of the list is reached. If the source is a V0 or V1 partition, the restore operation ends when the first object fails.

> **NOTE** To perform backup operations on Luna HSM Firmware 7.7.0 or newer (V0 or V1 partitions) you require at minimum:
>
> > Luna Backup HSM 7 Firmware 7.7.1
>
> > Luna Backup HSM G5 Firmware 6.28.0
>
> You can use a Luna Backup HSM with older firmware to restore objects to a V0 or V1 partition, but this is supported for purposes of getting your objects from the older partitions onto the newer V0 or V1 partitions only. V0 and V1 partitions are considered more secure than partitions at earlier firmware versions - any attempt to restore from a higher-security status to lower-security status fails gracefully.

Syntax

partition archive restore -slot <backup_slot> **-partition** <backup_partition> **-password** <your_unique_password_for_backup-partition> [**-replace**] [**-smkonly**] [**-objects**] [**-debug**] [**-force**]

Argument(s)	Shortcut	Description
-debug	**-deb**	Turn on additional error information (optional).
-force	**-f**	Force action with no prompting.

Argument(s)	Shortcut	Description
-objects <object_handles>	**-o**	Select specific individual objects to restore by specifying their object handles using any of the following methods: > a single object handle > **0** or **all**, to indicate that all objects are to be extracted > a list of handles, separated by commas. For example: **-objects 3,4,6** This option requires Luna HSM Client 10.3.0 or newer, and gives the capability to restore selected objects from a backup HSM.
-partition <backup_partition>	**-par**	Partition on the backup device. (maximum length of 64 characters) .
-password <password>	**-pas**	User password for the specified partition.
-replace	**-r**	Allow objects in the target user partition with the same OUID as the backup objects to be deleted and replaced. Objects with the same OUID are replaced only if they differ from the backup objects in some way. For example, if the object attributes have changed since the last backup, the object is replaced. **CAUTION!** The **-replace** option is deprecated and has been removed in Luna HSM Client 10.7.0 and newer. If you wish to restore an earlier version of an object, Thales recommends deleting the object(s) manually before restoring the partition from backup. Ensure that the target partition can receive objects from the backup HSM before deleting objects or using "partition archive restore" on the previous page with the **-replace** option; the cloning protocol may prevent objects from being restored, even if LunaCM states that `x objects will be restored`. This may occur if **HSM policy 55: Enable Restricted Restore** was enabled on the Luna Backup HSM 7 since the original backup was taken. If your partition is on an HSM with firmware older than Luna HSM Firmware 7.7.0, you must update to 7.7.0 or newer to restore objects from this backup.

Argument(s)	Shortcut	Description
-slot <see description>	**-s**	Target slot containing the backup device. It can be specified by any of the following: > <slot number>, if the backup slot is in the current system. > **direct** to specify a USB-attached backup device. If you know the slot number that contains the USB-attached HSM, you can specify that slot number explicitly (for example, **-s 5**)
-smkonly	**-smk**	Restore the SKS Master Key (SMK) without objects. This option applies to Luna HSM Firmware 7.7.0 and newer.

Example

```
lunacm:> partition archive restore -slot 6 -password <your_unique_password_for_backup-
partition> -partition mybackupPar

        Logging in to partition mybackupPar on slot 6 as the user.

        Verifying that all objects can be restored...

        1 object will be restored.

        Restoring objects...
        Cloned object 50 from partition mybackupPar (new handle 39).

        Restore Complete.

        1 objects have been restored from partition mybackupPar on slot 6.

Command Result : No Error
```

partition changelabel

Change the label of the partition in the active slot. This command affects the label originally set by the Partition SO during initialization.

You must be logged in as Partition SO to run this command.

> **NOTE** This feature requires minimum Luna HSM Firmware 7.2.0 and Luna HSM Client 7.2.0. This command is not applicable on DPoD Luna Cloud HSM services.

Syntax

partition changelabel -label <newlabel> [**-force**]

Argument(s)	Shortcut	Description
-force	**-f**	Force action without prompting for confirmation.
-label <newlabel>	**-l**	Specifies the new label for the partition. To include spaces in the partition label, enclose the new partition name in quotation marks.

Example

```
lunacm (64-bit) v7.2.0. Copyright (c) 2018 SafeNet. All rights reserved.


        Available HSMs:

        Slot Id ->              0
        Label ->                myUSBhsm
        Serial Number ->        7001812
        Model ->                G5Base
        Firmware Version ->     6.22.0
        Configuration ->        Luna HSM Admin Partition (PED) Signing With Cloning Mode
        Slot Description ->     Admin Token Slot
        HSM Configuration ->    Luna HSM Admin Partition (PED)
        HSM Status ->           OK

        Slot Id ->              3
        Label ->                originalpar
        Serial Number ->        1230507392695
        Model ->                Luna K7
        Firmware Version ->     7.2.0
        Configuration ->        Luna User Partition With SO (PW) Key Export With Cloning Mode
        Slot Description ->     User Token Slot

        Slot Id ->              4
        Label ->                myPCIeHSM
        Serial Number ->        528499
        Model ->                Luna K7
        Firmware Version ->     7.2.0
        Configuration ->        Luna HSM Admin Partition (PW) Key Export With Cloning Mode
```

```
        Slot Description ->     Admin Token Slot
        HSM Configuration ->    Luna HSM Admin Partition (PW)
        HSM Status ->           L3 Device


        Current Slot Id: 0

lunacm:>partition changeLabel -label newnamepar

        You are about to change the partition label.
        Are you sure you wish to continue?

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

Command Result : No Error

lunacm:>

lunacm:>slot list

        Slot Id ->              0
        Label ->                myUSBhsm
        Serial Number ->        7001812
        Model ->                G5Base
        Firmware Version ->     6.22.0
        Configuration ->        Luna HSM Admin Partition (PED) Signing With Cloning Mode
        Slot Description ->     Admin Token Slot
        HSM Configuration ->    Luna HSM Admin Partition (PED)
        HSM Status ->           OK

        Slot Id ->              3
        Label ->                newnamepar
        Serial Number ->        1230507392695
        Model ->                Luna K7
        Firmware Version ->     7.2.0
        Configuration ->        Luna User Partition With SO (PW) Key Export With Cloning Mode
        Slot Description ->     User Token Slot

        Slot Id ->              4
        Label ->                myPCIeHSM
        Serial Number ->        528499
        Model ->                Luna K7
        Firmware Version ->     7.2.0
        Configuration ->        Luna HSM Admin Partition (PW) Key Export With Cloning Mode
        Slot Description ->     Admin Token Slot
        HSM Configuration ->    Luna HSM Admin Partition (PW)
        HSM Status ->           L3 Device


        Current Slot Id: 3


Command Result : No Error
```

partition changepolicy

Change a user policy on the partition.

> **NOTE** If you are running more than one LunaCM session against the same partition, and change a partition policy in one LunaCM session, the policy change will be reflected in that session only. You must exit and restart the other LunaCM sessions to display the changed policy settings.

Syntax

partition changepolicy -policy <policy_id> **-value** <policy_value> [**-slot** <slot_number>] [**-force**]

Argument(s)	Shortcut	Description
-force	**-f**	Force action without prompting for confirmation.
-policy <policy_id>	**-p**	Specifies the ID of the policy you want to change. Change multiple policies by specifying a comma-separated list for **-policy** and **-value** (for example, **-policy 33,37,40 -value 0,1,1**).
-slot <slot_number>	**-s**	Specifies the slot where the partition is located.
-value <policy_value>	**-v**	Specifies the new value for the specified policy. Change multiple policies by specifying a comma-separated list for **-policy** and **-value** (for example, **-policy 33,37,40 -value 0,1,1**).

Example

The output will vary depending on the specific policy being changed and whether or not the change is destructive. Use the command "partition showpolicies" on page 183 with the **-verbose** option to see which commands are destructive and, if destructive, which direction -- On-to-off, or Off-to-on, or both directions.

```
C:\Program Files\SafeNet\LunaClient>lunacm.exe
lunacm.exe (64-bit) v10.6.0-431. Copyright (c) 2023 Thales Group. All rights reserved.


        Available HSMs:

        Slot Id ->              0
        Label ->                par
        Serial Number ->        1578912775566
        Model ->                LunaSA 7.8.3
        Firmware Version ->     7.9.0
        Bootloader Version ->   1.1.5
        Configuration ->        Luna User Partition With SO (PW) Key Export With Cloning Mode
        Slot Description ->     Net Token Slot
        FM HW Status ->         FM Ready


        Current Slot Id: 0
```

```
lunacm:> role login -n po -p userpin1

Command Result : No Error


lunacm:> partition showpolicies
        Partition Capabilities
                 0: Enable private key cloning : 1
                 1: Enable private key wrapping : 1
                 2: Enable private key unwrapping : 1
                 3: Enable private key masking : 1
                 4: Enable secret key cloning : 1
                 5: Enable secret key wrapping : 1
                 6: Enable secret key unwrapping : 1
                 7: Enable secret key masking : 1
                 9: Enable digest key : 1
                10: Enable multipurpose keys : 1
                11: Enable changing key attributes : 1
                15: Allow failed challenge responses : 1
                16: Enable operation without RSA blinding : 1
                17: Enable signing with non-local keys : 1
                18: Enable raw RSA operations : 1
                20: Max failed user logins allowed : 10
                21: Enable high availability recovery : 1
                22: Enable activation : 0
                23: Enable auto-activation : 0
                25: Minimum pin length (inverted: 255 - min) : 247
                26: Maximum pin length : 255
                28: Enable Key Management Functions : 1
                29: Enable RSA signing without confirmation : 1
                31: Enable private key unmasking : 1
                32: Enable secret key unmasking : 1
                33: Enable RSA PKCS mechanism : 1
                34: Enable CBC-PAD (un)wrap keys of any size : 1
                37: Enable enforcing Secure Trusted Channel : 1
                39: Enable Start/End Date Attributes : 1
                40: Enable Per-Key Authorization Data : 1
                41: Enable Partition Version : 1
                42: Enable CPv1 : 1
                43: Enable non-FIPS algorithms : 1
                44: Enable Extended Domain Management : 1

        Partition Policies
                 0: Allow private key cloning : 1
                 1: Allow private key wrapping : 0
                 2: Allow private key unwrapping : 1
                 3: Allow private key masking : 0
                 4: Allow secret key cloning : 1
                 5: Allow secret key wrapping : 1
                 6: Allow secret key unwrapping : 1
                 7: Allow secret key masking : 0
                 9: Allow digest key : 0
                10: Allow multipurpose keys : 1
                11: Allow changing key attributes : 1
                15: Ignore failed challenge responses : 1
                16: Operate without RSA blinding : 1
                17: Allow signing with non-local keys : 1
```

```
                18: Allow raw RSA operations : 1
                20: Max failed user logins allowed : 10
                21: Allow high availability recovery : 1
                25: Minimum pin length (inverted: 255 - min) : 247
                26: Maximum pin length : 255
                28: Allow Key Management Functions : 1
                29: Perform RSA signing without confirmation : 1
                31: Allow private key unmasking : 0
                32: Allow secret key unmasking : 0
                33: Allow RSA PKCS mechanism : 1
                34: Allow CBC-PAD (un)wrap keys of any size : 1
                37: Force Secure Trusted Channel : 0
                39: Allow Start/End Date Attributes : 0
                40: Require Per-Key Authorization Data : 0
                41: Partition Version : 0
                42: Allow CPv1 : 0
                43: Allow non-FIPS algorithms : 0
                44: Allow Extended Domain Management : 1


Command Result : No Error


lunacm:> partition domainlist

        Number of supported domains 3
        Defined Domains
                Domain #1 without label. Defined as primary domain.
                Domain #2 with label "domain".
                Domain #3 with label "domain%".

Command Result : No Error


lunacm:> partition changepolicy -v 0 -p  44 -f

Command Result : No Error


lunacm:> partition domainlist

        Number of supported domains 3
        Defined Domain
                Domain #1 without label. Defined as primary domain.

Command Result : No Error


lunacm:>
```

> **NOTE** In this particular example (above) of switching "Policy **44 - Allow Extended Domain Management**" from ON to OFF a partition with multiple domains retains the primary, but loses the non-primary domains.
>
> Other policy changes might have other important follow-on effects, and should be considered carefully for any HSM that is currently deployed.

partition changepw

Change the Crypto Officer password, or activation challenge password for the currently logged-in member partitions of an HA group.

From time to time, it might be necessary to change the secret associated with a role on an HSM or a partition of an HSM, or a cloning domain secret. Reasons for changing credentials include:

- Regular credential rotation as part of your organization's security policy
- Compromise of a partition challenge secret used in activation/auto-activation by applications connecting to a multifactor-quorum-athenticated HSM
- Personnel changes in your organization or changes to individual security clearances
- Changes to your security scheme (implementing/revoking M of N, PINs, or shared secrets)

This **partition changepw** command operates on the current *virtual* slot for the HA group, to perform password change for the entire group.

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

The following characters are allowed:

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

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

For further information and suggestions, see Changing passwords for an HA group.

Syntax

partition changepw -name <string> [**-oldpw** <oldpassword>] [**-newpw** <your_unique_password_for_co>] [[**-memberList** <serial_number>[,<serial_number>]+] [**-noRollback**] [**-logoutOther**]]

Argument(s)	Shortcut	Description
-logoutOther	**-l**	Log out all members of HA group, as well as the HA group itself from other applications. > *Include* the **-logoutOther** option if there is an immediate security concern, and you want all applications' access to be terminated immediately, to minimize damage due to a compromised credential. > *Omit* this option for relaxed situations like scheduled password roll-over, or personnel departing on good terms, or other non-urgent reasons, where you want the applications using the partition, with the current role credential, to have time to finish current tasks and end their sessions. When they resume activity, and need to create new sessions, they will do so only under the new credential for the role.
-memberlist <serial_number>	**-m**	A list of serial numbers for the HA group members on which the command will execute. Useful if some members were not successfully updated with the new password If this option is not included, the command defaults to attempting password change on all members of the group.
-oldpw <oldpassword>	**-old**	Current password (for application partition on PW authenticated HSM) or current challenge secret (for application partition on multifactor quorum-authenticated HSM). If you include option **-oldpw** the HSM assumes that you wish to change the challenge secret, which is the "secondary credential". This applies to Crypto Officer, which has primary and secondary credentials, but not to Partition SO, which has only primary credential. If you omit option **-oldpw** the HSM assumes that you wish to change the "primary credential" or PED key secret. Required if you wish to change the secondary credential.
-name <rolename>	**-n**	Name of role whose password is to change. Must be "co" until further notice. Required.
-newpw <newpassword>	**-new**	New password (for application partition on password-authenticated HSM) or new challenge secret (for application partition on multifactor quorum-authenticated HSM). Required if you have already provided an **-oldpw**.

Argument(s)	Shortcut	Description
-noRollback	**-no**	Default behavior, if the command encounters a member that cannot accept a new password, is to rollback all already-changed members to the current/old password, so that the HA group continues to function, while you investigate the problem. If **-noRollback** is specified, then the command updates the members that it can, and prints a list of members whose password could not be updated. You can use that list to populate **-memberlist** during a re-issue of the command.

Example

Change the CO password on all members of an HA group

```
lunacm> partition changePw -n co -oldPw userpin123 -newPw <your_unique_password_for_co> -
logoutOther

  Confirming all members of HA are online... [OK]

  Confirming all members of HA can be logged into... [OK]

  Changing password of all members of HA group... [OK]

  Final summary of members:


Member S/N           Member Label                 Password Status
==========           ============                 ===============
1213473506146        LNH_143.184_NTLS_v0_par1     Changed
91351086532          LNH_10.202_NTLS_v0_par1      Changed

Command Result : No Error
```

partition cipherdisable

Disables the indicated cipher suite for use when cloning objects.

Syntax

partition cipherdisable-id <cipher id>

Argument(s)	Shortcut	Description
-id <cipher id>	**-i**	The ID of the cipher to disable for cloning operations.

Example with firmware 7.9.0 onward

```
lunacm:>partition ciphershow
```

Cipher ID	Cipher Suite	Enabled
0	CPv3 RSA-4096-PKCS-SHA2-384 AES-256-GCM	Yes
1	CPv4 ECDSA-P521-SHA2-512 ECDH-P521-SHA2-512 AES-256-GCM	Yes
2	CPv4 ECDSA-P521-SHA2-512 ECDH-P521-SHA2-512 AES-256-CTR-HMAC-SHA2-512	Yes
3	CPv4 ECDSA-BP512-SHA2-512 ECDH-BP512-SHA2-512 AES-256-GCM	Yes
4	CPv4 ECDSA-BP512-SHA2-512 ECDH-BP512-SHA2-512 AES-256-CTR-HMAC-SHA2-512	Yes
5	CPv4 ECDSA-P521-SHA3-512 ECDH-P521-SHA3-512 AES-256-GCM	Yes
6	CPv4 ECDSA-P521-SHA3-512 ECDH-P521-SHA3-512 AES-256-CTR-HMAC-SHA3-512	Yes
7	CPv4 ECDSA-BP512-SHA3-512 ECDH-BP512-SHA3-512 AES-256-GCM	Yes
8	CPv4 ECDSA-BP512-SHA3-512 ECDH-BP512-SHA3-512 AES-256-CTR-HMAC-SHA3-512	Yes
9	CPv4 ECDSA-P521-SHA2-512 ECDH-P521-ML-KEM1024-SHA2-512 AES-256-GCM	Yes
10	CPv4 ECDSA-P521-SHA2-512 ECDH-P521-ML-KEM1024-SHA2-512 AES-256-CTR-HMAC-SHA2-512	Yes
11	CPv4 ECDSA-BP512-SHA2-512 ECDH-BP512-ML-KEM1024-SHA2-512 AES-256-GCM	Yes
12	CPv4 ECDSA-BP512-SHA2-512 ECDH-BP512-ML-KEM1024-SHA2-512 AES-256-CTR-HMAC-SHA2-512	Yes
13	CPv4 ECDSA-P521-SHA3-512 ECDH-P521-ML-KEM1024-SHA3-512 AES-256-GCM	Yes
14	CPv4 ECDSA-P521-SHA3-512 ECDH-P521-ML-KEM1024-SHA3-512 AES-256-CTR-HMAC-SHA3-512	Yes
15	CPv4 ECDSA-BP512-SHA3-512 ECDH-BP512-ML-KEM1024-SHA3-512 AES-256-GCM	Yes
16	CPv4 ECDSA-BP512-SHA3-512 ECDH-BP512-ML-KEM1024-SHA3-512 AES-256-CTR-HMAC-SHA3-512	Yes

```
Command Result : No Error

lunacm:>partition cipherdisable -id 0
CPv3 RSA-4096-PKCS-SHA-384 AES-256-GCM is now disabled

Command Result : No Error


lunacm:>partition ciphershow

 Cipher ID    Cipher Suite                                                  Enabled
_____________________________________________________________________________________

 0            CPv3 RSA-4096-PKCS-SHA2-384 AES-256-GCM                       No

 1            CPv4 ECDSA-P521-SHA2-512 ECDH-P521-SHA2-512 AES-256-GCM       Yes

 2            CPv4 ECDSA-P521-SHA2-512 ECDH-P521-SHA2-512                   Yes
              AES-256-CTR-HMAC-SHA2-512

 3            CPv4 ECDSA-BP512-SHA2-512 ECDH-BP512-SHA2-512                 Yes
              AES-256-GCM

 4            CPv4 ECDSA-BP512-SHA2-512 ECDH-BP512-SHA2-512                 Yes
              AES-256-CTR-HMAC-SHA2-512

 5            CPv4 ECDSA-P521-SHA3-512 ECDH-P521-SHA3-512 AES-256-GCM       Yes

 6            CPv4 ECDSA-P521-SHA3-512 ECDH-P521-SHA3-512                   Yes
              AES-256-CTR-HMAC-SHA3-512

 7            CPv4 ECDSA-BP512-SHA3-512 ECDH-BP512-SHA3-512                 Yes
              AES-256-GCM

 8            CPv4 ECDSA-BP512-SHA3-512 ECDH-BP512-SHA3-512                 Yes
              AES-256-CTR-HMAC-SHA3-512

 9            CPv4 ECDSA-P521-SHA2-512 ECDH-P521-ML-KEM1024-SHA2-512        Yes
              AES-256-GCM

 10           CPv4 ECDSA-P521-SHA2-512 ECDH-P521-ML-KEM1024-SHA2-512        Yes
              AES-256-CTR-HMAC-SHA2-512

 11           CPv4 ECDSA-BP512-SHA2-512                                     Yes
              ECDH-BP512-ML-KEM1024-SHA2-512 AES-256-GCM

 12           CPv4 ECDSA-BP512-SHA2-512                                     Yes
              ECDH-BP512-ML-KEM1024-SHA2-512
              AES-256-CTR-HMAC-SHA2-512

 13           CPv4 ECDSA-P521-SHA3-512 ECDH-P521-ML-KEM1024-SHA3-512        Yes
              AES-256-GCM

 14           CPv4 ECDSA-P521-SHA3-512 ECDH-P521-ML-KEM1024-SHA3-512        Yes
              AES-256-CTR-HMAC-SHA3-512

 15           CPv4 ECDSA-BP512-SHA3-512                                     Yes
```

```
              ECDH-BP512-ML-KEM1024-SHA3-512 AES-256-GCM

 16           CPv4 ECDSA-BP512-SHA3-512                                  Yes
              ECDH-BP512-ML-KEM1024-SHA3-512
              AES-256-CTR-HMAC-SHA3-512


Command Result : No Error
```

Example prior to firmware 7.9.0

```
lunacm:>partition cipherdisable -id 0
CPv3 RSA-4096-PKCS-SHA-384 AES-256-GCM is now disabled

Command Result : No Error


lunacm:>partition ciphershow

 Cipher ID    Cipher Suite                                                Enabled
_____________________________________________________________________________________

 0            CPv3 RSA-4096-PKCS-SHA-384 AES-256-GCM                     No

 1            CPv4 ECDSA-P521-SHA-512 ECDH-P521-SHA512 AES-256-GCM       Yes

 2            CPv4 ECDSA-P521-SHA-512 ECDH-P521-SHA512                   Yes
              AES-256-CTR-SHA256-HMAC

 3            CPv4 ECDSA-BP521-SHA-512 ECDH-BP521-SHA512 AES-256-GCM     Yes

 4            CPv4 ECDSA-BP521-SHA-512 ECDH-BP521-SHA512                 Yes
              AES-256-CTR-SHA256-HMAC

 5            CPv4 ECDSA-P521-SHA3-512 ECDH-P521-SHA3-512 AES-256-GCM    Yes

 6            CPv4 ECDSA-P521-SHA3-512 ECDH-P521-SHA3-512                Yes
              AES-256-CTR-SHA256-HMAC

 7            CPv4 ECDSA-BP521-SHA3-512 ECDH-BP521-SHA3-512              Yes
              AES-256-GCM

 8            CPv4 ECDSA-BP521-SHA3-512 ECDH-BP521-SHA3-512              Yes
              AES-256-CTR-SHA256-HMAC


Command Result : No Error
```

partition cipherenable

Enables the indicated cipher suite for use when cloning objects.

Syntax

partition cipherenable-id <cipher id>

Argument(s)	Shortcut	Description
-id <cipher id>	**-i**	The ID of the cipher to enable for cloning operations.

Example firmware 7.9.0 onward

```
lunacm:>partition ciphershow

 Cipher ID    Cipher Suite                                                    Enabled
_____________________________________________________________________________________
 0            CPv3 RSA-4096-PKCS-SHA2-384 AES-256-GCM                         No

 1            CPv4 ECDSA-P521-SHA2-512 ECDH-P521-SHA2-512 AES-256-GCM         No

 2            CPv4 ECDSA-P521-SHA2-512 ECDH-P521-SHA2-512                     No
              AES-256-CTR-HMAC-SHA2-512

 3            CPv4 ECDSA-BP512-SHA2-512 ECDH-BP512-SHA2-512                   No
              AES-256-GCM

 4            CPv4 ECDSA-BP512-SHA2-512 ECDH-BP512-SHA2-512                   No
              AES-256-CTR-HMAC-SHA2-512

 5            CPv4 ECDSA-P521-SHA3-512 ECDH-P521-SHA3-512 AES-256-GCM         No

 6            CPv4 ECDSA-P521-SHA3-512 ECDH-P521-SHA3-512                     No
              AES-256-CTR-HMAC-SHA3-512

 7            CPv4 ECDSA-BP512-SHA3-512 ECDH-BP512-SHA3-512                   No
              AES-256-GCM

 8            CPv4 ECDSA-BP512-SHA3-512 ECDH-BP512-SHA3-512                   No
              AES-256-CTR-HMAC-SHA3-512

 9            CPv4 ECDSA-P521-SHA2-512 ECDH-P521-ML-KEM1024-SHA2-512          No
              AES-256-GCM

 10           CPv4 ECDSA-P521-SHA2-512 ECDH-P521-ML-KEM1024-SHA2-512          No
              AES-256-CTR-HMAC-SHA2-512

 11           CPv4 ECDSA-BP512-SHA2-512                                       No
              ECDH-BP512-ML-KEM1024-SHA2-512 AES-256-GCM

 12           CPv4 ECDSA-BP512-SHA2-512                                       No
              ECDH-BP512-ML-KEM1024-SHA2-512
              AES-256-CTR-HMAC-SHA2-512

 13           CPv4 ECDSA-P521-SHA3-512 ECDH-P521-ML-KEM1024-SHA3-512          No
              AES-256-GCM

 14           CPv4 ECDSA-P521-SHA3-512 ECDH-P521-ML-KEM1024-SHA3-512          No
              AES-256-CTR-HMAC-SHA3-512

 15           CPv4 ECDSA-BP512-SHA3-512                                       No
              ECDH-BP512-ML-KEM1024-SHA3-512 AES-256-GCM
```

```
 16           CPv4 ECDSA-BP512-SHA3-512                                  No
              ECDH-BP512-ML-KEM1024-SHA3-512
              AES-256-CTR-HMAC-SHA3-512


Command Result : No Error

lunacm:>partition cipherenable -id 9
CPv4 ECDSA-P521-SHA2-512 ECDH-P521-ML-KEM1024-SHA2-512 AES-256-GCM is now enabled

Command Result : No Error


lunacm:> partition cipherenable -id 10
CPv4 ECDSA-P521-SHA2-512 ECDH-P521-ML-KEM1024-SHA2-512 AES-256-CTR-HMAC-SHA2-512 is now enabled

Command Result : No Error


lunacm:> partition cipherenable -id 11
CPv4 ECDSA-BP512-SHA2-512 ECDH-BP512-ML-KEM1024-SHA2-512 AES-256-GCM is now enabled

Command Result : No Error


lunacm:> partition cipherenable -id 12
CPv4 ECDSA-BP512-SHA2-512 ECDH-BP512-ML-KEM1024-SHA2-512 AES-256-CTR-HMAC-SHA2-512 is now
enabled

Command Result : No Error


lunacm:> partition cipherenable -id 13
CPv4 ECDSA-P521-SHA3-512 ECDH-P521-ML-KEM1024-SHA3-512 AES-256-GCM is now enabled

Command Result : No Error


lunacm:> partition cipherenable -id 14
CPv4 ECDSA-P521-SHA3-512 ECDH-P521-ML-KEM1024-SHA3-512 AES-256-CTR-HMAC-SHA3-512 is now enabled

Command Result : No Error


lunacm:> partition cipherenable -id 15
CPv4 ECDSA-BP512-SHA3-512 ECDH-BP512-ML-KEM1024-SHA3-512 AES-256-GCM is now enabled

Command Result : No Error


lunacm:> partition cipherenable -id 16
CPv4 ECDSA-BP512-SHA3-512 ECDH-BP512-ML-KEM1024-SHA3-512 AES-256-CTR-HMAC-SHA3-512 is now
enabled

Command Result : No Error
```

```
lunacm:>partition ciphershow

 Cipher ID    Cipher Suite                                                  Enabled
_____________________________________________________________________________________
 0            CPv3 RSA-4096-PKCS-SHA2-384 AES-256-GCM                       No

 1            CPv4 ECDSA-P521-SHA2-512 ECDH-P521-SHA2-512 AES-256-GCM       No

 2            CPv4 ECDSA-P521-SHA2-512 ECDH-P521-SHA2-512                   No
              AES-256-CTR-HMAC-SHA2-512

 3            CPv4 ECDSA-BP512-SHA2-512 ECDH-BP512-SHA2-512                 No
              AES-256-GCM

 4            CPv4 ECDSA-BP512-SHA2-512 ECDH-BP512-SHA2-512                 No
              AES-256-CTR-HMAC-SHA2-512

 5            CPv4 ECDSA-P521-SHA3-512 ECDH-P521-SHA3-512 AES-256-GCM       No

 6            CPv4 ECDSA-P521-SHA3-512 ECDH-P521-SHA3-512                   No
              AES-256-CTR-HMAC-SHA3-512

 7            CPv4 ECDSA-BP512-SHA3-512 ECDH-BP512-SHA3-512                 No
              AES-256-GCM

 8            CPv4 ECDSA-BP512-SHA3-512 ECDH-BP512-SHA3-512                 No
              AES-256-CTR-HMAC-SHA3-512

 9            CPv4 ECDSA-P521-SHA2-512 ECDH-P521-ML-KEM1024-SHA2-512        Yes
              AES-256-GCM

 10           CPv4 ECDSA-P521-SHA2-512 ECDH-P521-ML-KEM1024-SHA2-512        Yes
              AES-256-CTR-HMAC-SHA2-512

 11           CPv4 ECDSA-BP512-SHA2-512                                     Yes
              ECDH-BP512-ML-KEM1024-SHA2-512 AES-256-GCM

 12           CPv4 ECDSA-BP512-SHA2-512                                     Yes
              ECDH-BP512-ML-KEM1024-SHA2-512
              AES-256-CTR-HMAC-SHA2-512

 13           CPv4 ECDSA-P521-SHA3-512 ECDH-P521-ML-KEM1024-SHA3-512        Yes
              AES-256-GCM

 14           CPv4 ECDSA-P521-SHA3-512 ECDH-P521-ML-KEM1024-SHA3-512        Yes
              AES-256-CTR-HMAC-SHA3-512

 15           CPv4 ECDSA-BP512-SHA3-512                                     Yes
              ECDH-BP512-ML-KEM1024-SHA3-512 AES-256-GCM

 16           CPv4 ECDSA-BP512-SHA3-512                                     Yes
              ECDH-BP512-ML-KEM1024-SHA3-512
              AES-256-CTR-HMAC-SHA3-512


Command Result : No Error
```

Example prior to firmware 7.9.0

```
lunacm:>partition ciphershow

 Cipher ID    Cipher Suite                                                  Enabled
_____________________________________________________________________________________

 0            CPv3 RSA-4096-PKCS-SHA-384 AES-256-GCM                        Yes

 1            CPv4 ECDSA-P521-SHA-512 ECDH-P521-SHA512 AES-256-GCM          No

 2            CPv4 ECDSA-P521-SHA-512 ECDH-P521-SHA512                      No
              AES-256-CTR-SHA256-HMAC

 3            CPv4 ECDSA-BP521-SHA-512 ECDH-BP521-SHA512 AES-256-GCM        No

 4            CPv4 ECDSA-BP521-SHA-512 ECDH-BP521-SHA512                    No
              AES-256-CTR-SHA256-HMAC

 5            CPv4 ECDSA-P521-SHA3-512 ECDH-P521-SHA3-512 AES-256-GCM       No

 6            CPv4 ECDSA-P521-SHA3-512 ECDH-P521-SHA3-512                   No
              AES-256-CTR-SHA256-HMAC

 7            CPv4 ECDSA-BP521-SHA3-512 ECDH-BP521-SHA3-512                 No
              AES-256-GCM

 8            CPv4 ECDSA-BP521-SHA3-512 ECDH-BP521-SHA3-512                 No
              AES-256-CTR-SHA256-HMAC


Command Result : No Error

lunacm:>partition cipherenable -id 1
CPv4 ECDSA-P521-SHA-512 ECDH-P521-SHA512 AES-256-GCM is now enabled

Command Result : No Error


lunacm:>partition ciphershow

 Cipher ID    Cipher Suite                                                  Enabled
_____________________________________________________________________________________

 0            CPv3 RSA-4096-PKCS-SHA-384 AES-256-GCM                        Yes

 1            CPv4 ECDSA-P521-SHA-512 ECDH-P521-SHA512 AES-256-GCM          Yes

 2            CPv4 ECDSA-P521-SHA-512 ECDH-P521-SHA512                      No
              AES-256-CTR-SHA256-HMAC

 3            CPv4 ECDSA-BP521-SHA-512 ECDH-BP521-SHA512 AES-256-GCM        No

 4            CPv4 ECDSA-BP521-SHA-512 ECDH-BP521-SHA512                    No
              AES-256-CTR-SHA256-HMAC

 5            CPv4 ECDSA-P521-SHA3-512 ECDH-P521-SHA3-512 AES-256-GCM       No
```

```
 6              CPv4 ECDSA-P521-SHA3-512 ECDH-P521-SHA3-512             No
                AES-256-CTR-SHA256-HMAC

 7              CPv4 ECDSA-BP521-SHA3-512 ECDH-BP521-SHA3-512           No
                AES-256-GCM

 8              CPv4 ECDSA-BP521-SHA3-512 ECDH-BP521-SHA3-512           No
                AES-256-CTR-SHA256-HMAC


Command Result : No Error
```

partition ciphershow

Shows the cipher suites available for cloning operations.

Multiple cipher suite options are available for use by Cloning Protocol version 4 (CPv4). When two CPv4 partitions begin a cloning operation, they negotiate for the strongest cipher suite available to both parties. You can affect the result by disabling some suites - all are enabled by default. Use the **partition cipherenable** and **partition cipherdisable** commands.

Cloning cipher suites for CPv4 have the following format:

CPv4 <signature><key agreement<symmetric>

CPv4 ECDSA-P521-SHA-512 ECDH-P521 AES-256-KWP

In addition, CPv3 has a single cipher suite, which can be disabled (enabled by default).

Cloning cipher suite for CPv3 has the following format:

CPv3 <key transport><symmetric>

CPv3 RSA-4096-PKCS-SHA-284 AES-256-GCM

If all cipher suites are disabled, cloning (including backup) is not possible for the partition and contents.

If Partition Policy 42 is set (allow CPv1), then CPv3 and CPv4 are disabled.

Syntax

partition ciphershow

Example using Luna HSM Firmware 7.9.0 or Newer

```
lunacm:>partition ciphershow

 Cipher ID    Cipher Suite                                              Enabled
_____________________________________________________________________________
 0            CPv3 RSA-4096-PKCS-SHA2-384 AES-256-GCM                   Yes

 1            CPv4 ECDSA-P521-SHA2-512 ECDH-P521-SHA2-512 AES-256-GCM Yes

 2            CPv4 ECDSA-P521-SHA2-512 ECDH-P521-SHA2-512               Yes
              AES-256-CTR-HMAC-SHA2-512

 3            CPv4 ECDSA-BP512-SHA2-512 ECDH-BP512-SHA2-512             Yes
```

```
              AES-256-GCM

 4            CPv4 ECDSA-BP512-SHA2-512 ECDH-BP512-SHA2-512           Yes
              AES-256-CTR-HMAC-SHA2-512

 5            CPv4 ECDSA-P521-SHA3-512 ECDH-P521-SHA3-512 AES-256-GCM Yes

 6            CPv4 ECDSA-P521-SHA3-512 ECDH-P521-SHA3-512             Yes
              AES-256-CTR-HMAC-SHA3-512

 7            CPv4 ECDSA-BP512-SHA3-512 ECDH-BP512-SHA3-512           Yes
              AES-256-GCM

 8            CPv4 ECDSA-BP512-SHA3-512 ECDH-BP512-SHA3-512           Yes
              AES-256-CTR-HMAC-SHA3-512

 9            CPv4 ECDSA-P521-SHA2-512 ECDH-P521-ML-KEM1024-SHA2-512  Yes
              AES-256-GCM

 10           CPv4 ECDSA-P521-SHA2-512 ECDH-P521-ML-KEM1024-SHA2-512  Yes
              AES-256-CTR-HMAC-SHA2-512

 11           CPv4 ECDSA-BP512-SHA2-512                               Yes
              ECDH-BP512-ML-KEM1024-SHA2-512 AES-256-GCM

 12           CPv4 ECDSA-BP512-SHA2-512                               Yes
              ECDH-BP512-ML-KEM1024-SHA2-512
              AES-256-CTR-HMAC-SHA2-512

 13           CPv4 ECDSA-P521-SHA3-512 ECDH-P521-ML-KEM1024-SHA3-512  Yes
              AES-256-GCM

 14           CPv4 ECDSA-P521-SHA3-512 ECDH-P521-ML-KEM1024-SHA3-512  Yes
              AES-256-CTR-HMAC-SHA3-512

 15           CPv4 ECDSA-BP512-SHA3-512                               Yes
              ECDH-BP512-ML-KEM1024-SHA3-512 AES-256-GCM

 16           CPv4 ECDSA-BP512-SHA3-512                               Yes
              ECDH-BP512-ML-KEM1024-SHA3-512
              AES-256-CTR-HMAC-SHA3-512



Command Result : No Error
```

Example using Luna HSM Firmware 7.8.9 or Older

```
lunacm:>partition ciphershow

 Cipher ID    Cipher Suite                                            Enabled
_____________________________________________________________________________

 0            CPv3 RSA-4096-PKCS-SHA-384 AES-256-GCM                  Yes

 1            CPv4 ECDSA-P521-SHA-512 ECDH-P521-SHA512 AES-256-GCM    Yes
```

```
2            CPv4 ECDSA-P521-SHA-512 ECDH-P521-SHA512                Yes
             AES-256-CTR-SHA256-HMAC

3            CPv4 ECDSA-BP521-SHA-512 ECDH-BP521-SHA512 AES-256-GCM  Yes

4            CPv4 ECDSA-BP521-SHA-512 ECDH-BP521-SHA512              Yes
             AES-256-CTR-SHA256-HMAC

5            CPv4 ECDSA-P521-SHA3-512 ECDH-P521-SHA3-512 AES-256-GCM Yes

6            CPv4 ECDSA-P521-SHA3-512 ECDH-P521-SHA3-512             Yes
             AES-256-CTR-SHA256-HMAC

7            CPv4 ECDSA-BP521-SHA3-512 ECDH-BP521-SHA3-512           Yes
             AES-256-GCM

8            CPv4 ECDSA-BP521-SHA3-512 ECDH-BP521-SHA3-512           Yes
             AES-256-CTR-SHA256-HMAC


Command Result : No Error
```

The above list might change with time, as newer cipher suites are added, or others age out.

partition clear

Delete all User partition objects. You must be logged in as the user. The partition structure remains in place.

Syntax

partition clear [**-force**]

Argument(s)	Shortcut	Description
-force	**-f**	Force the action without prompting for confirmation (useful for scripting). The **-force** option cannot be used on a virtual slot belonging to an HA group.

Example

```
lunacm:>partition clear

        You are about to delete all token objects.
        Are you sure you wish to continue?

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

        2 objects were deleted.

Command Result : No Error
```

 Copyright 2001-2026 Thales Group

partition clone

Clone partition objects from the current active slot to the specified slot.

> **CAUTION!** If you are cloning objects to a different kind of partition (for example, between a Luna partition and a Luna Cloud HSM service) or a partition on an HSM running a different firmware version, refer to Cloning Keys Between Luna 6, Luna 7, and Luna Cloud HSM, Password or Multifactor Quorum for important information about cloning capabilities.

Cloning is a repeating atomic action

When you call for a cloning operation (such as backup or restore), the source HSM transfers a single object, encrypted with the source domain. The target HSM then decrypts and verifies the received blob.

If the verification is successful, the object is stored at its destination – the domains are a match. If the verification fails, then the blob is discarded and the target HSM reports the failure. Most likely the domain string or the domain PED key, that you used when creating the target partition, did not match the domain of the source HSM partition. The source HSM moves to the next item in the object list and attempts to clone again, until the end of the list is reached.

This means that if you issue a backup command for a source partition containing several objects, but have a mismatch of domains between your source HSM partition and the backup HSM partition, then you will see a separate error message for every object on the source partition as it individually fails verification at the target HSM.

If you invoked scalable key storage (SKS) for your applications to create and store large numbers of keys, then the partition is V1. If you perform cloning operations (including HA) or Backup and Restore, see Cloning or Backup / Restore with SKS.

Syntax

partition clone -objects <handles> **-password** <password> **-slot** <slot_number> [**-force**]

Argument(s)	Shortcut	Description
-force	**-f**	Force the action without prompting for confirmation.
-objects <handles>	**-o**	Specifies the object handles to extract. You can specify the object handles to clone using any of the following methods: > a single object handle > **0** or **all**, to indicate that all objects are to be extracted > a list of handles, separated by commas. For example: **-objects 3,4,6**
-password <password>	**-p**	The target slot password. This option does not apply to multifactor quorum-authenticated HSMs/tokens.
-slot <slot_number>	**-s**	The target slot.

Example

```
lunacm:> partition clone -objects 124,140 -slot 1

        Option -password was not supplied.  It is required.

        Enter the password for the target slot: ********

        Verifying that the specified objects can be cloned.

        All objects can be cloned.

        Logging in to target slot 1

        Checking if objects already exist on target slot 1.

        Cloning the objects.
                Handle 124 on slot 0 is now handle 141 on slot 1
                Handle 140 on slot 0 is now handle 28 on slot 1

Command Result : No Error
```

partition contents

Display a list of the objects on the partition. This command will display all objects accessible to the role that is currently logged in. The total object count is also displayed. For each object found, the label, handle, object type, and object UID are displayed.

Syntax

partition contents

Example

```
lunacm:> partition contents

        The 'Crypto User' is currently logged in.  Looking for objects
        accessible to the 'Crypto User'.

        Object list:

        Label:
        Handle:         141
        Object Type:    Private Key
        Object UID:     7c080000090000061b030100

        Label:
        Handle:         140
        Object Type:    Public Key
        Object UID:     7b080000090000061b030100

        Label:
        Handle:         125
        Object Type:    Private Key
        Object UID:     7a080000090000061b030100

        Label:
        Handle:         124
        Object Type:    Public Key
        Object UID:     790800000090000061b030100


        Number of objects:  4


Command Result : No Error
```

partition create

Create an application partition on a locally installed or USB-connected HSM.

The command is run from the HSM administrative partition. The HSM SO must be logged in.

Syntax

partition create [**-slot** <number>] [**-size** <bytes>] [**-force**]

Argument(s)	Shortcut	Description
-force	**-f**	Force the action without prompting for confirmation (useful when scripting commands).
-size <bytes>	**-si**	Storage size of partition in bytes (used only for HSMs supporting multiple application partitions, to specify a size other than the calculated default size - depends on HSM memory, existing application partitions, and their specifications)
-slot <number>	**-sl**	Slot where the new partition is to be created (not used if **-label** is specified)
-version <number>	**-v**	Create a partition with version (0 or 1)

> **NOTE** If the HSM supports just a single application partition, and one already exists, the **partition create** command stops and throws the error "Error in execution : CKR_LICENSE_CAPACITY_EXCEEDED." To create a new application partition, delete the existing one first, with **partition delete**, then re-issue **partition create**.

Example without version specified

The partition in slot 3 is the administrative partition for the Luna PCIe HSM 7, and is not used by applications for crypto operations.

```
lunacm:> slot list

        Slot Id ->              3
        Tunnel Slot Id ->       2
        Label ->                mypcie7
        Serial Number ->        150022
        Model ->                Luna K7
        Firmware Version ->     7.0.1
        Configuration ->        Luna HSM Admin Partition (PED) Signing With Cloning Mode
        Slot Description ->     Admin Token Slot
        HSM Configuration ->    Luna HSM Admin Partition (PED)
        HSM Status ->           OK

        Slot Id ->              4
        HSM Label ->            myG5pw
        HSM Serial Number ->    7001312
        HSM Model ->            G5Base
```

```
        HSM Firmware Version -> 6.10.4
        HSM Configuration ->    Luna USB HSM (PW) Signing With Cloning Mode
        HSM Status ->           OK

        Current Slot Id: 3

Command Result : No Error


lunacm:> partition create

Command Result : No Error

lunacm:> slot list

        Slot Id ->              3
        Tunnel Slot Id ->       2
        Label ->
        Serial Number ->        349297122736
        Model ->                Luna K7
        Firmware Version ->     7.7.0
        Configuration ->        Luna User Partition With SO (PED) Signing With Cloning Mode
        Slot Description ->     User Token Slot

        Slot Id ->              4
        Tunnel Slot Id ->       2
        Label ->                mypcie7
        Serial Number ->        150022
        Model ->                Luna K7
        Firmware Version ->     7.7.0
        Configuration ->        Luna HSM Admin Partition (PED) Signing With Cloning Mode
        Slot Description ->     Admin Token Slot
        HSM Configuration ->    Luna HSM Admin Partition (PED)
        HSM Status ->           OK


        Current Slot Id: 1

Command Result : No Error
```

Example *with* version specified

The partition in slot 3 is the administrative partition for the Luna PCIe HSM 7, and is not used for applications and crypto.

```
lunacm:> slot list

        Slot Id ->              3
        Tunnel Slot Id ->       2
        Label ->                mypcie7
        Serial Number ->        150022
        Model ->                Luna K7
        Firmware Version ->     7.8.0
        Configuration ->        Luna HSM Admin Partition (PED) Signing With Cloning Mode
        Slot Description ->     Admin Token Slot
        HSM Configuration ->    Luna HSM Admin Partition (PED)
        HSM Status ->           OK
```

```
        Current Slot Id: 3

Command Result : No Error

lunacm:> partition create -version 1

Command Result : No Error


lunacm:> slot list

        Slot Id ->              3
        Label ->
        Serial Number ->        1230507392701
        Model ->                Luna K7
        Firmware Version ->     7.8.0
        Bootloader Version ->   1.1.4
        Configuration ->        Luna User Partition With SO (PW) Key Export With Cloning Mode
        Slot Description ->     User Token Slot
        FM HW Status ->         FM Ready

        Slot Id ->              4
        Tunnel Slot Id ->       2
        Label ->                mypcie7
        Serial Number ->        150022
        Model ->                Luna K7
        Firmware Version ->     7.8.0
        Configuration ->        Luna HSM Admin Partition (PED) Signing With Cloning Mode
        Slot Description ->     Admin Token Slot
        HSM Configuration ->    Luna HSM Admin Partition (PED)
        HSM Status ->           OK


        Current Slot Id: 4
```

partition delete

Delete an application partition. This command must be invoked from the HSM administrative partition, and operates against the application partition at the indicated slot.

Syntax

partition delete -slot <slotnumber> [**-force**]

Argument(s)	Shortcut	Description
-slot <slotnumber>	**-sl**	Slot number of partition to be deleted.
-force	**-f**	Force the action without prompting for confirmation (useful for scripting).

Example of partition delete command, showing slot list before and after

```
lunacm:> slot list

        Slot Id ->              0
        Tunnel Slot Id ->       2
        Label ->                pciepartition
        Serial Number ->        349297122733
        Model ->                Luna K7
        Firmware Version ->     7.0.1
        Configuration ->        Luna User Partition With SO (PED) Signing With Cloning Mode
        Slot Description ->     User Token Slot

        Slot Id ->              1
        Tunnel Slot Id ->       2
        Label ->                mypcie7
        Serial Number ->        150022
        Model ->                Luna K7
        Firmware Version ->     7.0.1
        Configuration ->        Luna HSM Admin Partition (PED) Signing With Cloning Mode
        Slot Description ->     Admin Token Slot
        HSM Configuration ->    Luna HSM Admin Partition (PED)
        HSM Status ->           OK

        Slot Id ->              3
        HSM Label ->            myG5pw
        HSM Serial Number ->    7001312
        HSM Model ->            G5Base
        HSM Firmware Version -> 6.10.4
        HSM Configuration ->    Luna USB HSM (PW) Signing With Cloning Mode
        HSM Status ->           OK



        Current Slot Id: 1


Command Result : No Error
```

```
lunacm:> partition delete -slot 0

        You are about to delete partition.
        Are you sure you wish to continue?

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

Command Result : No Error

lunacm:> slot list

        Slot Id ->              1
        Tunnel Slot Id ->       2
        Label ->                mypcie7
        Serial Number ->        150022
        Model ->                Luna K7
        Firmware Version ->     7.0.1
        Configuration ->        Luna HSM Admin Partition (PED) Signing With Cloning Mode
        Slot Description ->     Admin Token Slot
        HSM Configuration ->    Luna HSM Admin Partition (PED)
        HSM Status ->           OK

        Slot Id ->              3
        HSM Label ->            myG5pw
        HSM Serial Number ->    7001312
        HSM Model ->            G5Base
        HSM Firmware Version -> 6.10.4
        HSM Configuration ->    Luna USB HSM (PW) Signing With Cloning Mode
        HSM Status ->           OK



        Current Slot Id: 1


Command Result : No Error
```

partition domainadd

Add a cloning domain to the partition. Partitions are assigned their original/own domain when initialized, and in that default state can perform cloning/HA operations only with other partitions sharing that single domain.

Which domain is primary and how to change - All partitions, after initialization, have the current or original security/cloning domain marked as the primary, the domain that is chosen by default for cloning. For a partition with more than one domain, either of the others can be designated as primary, instead, using the **partition domainadd** and **partition domainchangelabel** commands, by invoking their **-primary** option.

The **partition domainadd** command is meant to add a domain so that the partition can clone objects with partitions that have the new/added domain, as well as with partitions that have the same domain as originally assigned to the current partition during initialization.

> A maximum of two additional domains can be added to the original partition domain; they can be either password-authenticated or multifactor quorum-authenticated.
  - If you are adding a text domain for some other password-authenticated partition, then
    - *do* include the **-domain** option with the domain string from that other partition and
    - *do not* include the **-domainped** option).
  - If you are adding a domain PED key secret for some other multifactor quorum-authenticated partition, then
    - *do not include* the **-domain** option, and
    - *do* include the **-domainped** option causing the HSM to look for a connected PED with red PED key, to retrieve that key's content as the domain to add to the current partition.

> If you have more than one domain in your partition, the system assumes that you want to be able to tell them apart, so include the **-domainlabel** option each time you add a domain (the label is a string between 1 and 32 characters).

> The **-domainlabel** is added as an option with Luna HSM Firmware 7.8.0Luna USB HSM 7 Firmware 7.9.2. Pre-existing partitions (created prior to firmware 7.8.0) can continue to have no label for continuity of established procedures and processes. However if you create or import a domain, the system ensures that no two can have the same label.
  - a label is necessary when adding a domain if an existing domain is not labeled.

> **CAUTION!** Domain secret strings for password-authenticated HSMs and Luna Cloud HSMs are used to generate the secret key for cloning, and are as cryptographically sensitive as a user password. The domain label associated with a domain string is not sensitive, and is used only to distinguish the domain from others assigned to the same partition. ***Never use the same string for the domain* label *and for the domain* secret.**

> Use "partition domainchangelabel" on page 159 to change label for a domain,
  - including applying a label to a domain that did not already have one.

Primary domain - On pre-firmware 7.8.0 HSM partitions the single possible domain is effectively the primary domain. For firmware 7.8.0 or newer, partitions can have as many as three domains. Of the three possible, one domain is always primary, but the status of primary can be moved to another domain if needed. "Primary" in this context means "the one that is tried first". If there is no match for the primary domain on the source partition, the systems goes on to try for other matching domains.

[**Summary**]

When cloning from a partition of an HSM with a firmware version lower than 7.8.0 to a version 7.8.0 or higher with multiple domains, the primary domain is used.

[**Explanation**]

On firmware version 7.8.0-or-newer HSM partitions, the partition always has at least one domain, and can have as many as three, any of which can be a password-style text domain, or a multi-factor quorum type (PED key-secret domain. One of the three possible domains is designated primary, and is the first one looked at when a cloning/migration operation is attempted.

If a firmware version 7.8.0-or-newer target is already a member of the same domain as a pre-7.8.0 firmware source partition, and that domain is primary on the v7.8.0-or-newer partition, then cloning/migration can proceed straightaway.

If the target HSM partition is at firmware 7.8.0 or newer, then if its partition initially has a different domain from the source partition, the target partition can:

- use Extended Domain Management to add the source partition's domain as one of the three domains that the target can support and
- make the domain that was obtained from the source become the primary domain on the target by using the **-primary** option when adding a domain with "partition domainadd" on the previous page, and
- cloning/migration can proceed (includes backup, HA, etc.).

> **NOTE** This extended domain management command requires minimum Luna HSM Client 10.5.0 and Luna HSM Firmware 7.8.0 (command not visible for HSMs with prior firmware versions).
>
> Partition PO role login is required, to create or change a domain (after the first domain created by partition initialization). This command requires that **partition policy 44:** Allow Extended Domain Management is set to ON.

See also Considerations When Cloning / Copying Between Domains.

Syntax

partition domainadd {**-domain** <string> | [**-domainped**} [**-domainlabel** <string>] [**-primary**]

Argument(s)	Shortcut	Description
-domain <domain>	**-d**	Partition domain string for password-authenticated partitions. If this is omitted, then a connected PED with a domain on a PED key is expected.

Argument(s)	Shortcut	Description
-domainlabel <label>	**-dl**	Partition domain label - to distinguish among domains when a partition has more than one, and to match with domains on other partitions.
-domainped	**-dped**	Partition domain from a PED key.
-primary	**-p**	Mark this domain as primary (always used for the older cloning protocols, prior to CPv4)

Example with password-authentication

```
lunacm:> partition domainadd -domain seconddomain -domainlabel brotherdaryl

 Command Result : No Error
```

Example with multifactor quorum PED authentication

```
lunacm:>par domainadd -domainped -domainlabel NewPEDDomain

Please attend to the PED.

Command Result : No Error

lunacm:>par domainlist

Domain List
Domain Label[0]: PrimaryPED - primary KCV
Domain Label[1]: Label not set
Domain Label[2]: NewPEDDomain

Command Result : No Error
```

Example - add an unlabeled domain while existing domain does not have a label (PED authentication)

```
lunacm:>par domainlist

Domain List
Domain Label[0]: PrimaryPED - primary KCV
Domain Label[1]: Label not set
Domain Label[2]: Domain not created

Command Result : No Error

lunacm:>par domainadd -domainped

Please attend to the PED.

Error in execution: CKR_DATA_INVALID.
```

```
Command Result : 0x20 (CKR_DATA_INVALID)

lunacm:>
```

That attempt failed because it would have resulted in two domains with the same label "Label not set".

Example - add a third domain while second does not have a label (PED authentication)

```
lunacm:>par domainlist

Domain List
Domain Label[0]: PrimaryPED - primary KCV
Domain Label[1]: Label not set
Domain Label[2]: Domain not created

Command Result : No Error

lunacm:>par domainadd -domainped -domainlabel NewPEDDomain

Please attend to the PED.

Command Result : No Error

lunacm:>par domainlist

Domain List
Domain Label[0]: PrimaryPED - primary KCV
Domain Label[1]: Label not set
Domain Label[2]: NewPEDDomain

Command Result : No Error>
```

This attempt succeeds because the proposed -domainlabel is different from the two existing labels "PrimaryPED" and "Label not set".

Example - add a password-authenticated domain to a PED-authenticated HSM partition

> **NOTE** The commands for this operation are the same as those for adding a password-authenticated domain to a password-authenticated HSM partition. The only difference is that you must attend to the PED commands and use a blue PED key to sign in as HSM SO.

```
lunacm:> partition domainlist

        Number of supported domains 3
        Defined Domain
                Domain #1 with label "DM1". Defined as primary domain.
lunacm:> partition domainadd -domain Domain #2 -domainlabel DM2

Command Result : No Error
lunacm:> partition domainlist
        Number of supported domains 3
        Defined Domains
                Domain #1 with label "DM1". Defined as primary domain.
```

```
                Domain #2 with label "DM2".

Command Result : No Error
```

Example - add a PED-authentication domain to a password-authenticated HSM partition

> **NOTE** The simplest way to share a common domain between a PED-authenticated and password-authenticated HSM partition is to copy the domain from the password-authenticated to the PED-authenticated HSM partition, as this does not require a PED connection to the password-authenticated HSM. If, however, you wish to clone a domain from a PED-authenticated to a password-authenticated HSM partition, you will have to do so while you have local access to the password-authenticated HSM. Initiating this procedure causes the password-authenticated HSM to prompt for a red PED Key containing the domain secret, which requires the PED to be connected locally to the target password-authenticated HSM.

```
lunacm:> partition domainlist

        Number of supported domains 3
        Defined Domain
                Domain #1 without label. Defined as primary domain.

Command Result : No Error
lunacm:> partition domainadd -domainped -domainlabel PEDdomain
        Please attend to the PED.
lunacm:> partition domainlist
        Number of supported domains 3
        Defined Domains
                Domain #1 without label. Defined as primary domain.
                Domain #2 with label "PEDdomain".

Command Result : No Error
```

partition domainchangelabel

The **partition domainchangelabel** command changes the domain label of an existing domain.

Which domain is primary and how to change - All partitions, after initialization, have the current or original security/cloning domain marked as the primary, the domain that is chosen by default for cloning. For a partition with more than one domain, either of the others can be designated as primary, instead, using the **partition domainadd** and **partition domainchangelabel** commands, by invoking their **-primary** option.

A partition is initialized *without* a domain label (default to comply with pre-firmware-7.9.2), or optionally *with* a domain label (1 to 32 characters).

> **CAUTION!** Domain secret strings for password-authenticated HSMs and Luna Cloud HSMs are used to generate the secret key for cloning, and are as cryptographically sensitive as a user password. The domain label associated with a domain string is not sensitive, and is used only to distinguish the domain from others assigned to the same partition. ***Never use the same string for the domain* label *and for the domain* secret.**

Where the domain label framework is in effect (Luna HSM Firmware 7.8.0 and newer with Luna HSM Client 10.5.0 and newer):

- pre-firmware-7.8.0 partitions that are updated to Luna HSM Firmware 7.8.0 or newer can have an existing domain that is unlabeled and
  - can remain unlabeled with no consequence to your existing applications and processes
  - can have a domain label applied with the **partition domainchangelabel** command
- new partitions created under Luna HSM Firmware 7.8.0 can be initialized
  - without a domain label for continuity with your existing applications and processes
  - with a domain label that can remain as-is
  - can have a label added or changed later with the **partition domainchangelabel** command
- new partitions created with Luna HSM Firmware 7.8.0 or newer, can have up to two additional domains added (typed for password-authenticated, or imported from a red PED keyy for multifactor quorum-authenticated), and the **partition domainchangelabel** command can ensure that the labels are applied/adjusted
  - to enforce that no two domain labels would be identical (which prevents adding of a new domain label)
  - to identify for which other HSM partition each additional label was added (created or imported)

> **NOTE** This extended domain management command requires minimum Luna HSM Client 10.5.0 and Luna HSM Firmware 7.8.0 (command not visible for HSMs with prior firmware versions).

> **NOTE** The "partition domainchangelabel" on the previous page command is visible as soon as the partition is created.
>
> You must be logged in as partition SO (po) to run this command, which implies that the partition must first be initialized.
>
> This command does **not** require partition policy 44 to be set.

Primary domain - On pre-firmware 7.8.0 HSM partitions the single possible domain is effectively the primary domain. For firmware 7.8.0 or newer, partitions can have as many as three domains. Of the three possible, one domain is always primary, but the status of primary can be moved to another domain if needed. "Primary" in this context means "the one that is tried first". If there is no match for the primary domain on the source partition, the systems goes on to try for other matching domains.

[**Summary**]

When cloning from a partition of an HSM with a firmware version lower than 7.8.0 to a version 7.8.0 or higher with multiple domains, the primary domain is used.

[**Explanation**]

On firmware version 7.8.0-or-newer HSM partitions, the partition always has at least one domain, and can have as many as three, any of which can be a password-style text domain, or a multi-factor quorum type (PED key-secret domain. One of the three possible domains is designated primary, and is the first one looked at when a cloning/migration operation is attempted.

If a firmware version 7.8.0-or-newer target is already a member of the same domain as a pre-7.8.0 firmware source partition, and that domain is primary on the v7.8.0-or-newer partition, then cloning/migration can proceed straightaway.

If the target HSM partition is at firmware 7.8.0 or newer, then if its partition initially has a different domain from the source partition, the target partition can:

- use Extended Domain Management to add the source partition's domain as one of the three domains that the target can support and
- make the domain that was obtained from the source become the primary domain on the target by using the **-primary** option when adding a domain with "partition domainadd" on page 154, and
- cloning/migration can proceed (includes backup, HA, etc.).

Syntax

partition domainchangelabel -oldlabel <label> **-newlabel** <label> **-force**

Argument(s)	Shortcut	Description
-force	**-f**	Change the domain label without asking for confirmation.
-newlabel <label>	**-nl**	The new label to assign to the domain.
-oldlabel <label>	**-ol**	The old label of the domain you wish to change.

Example - apply a domain label to a partition that was initialized without one

```
lunacm:>par init -label myPEDpar

You are about to initialize the partition.

Are you sure you wish to continue?

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

Please attend to the PED.

Command Result : No Error

lunacm:>par domainlist

        Number of supported domains 3
        Defined Domain
                Domain #1 without label. Defined as primary domain.

Command Result : No Error

lunacm:> partition domainchangelabel

        The partition SO must be logged in.

Error in execution: command cancelled.

Command Result : 0xb (User Cancelled Operation)


lunacm:> role login -name po


        enter password: ********


Command Result : No Error
```

Now you can rename the first partition's domainlabel.

```
lunacm:>par domainchangelabel -nl PrimaryPED

Command Result : No Error

lunacm:>par domainlist

Domain List
Domain Label[0]: PrimaryPED - primary KCV
Domain Label[1]: Domain not created
Domain Label[2]: Domain not created

Command Result : No Error
```

Example - change a password-authenticated domain label

```
lunacm:>par domainlist

Domain List
Domain Label[0]: PrimaryPED - primary KCV
Domain Label[1]: Label not set
Domain Label[2]: NewPEDDomain

Command Result : No Error

lunacm:>par domainchangelabel -nl MiddledPW
Command Result : No Error

lunacm:>par domainlist

Domain List
Domain Label[0]: PrimaryPED - primary KCV
Domain Label[1]: MiddledPW
Domain Label[2]: NewPEDDomain

Command Result : No Error
```

Example - change a multifactor quorum-authenticated domain label

```
lunacm:>par domainlist

Domain List
Domain Label[0]: PrimaryPED - primary KCV
Domain Label[1]: Label not set
Domain Label[2]: NewPEDDomain

Command Result : No Error

lunacm:>par domainchangelabel -nl MiddledPED

Command Result : No Error

lunacm:>par domainlist

Domain List
Domain Label[0]: PrimaryPED - primary KCV
Domain Label[1]: MiddledPED
Domain Label[2]: NewPEDDomain

Command Result : No Error
```

The action is the same as for a password-authenticated partition, no PED action is needed for a label change

partition domaindelete

The **partition domaindelete** command deletes an existing domain from the current partition.

A partition is initialized with a domain, but *without* a domain label (default to comply with pre-firmware-7.8.0), or optionally with a domainlabel if one is specified .

In the domain label framework (Luna HSM Firmware 7.8.0 and newer with Luna HSM Client 10.5.0 and newer):

> the *original* domain, assigned to the partition at initialization
  - can be renamed (or have a domain label added) with the **partition domainchangelabel** command, but
  - cannot be deleted without deleting the partition, whether or not that original domain has a domain label

> a domain added to the partition *without a domain label*
  - can be deleted without need to specify a label,

> a domain added to the partition *with a domain label* (or with a label applied later by the **partition domainchangelabel** command)
  - can be deleted if that domain's label is provided in the **partition domaindelete** command, whether it is the only added domain or it is one of two added domains
  - If a domain is deleted, this implies that at least one remains; any object that was cloned in with a domain that is then deleted remains usable in the partition, and can be cloned to another HSM/partition that shares a domain still associated with this current partition.

NOTE

> This extended domain management command requires minimum Luna HSM Client 10.5.0 and Luna HSM Firmware 7.8.0 (command not visible for HSMs with prior firmware versions).

> Partition PO role login is required, to create or change a domain (after the first domain created by partition initialization). This command requires that **partition policy 44:** Allow Extended Domain Management is set to ON.

Syntax

partition domaindelete [**-domainlabel** <string>] **-force**

Argument(s)	Shortcut	Description
-domainlabel <label>	**-dl**	Partition domain label identifies the domain to be deleted from the partition.
-force	**-f**	Force the action with no prompts.

Example

```
lunacm:>partition domaindelete

Domains
```

```
Domain #1 with label "4th".
Domain #2 with label "5th".

Enter the domain number to delete: 1

You are about to delete domain #1
Are you sure you wish to continue?

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

Command Result : No Error
```

partition domainlist

Display a list of the domains available in the current slot.

> **NOTE** This extended domain management command requires minimum Luna HSM Client 10.5.0 and Luna HSM Firmware 7.8.0 (command not visible for HSMs with prior firmware versions).

> **NOTE** The "partition domainlist" above command is visible as soon as the partition is created. No login is needed to run this command; it can be used as soon as the partition is initialized. This command does **not** require partition policy 44 to be set.

Syntax

partition domainlist

Example before partition is initialized

```
lunacm:> partition domainlist

        Number of supported domains 3
        No Domain has been defined


Command Result : No Error
```

Example with no labels

```
lunacm:> partition domainlist

        Number of supported domains 3
        Defined Domain
                Domain #1 without label. Defined as primary domain.


Command Result : No Error
```

Example with original domain labeled

```
lunacm:> partition domainlist

        Number of supported domains 3
        Defined Domain
                Domain #1 with label "original". Defined as primary domain.

Command Result : No Error
```

Example with all domains labeled

```
lunacm:> partition domainlist

        Number of supported domains 3
```

```
        Defined Domains
                Domain #1 with label "original". Defined as primary domain.
                Domain #2 with label "seconddomain".
                Domain #3 with label "thirddomain".

Command Result : No Error
```

partition init

Initialize an application partition. This command is used within the partition being initialized.

For password-authenticated HSMs, if the password is not provided via the command line, the user is interactively prompted for it. Input is echoed as asterisks, and user is asked for password confirmation. This creates the Partition Security Officer role.

For multifactor quorum-authenticated HSMs, PED action is required, and a Partition SO PED key (blue) is imprinted. Any password provided at the command line is ignored.

> **CAUTION!** VERIFY SUCCESSFUL PARTITION CREATION BEFORE PROCEEDING
> Partition initialization can partially fail during domain creation, without obvious notification, due to timeouts during the multi-step process, which can happen:
>
> - with larger MofN split quantities (multiple PED iKeys per domain secret), or
> - if the Luna PED times out, or
> - if the PED is disconnected during the process.
>
> This can leave the partition in a state where keys can be created, but cannot be copied out or in (no HA, no backup, no direct cloning command).
>
> A similar failure is possible but unlikely with password-authenticated HSM partitions.
>
> **Mitigation**
>
> Following partition initialization, run lunacm:> "partition showinfo" on page 177. Successful initialization can be confirmed by verifying that **TOKEN_KCV_CREATED** appears in the **Extended Token Flags** on V1 partition or in the second Token Flags on V0 partition.
>
> If that flag is not present, then do not use the partition - delete it and create a new one with the same name.
>
> **Workaround**
>
> 1. Update the HSM Firmware to 7.8.x or newer.
> 2. Enable partition policy 44: Allow Extended Domain Management.
> 3. Add the same cloning domain ped key as a domain using "partition domainadd" on page 154 command.
>
> After this, cloning is successful.

Domain matching and the default domain

If you do not specify a domain in the command line, you are prompted for it.

If you type a character string at the prompt, that string becomes the domain for the partition.

When you run the **partition backup** command, you are again prompted for a domain for the target partition on the backup HSM. You can specify a string at the command line, or omit the parameter at the command line and specify a string when prompted. Otherwise press **Enter** with no string at the prompt to apply the default domain. The domain that you apply to a backup HSM must match the domain on your source HSM partition.

Syntax

partition init -label <string> [**-password** <your_unique_password_for_pso>] [**-domain** <string>] [**-applytemplate** <filepath/filename>] [**-domainlabel**] [**-importpeddomain**] [**-defaultdomain**] [**-auth**] [**-force**]

Argument(s)	Shortcut	Description
-applytemplate <filepath/filename>	**-at**	Apply a policy template located in the specified directory. This feature requires minimum Luna HSM Firmware 7.1.0 and Luna HSM Client 7.1.0. **NOTE** If there is a mismatch between template policies and the default values of newer or dependent policies, then the attempt to apply the old policy would fail with CKR_FAILED_DEPENDENCIES. You have the option to edit a policy file before applying it, to add newer policies.
-auth	**-a**	Log in after the initialization.
-defaultdomain	**-def**	This option is deprecated. It applies to password-authenticated HSMs only. It allows you to set a default domain that is compatible with certain legacy HSMs, instead of specifying a unique domain string with **-domain**. Using a default domain secret means that key cloning and backup/restore operations are protected by Crypto Officer authentication only.
-domain	**-d**	Partition cloning domain string. Used only on password-authenticated HSMs; ignored for multifactor quorum-authenticated. The domain secret allows for two layers of cloning security: > The Partition SO determines which partitions can clone objects to each other by setting the same domain on the source and destination partitions. > The Crypto Officer for the partition must authorize the cloning operation. The domain string must be 1-128 characters in length. The following characters are allowed: `abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789 !@#$%^*-_=+[]{}()/:',.~` The following characters are problematic or invalid and must not be used in a domain string: `"&;<>?\`|` Spaces are allowed, as long as the leading character is not a space; to specify a domain string with spaces using the **-domain** option, enclose the string in double quotation marks. For password-authenticated HSMs, the domain string should match the complexity of the partition password. See Domain Planning for more information.

Argument(s)	Shortcut	Description
-domainlabel <string>	**-dl**	Partition domain label. Optional. > Used when initializing password-authenticated or multifactor quorum-authenticated partitions. > Requires Luna HSM Firmware 7.8.0 or newer and Luna HSM Client 10.5.0 or newer, • for use in conjunction with Extended Domain Management (partition domain|list|add|changelabel|delete commands) • facilitates the ability of a partition to have multiple cloning domains. > Can be added later, if desired.
-force	**-f**	Force the action (useful for scripting).
-importpeddomain	**-i**	Import the secret from a red domain PED key to initialize the domain on a Luna Cloud HSM service. This feature allows you to clone objects between Luna Cloud HSM and multifactor quorum-authenticated application partitions. **NOTE** This option was introduced in Luna HSM Client 10.4.1, and removed in Luna HSM Client 10.6.0 and newer. For newer client versions, Thales recommends using Universal Cloning to manage cloning between multifactor quorum-authenticated Luna HSMs and Luna Cloud HSM. This option is available only when the current slot is a Luna Cloud HSM service. All multifactor quorum-authenticated firmware versions are currently compatible with Luna Cloud HSM.
-label	**-l**	Label for the partition. In LunaCM, the partition label created during initialization must be 1-32 characters in length. If you specify a longer label, it will automatically be truncated to 32 characters. The following characters are allowed: `abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789 !@#$%^&*()-_=+[]{}|/;:',.<>`~` Spaces are allowed; enclose the label in double quotation marks if it includes spaces.

Argument(s)	Shortcut	Description
-password	**-p**	Partition Security Officer Password. Used only on password-authenticated HSMs; ignored for multifactor quorum-authenticated. Passwords and activation challenge secrets must be 8-255 characters in length. Spaces are allowed; to specify a password with spaces using command-line options, enclose the password in double quotation marks. The space character may not be used as the first character in a password. The following characters are allowed: `!#$%'()*+,-./0123456789:=? @ABCDEFGHIJKLMNOPQRSTUVWXYZ[]^_ abcdefghijklmnopqrstuvwxyz{}~` This character set is enforced when using Luna HSM Client 10.8.0 or newer, and recommended for all previous versions. Previously-set passwords and challenge secrets are unaffected, but the new character set is enforced when these passwords are changed.

Example

```
lunacm:> partition init -label par2

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

        Are you sure you wish to continue?

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

        Enter password for Partition SO: ********

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

        Option -domain was not specified.  It is required.

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

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

Command Result : No Error
```

 Copyright 2001-2026 Thales Group

partition login

Log in to an HA group using the common Crypto Officer password or challenge secret. This command is available in LunaCM only when the current slot is an HA virtual slot.

Syntax

partition login [**-password** <password/challenge>]

Argument(s)	Shortcut	Description
-password <password/challenge>	**-pa**	Specifies the Crypto Officer password or challenge secret for the HA group. If you do not specify this parameter, you are prompted to enter the password (masked by asterisks).

Example

```
lunacm:> partition login

        Option -password was not supplied.  It is required.


        Enter the password: ********

Command Result : No Error
```

partition logout

Log out of an HA group. This command is only available in LunaCM when the current slot is an HA virtual slot.

Syntax

partition logout

Example

```
lunacm:> partition logout

Command Result : No Error
```

partition logoutother

Log a user out of all sessions other than the current one. You must be logged in as the Crypto Officer.

Syntax

partition logoutother [-name]

Argument(s)	Shortcut	Description
-name	**-n**	Specifies the role you want to log out of other sessions.

Example

```
lunacm:> partition logoutother -name co

Command Result : No Error
```

partition resize

Change the size of an application partition.

> **NOTE** This command is not applicable on DPoD Luna Cloud HSM services.

Syntax

partition resize -slot <number> **-size** <bytes> {**-partition** <name> | **-all**} [**-force**]

Argument(s)	Shortcut	Description
-all	**-a**	Resize all partitions on the backup HSM.
-force	**-f**	Force the action without prompting for confirmation.
-partition <name>	**-par**	The name of the affected partition.
-size <bytes>	**-si**	The desired size (in bytes) of the partition.
-slot <number>	**-sl**	The slot where the partition is located.

Example

To see information about a partition/slot, go to that slot using **slot set** and then use the **partition showinfo** command.

```
lunacm:>partition archive list -slot 2

        HSM Storage Information for slot 2:

          Total HSM Storage Space: 16252928
          Used HSM Storage Space:  206732
          Free HSM Storage Space:  16046196
          Allowed Partitions:      2
          Number Of Partitions:    3

        Partition list for slot 2

          Number of partition: 2

          Name:                    backup1
          Total Storage Size:      132
          Used Storage Size:       0
          Free Storage Size:       132
          Number Of Objects:       0

          Name:                    backup2
          Total Storage Size:      132
          Used Storage Size:       0
          Free Storage Size:       132
          Number Of Objects:       0
```

```
Command Result : No Error


lunacm:>slot set slot 2

        Current Slot Id: 2 (Luna G5 6.10.9 (PED) Backup Device)

Command Result : No Error


lunacm:>hsm login

        Please attend to the PED.

Command Result : No Error


lunacm:>partition resize -slot 2 -size 100000 -partition backup1

        This command will resize the user partition(s).
        Are you sure you wish to continue?

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

Command Result : No Error


lunacm:>partition archive list -slot 2

        HSM Storage Information for slot 2:

          Total HSM Storage Space: 16252928
          Used HSM Storage Space:  306600
          Free HSM Storage Space:  15946328
          Allowed Partitions:      20
          Number Of Partitions:    3

        Partition list for slot 2

          Number of partition: 2

          Name:                        backup1
          Total Storage Size:          100000
          Used Storage Size:           0
          Free Storage Size:           100000
          Number Of Objects:           0

          Name:                        backup2
          Total Storage Size:          132
          Used Storage Size:           0
          Free Storage Size:           132
          Number Of Objects:           0

Command Result : No Error
```

partition restoresim3file

Restore/insert HSM information from a SIM3 backup file. All objects in the file are restored to the HSM.

> **NOTE** This command applies to Luna 6.x partitions only. SIM is not supported by Luna 7 or Luna Cloud HSM service.

Syntax

partition restoresim3file -filename <input_file>

Argument(s)	Shortcut	Description
-filename <input_file>	**-fi**	The name of the backup file on your computer, from which the restore operation is performed.

Example

```
lunacm:>partition restoresim3file -filename somepartfile

        Restored Objects:

        Object Handle: 14 (0xe)
        Object Class: CKO_SECRET_KEY
        Key Type: CKK_DES3
        Label: Generated DES3 Key

        Object Handle: 20 (0x14)
        Object Class: CKO_SECRET_KEY
        Key Type: CKK_DES3
        Label: Generated DES3 Key

        Object Handle: 30 (0x1e)
        Object Class: CKO_SECRET_KEY
        Key Type: CKK_DES2
        Label: Generated DES2 Key

        Object Handle: 31 (0x1f)
        Object Class: CKO_SECRET_KEY
        Key Type: CKK_AES
        Label: Generated AES Key

        Object Handle: 32 (0x20)
        Object Class: CKO_PRIVATE_KEY
        Key Type: CKK_RSA
        Label: Generated RSA Private Key

Command Result : No Error
```

 Copyright 2001-2026 Thales Group

partition setlegacydomain

Set the legacy (Luna 4.x) cloning domain on a Luna 7 partition for the purposes of key migration:

- The legacy cloning domain for password-authenticated HSM partitions is the text string that was used as a cloning domain on the legacy HSM whose contents are to be migrated to the Luna PCIe HSM 7 partition.
- The legacy cloning domain for multifactor quorum-authenticated HSM partitions is the cloning domain secret on the red PED key for the legacy multifactor quorum-authenticated HSM whose contents are to be migrated to the Luna PCIe HSM 7 partition.

Your target HSM partition has, and retains, whatever modern partition cloning domain was imprinted (on a red PED key) when the partition was created. This command takes the domain value from your legacy HSM's red PED key and associates that with the modern-format domain of the partition, to allow the partition to be the cloning (restore...) recipient of objects from the legacy (token) HSM.

You cannot migrate objects from a password-authenticated token/HSM to a multifactor quorum-authenticated HSM partition, and you cannot migrate objects from a multifactor quorum-authenticated token/HSM to a password-authenticated HSM partition. Again, this is a security provision.

See About the Key Migration Guide for information on the possible combinations of source (legacy) tokens/HSMs and target (modern) HSM partitions and the disposition of token objects from one to the other.

> **NOTE** You can use this command repeatedly to associate different legacy domains to the current partition's cloning domain. This allows you to consolidate content from multiple legacy HSMs onto a single partition of a modern HSM.
>
> This command is not applicable on DPoD Luna Cloud HSM services.

Syntax

partition setlegacydomain [**-legacydomain** <legacystring>] [**-force**]

Argument(s)	Shortcut	Description
-force	**-f**	Force action without prompting for confirmation.
-legacydomain <legacystring>	**-ld**	Legacy cloning domain string. This parameter must be specified for password-authenticated HSMs. It is optional for PED authenticated HSMs. If not specified, the domain is obtained using the PED.

Example

```
lunacm:> partition setlegacydomain

        Existing Legacy Cloning Domain will be destroyed.
        Are you sure you wish to continue?

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

The PED prompts for the legacy red domain PED key (notice mention of "raw data" in the PED message).

```
Command result: No Error
```

partition showinfo

Display partition-level information for the current slot. The output from this command varies depending on the type of partition in the current slot.

Syntax

partition showinfo

> **NOTE** **The Partition Status** field indicates the state of the partition. The value **L3 Device** means that the partition is following FIPS L3 guidelines. The other possible values are **L3 Device, Tampered**; **L3 Device, Transport Mode**; **L3 Device, Zeroized**; and **L3 Device, Decommissioned**. Each represents a possible partition state.

Examples

Partition Info for an HSM admin partition

```
lunacm:> hsm showinfo

        Partition Label -> myPCIeHSM
        Partition Manufacturer -> SafeNet
        Partition Model -> Luna K7
        Partition Serial Number -> 67842
        Partition Status -> L3 Device
        HSM Part Number -> 808-000048-002
        HSM Serial Number -> 67842
        Token Flags ->
                CKF_RNG
                CKF_RESTORE_KEY_NOT_NEEDED
                CKF_TOKEN_INITIALIZED
        RPV Initialized -> No
        Slot Id -> 16
        Session State -> CKS_RW_SO_FUNCTIONS
        Role Status ->   SO logged in

        Partition SMK OUIDs:
                SMK-FW4: Not Initialized
                SMK-FW6: Not Initialized
                SMK-FW7-FM: Not Initialized
                SMK-FW7-Rollover: Not Initialized
                SMK-FW7-Primary: 2a0000003a00000102090100

        Extended Token Flags ->
                TOKEN_KCV_CREATED
        Partition OUID -> 00000000000000002090100

        Partition Storage:
                Total Storage Space:  655360
                Used Storage Space:   0
                Free Storage Space:   655360
                Object Count:         0
                Overhead:             16192
```

```
        *** The HSM is NOT in FIPS approved operation mode. ***

        FM HW Status -> FM Ready
        Firmware Version -> 7.8.4
        Bootloader Version ->  1.1.5
        Rollback Firmware Version -> 7.4.2

        System Times:
                HSM  : Wed Nov 27 20:20:21 UTC 2024
                Host : Wed Nov 27 20:20:21 UTC 2024
                Difference: 0 sec

        Environmental:
                Fan 1 Status                            : active
                Fan 2 Status                            : active
                Battery Voltage                         : 3.093 V
                Battery Warning Threshold Voltage       : 2.750 V
                System Temp                             : 64 deg. C
                System Temperature Warning Threshold    : 75 deg. C

        HSM Storage:
                Total Storage Space:  67108864
                Used Storage Space:   7315283
                Free Storage Space:   59793581
                Allowed Partitions:   1
                Number of Partitions: 1

        License Count:
                1. 621000068-000 Test Cert : K7 Base
                2. 621010185-003 Key backup via cloning protocol
                3. 621000138-001 Controlled tamper recovery
                4. 621000134-002 Enable 64 megabytes of object storage
                5. 621000021-002 Maximum performance
                6. 621000135-002 Enable allow decommissioning
                7. 621000154-001 Enable decommission on tamper with policy off


Command Result : No Error
```

> **NOTE** The **System Times** field does not appear until the HSM time has been synchronized with the host system using lunacm:> "hsm time sync" on page 101.

Partition Info for an application partition (pre-f/w 7.7)

```
lunacm:> partition showinfo

        Partition Label -> par0
        Partition Manufacturer -> Safenet, Inc.
        Partition Model -> LunaSA 7.0.0
        Partition Serial Number -> 154438865317
        Partition Status -> L3 Device
        HSM Part Number -> 808-000048-002
        Token Flags ->
                CKF_LOGIN_REQUIRED
                CKF_USER_PIN_INITIALIZED
                CKF_RESTORE_KEY_NOT_NEEDED
                CKF_TOKEN_INITIALIZED
```

```
        RPV Initialized -> Not Supported
        Slot Id -> 0
        Session State -> CKS_RW_PUBLIC_SESSION
        Role Status ->   none logged in
        Token Flags ->
                TOKEN_KCV_CREATED
        Partition OUID: 01010000090000061b030100

        Partition Storage:
                Total Storage Space:  324096
                Used Storage Space:   0
                Free Storage Space:   324096
                Object Count:         0
                Overhead:             9648

        *** The partition is NOT in FIPS 140-2 approved operation mode. ***


Command Result : No Error
```

Partition info for a V1 partition (f/w 7.7.0 or newer)

```
lunacm:> partition showinfo

        Partition Label -> myPCIePar
        Partition Manufacturer -> SafeNet
        Partition Model -> Luna K7
        Partition Serial Number -> 157956935657
        Partition Status -> L3 Device
        HSM Part Number -> 808-000048-002
        HSM Serial Number -> 67842
        Token Flags ->
                CKF_RNG
                CKF_LOGIN_REQUIRED
                CKF_USER_PIN_INITIALIZED
                CKF_RESTORE_KEY_NOT_NEEDED
                CKF_TOKEN_INITIALIZED
        RPV Initialized -> No
        Slot Id -> 6
        Session State -> CKS_RW_PUBLIC_SESSION
        Role Status ->   none logged in

        Partition SMK OUIDs:
                SMK-FW4: Not Initialized
                SMK-FW6: Not Initialized
                SMK-FW7-FM: Not Initialized
                SMK-FW7-Rollover: Not Initialized
                SMK-FW7-Primary: 320000003a00000102090100

        Extended Token Flags ->
                TOKEN_KCV_CREATED
        Partition OUID -> 2b0000003a00000102090100

        Partition Storage:
                Total Storage Space:  6627739
                Used Storage Space:   84480
                Free Storage Space:   6543259
                Object Count:         256
```

```
                Overhead:             15992


        *** The HSM is NOT in FIPS approved operation mode. ***

        FM HW Status -> FM Ready
        Firmware Version -> 7.8.4
        Bootloader Version ->  1.1.5
        Rollback Firmware Version -> 7.4.2

        System Times:
                HSM  : Wed Nov 27 20:27:47 UTC 2024
                Host : Wed Nov 27 20:27:46 UTC 2024
                Difference: 1 sec

Command Result : No Error
```

NOTE

- The **System Times** field does not appear until the HSM time has been synchronized with the host system using lunacm:> "hsm time sync" on page 101.
- If you are migrating a Secure Master Key (SMK) from a Luna 6 HSM to a Luna 7 HSM, in addition to the SMK-FW6, the SMK-FW4 on the Luna 7 HSM is also overwritten by a new one (even if you have *not* initialized an SMK-FW4 on the Luna 6 HSM by a prior migration) and this command reports the presence of an SMK-FW4 on the Luna 7 HSM.

 Copyright 2001-2026 Thales Group

partition showmechanism

Lists the supported mechanisms, or shows some detail about a named mechanism.

Syntax

partition showmechanism [**-m** <mech_ID_number>]

Argument(s)	Short	Description
[no arguments]	**.**	Lists all available mechanisms.
-m <mech_ID_number>	**-m**	Shows expanded information for the indicated mechanism (optional), where <mech_ID_number> is a hex mechanism number either 4 or 8 digits long.

Example

List all mechanisms available to the partition

```
lunacm:> partition showmechanism


 Mechanisms Supported:
         0x00000000 - CKM_RSA_PKCS_KEY_PAIR_GEN
         0x00000001 - CKM_RSA_PKCS
         0x00000003 - CKM_RSA_X_509
         0x00000006 - CKM_SHA1_RSA_PKCS
         0x00000009 - CKM_RSA_PKCS_OAEP
         0x0000000a - CKM_RSA_X9_31_KEY_PAIR_GEN
         0x80000142 - CKM_RSA_FIPS_186_3_AUX_PRIME_KEY_PAIR_GEN
         0x80000143 - CKM_RSA_FIPS_186_3_PRIME_KEY_PAIR_GEN
         0x0000000b - CKM_RSA_X9_31
         0x0000000c - CKM_SHA1_RSA_X9_31
         0x80000135 - CKM_SHA224_RSA_X9_31
         0x80000136 - CKM_SHA256_RSA_X9_31
         0x80000137 - CKM_SHA384_RSA_X9_31
         0x80000138 - CKM_SHA512_RSA_X9_31
         0x8000013e - CKM_RSA_X9_31_NON_FIPS
         0x80000139 - CKM_SHA1_RSA_X9_31_NON_FIPS
         0x8000013a - CKM_SHA224_RSA_X9_31_NON_FIPS
         0x8000013b - CKM_SHA256_RSA_X9_31_NON_FIPS
         0x8000013c - CKM_SHA384_RSA_X9_31_NON_FIPS
         0x8000013d - CKM_SHA512_RSA_X9_31_NON_FIPS
         0x0000000d - CKM_RSA_PKCS_PSS
         0x0000000e - CKM_SHA1_RSA_PKCS_PSS
         :
         :
         0x00000391 - CKM_MD2_KEY_DERIVATION
         0x00000390 - CKM_MD5_KEY_DERIVATION
         0x00000392 - CKM_SHA1_KEY_DERIVATION
         0x00000350 - CKM_GENERIC_SECRET_KEY_GEN
         0x00000371 - CKM_SSL3_MASTER_KEY_DERIVE
         0x00000372 - CKM_SSL3_KEY_AND_MAC_DERIVE
```

 Copyright 2001-2026 Thales Group

```
         0x00000380 - CKM_SSL3_MD5_MAC
         0x00000381 - CKM_SSL3_SHA1_MAC
         0x00000221 - CKM_SHA_1_HMAC
         0x00000222 - CKM_SHA_1_HMAC_GENERAL
         0x00000211 - CKM_MD5_HMAC
         0x00000212 - CKM_MD5_HMAC_GENERAL
         0x00000370 - CKM_SSL3_PRE_MASTER_KEY_GEN
         0x80000140 - CKM_DSA_SHA224
         0x80000141 - CKM_DSA_SHA256
         0x80000a02 - CKM_NIST_PRF_KDF
         0x80000a03 - CKM_PRF_KDF

Command Result : No Error
```

Show information about a particular mechanism

```
lunacm:> partition showmechanism -m 80000142

(0x80000142 - -2147483326) CKM_RSA_FIPS_186_3_AUX_PRIME_KEY_PAIR_GEN
         Min Key Size 1024
         Max Key Size 3072
         Flags 0x10001
Command Result : No Error
```

partition showpolicies

Displays the partition-level capability and policy settings for the indicated user/application partition, including whether the policy is destructive when it is enabled or disabled (verbose mode). Only policies that the Partition SO can change (the corresponding capability is not set to **0**) are included in the output. Include the **-exporttemplate** option to export the current state of all partition policies to a partition policy template (PPT).

Policy template export is supported for application partitions only
The **partition showpolicies -exporttemplate** function is not supported for HSM admin partitions.

To export HSM-wide policies from HSMs connected locally to the HSM host, use the command "hsm showpolicies" on page 91 with the **-exporttemplate** option.

Multiple sessions and policy changes
If you are running more than one LunaCM session against the same partition, and change a partition policy in one LunaCM session, the policy change is reflected in that session only. You must exit and restart the other LunaCM sessions to display the changed policy settings.

Syntax

partition showpolicies [**-slot** <slot>] [**-verbose**] [**-exporttemplate** <filepath/filename>]

Argument(s)	Short	Description
-exporttemplate <filepath/filename>	**-et**	Export the current state of all partition policies to a policy template in the specified location. **NOTE** If there is a mismatch between template policies and the default values of newer or dependent policies, then the attempt to apply the old policy would fail with CKR_FAILED_DEPENDENCIES. You have the option to edit a policy file before applying it, to add newer policies.
-slot <slot>	**-s**	Specifies the slot number for which to display partition policy settings. If no slot is specified, the policies for the currently-active slot are displayed.
-verbose	**-v**	Include information that specifies whether the policy is destructive when enabled/disabled.

Examples

With -exporttemplate specified

```
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
```

Normal mode (pre-firmware 7.7.0)

```
lunacm:> partition showpolicies
        Partition Capabilities
                 0: Enable private key cloning : 1
                 1: Enable private key wrapping : 1
                 2: Enable private key unwrapping : 1
                 3: Enable private key masking : 0
                 4: Enable secret key cloning : 1
                 5: Enable secret key wrapping : 1
                 6: Enable secret key unwrapping : 1
                 7: Enable secret key masking : 0
                10: Enable multipurpose keys : 1
                11: Enable changing key attributes : 1
                15: Allow failed challenge responses : 1
                16: Enable operation without RSA blinding : 1
                17: Enable signing with non-local keys : 1
                18: Enable raw RSA operations : 1
                20: Max failed user logins allowed : 10
                21: Enable high availability recovery : 1
                22: Enable activation : 1
                23: Enable auto-activation : 1
                25: Minimum pin length (inverted: 255 - min) : 248
                26: Maximum pin length : 255
                28: Enable Key Management Functions : 1
                29: Enable RSA signing without confirmation : 1
                31: Enable private key unmasking : 1
                32: Enable secret key unmasking : 1
                33: Enable RSA PKCS mechanism : 1
                34: Enable CBC-PAD (un)wrap keys of any size : 1
                37: Enable Secure Trusted Channel : 1
                39: Enable  Start/End Date Attributes : 1

        Partition Policies
                 0: Allow private key cloning : 1
                 1: Allow private key wrapping : 0
                 2: Allow private key unwrapping : 1
                 4: Allow secret key cloning : 1
                 5: Allow secret key wrapping : 1
                 6: Allow secret key unwrapping : 1
                10: Allow multipurpose keys : 1
                11: Allow changing key attributes : 1
                15: Ignore failed challenge responses : 1
                16: Operate without RSA blinding : 1
                17: Allow signing with non-local keys : 1
                18: Allow raw RSA operations : 1
                20: Max failed user logins allowed : 10
```

```
                21: Allow high availability recovery : 1
                22: Allow activation : 0
                23: Allow auto-activation : 0
                25: Minimum pin length (inverted: 255 - min) : 248
                26: Maximum pin length : 255
                28: Allow Key Management Functions : 1
                29: Perform RSA signing without confirmation : 1
                31: Allow private key unmasking : 1
                32: Allow secret key unmasking : 1
                33: Allow RSA PKCS mechanism : 1
                34: Allow CBC-PAD (un)wrap keys of any size : 1
                37: Force Secure Trusted Channel : 0
                39: Allow Start/End Date Attributes : 0

Command Result : No Error
```

For Luna HSM Firmware 7.7.0 and newer, when viewed from an up-to-date Client, the command shows the newer Capabilities and Policies as well as the status of pre-existing policies that have new default settings like policies 3, 7, 31, and 32 for example, regardless of partition V0 or V1 status. However, older clients cannot see newer policies to display them. Newer clients show capabilities and policies for firmware <7.7.0 partitions as the older firmware presents them.

Verbose mode (pre-firmware 7.7.0)

```
lunacm:> partition showpolicies -verbose
        Partition Capabilities
                 0: Enable private key cloning : 1
                 1: Enable private key wrapping : 1
                 2: Enable private key unwrapping : 1
                 3: Enable private key masking : 0
                 4: Enable secret key cloning : 1
                 5: Enable secret key wrapping : 1
                 6: Enable secret key unwrapping : 1
                 7: Enable secret key masking : 0
                10: Enable multipurpose keys : 1
                11: Enable changing key attributes : 1
                15: Allow failed challenge responses : 1
                16: Enable operation without RSA blinding : 1
                17: Enable signing with non-local keys : 1
                18: Enable raw RSA operations : 1
                20: Max failed user logins allowed : 10
                21: Enable high availability recovery : 1
                22: Enable activation : 1
                23: Enable auto-activation : 1
                25: Minimum pin length (inverted: 255 - min) : 248
                26: Maximum pin length : 255
                28: Enable Key Management Functions : 1
                29: Enable RSA signing without confirmation : 1
                31: Enable private key unmasking : 1
                32: Enable secret key unmasking : 1
                33: Enable RSA PKCS mechanism : 1
                34: Enable CBC-PAD (un)wrap keys of any size : 1
                37: Enable Secure Trusted Channel : 1
                39: Enable  Start/End Date Attributes : 1

Partition Policies
                                                          Destructive
 Code Description                                  Value Off-To-On On-To-Off
```

```
  0   Allow private key cloning                        On      Yes       No
  1   Allow private key wrapping                       Off     Yes       No
  2   Allow private key unwrapping                     On      No        No
  4   Allow secret key cloning                         On      Yes       No
  5   Allow secret key wrapping                        On      Yes       No
  6   Allow secret key unwrapping                      On      No        No
  10  Allow multipurpose keys                          On      Yes       No
  11  Allow changing key attributes                    On      Yes       No
  15  Ignore failed challenge responses                On      Yes       No
  16  Operate without RSA blinding                     On      Yes       No
  17  Allow signing with non-local keys                On      No        No
  18  Allow raw RSA operations                         On      Yes       No
  20  Max failed user logins allowed                   10      N/A       N/A
  21  Allow high availability recovery                 On      No        No
  22  Allow activation                                 Off     No        No
  23  Allow auto-activation                            Off     No        No
  25  Minimum pin length (inverted: 255 - min)         248     N/A       N/A
  26  Maximum pin length                               255     N/A       N/A
  28  Allow Key Management Functions                   On      Yes       No
  29  Perform RSA signing without confirmation         On      Yes       No
  31  Allow private key unmasking                      On      No        No
  32  Allow secret key unmasking                       On      No        No
  33  Allow RSA PKCS mechanism                         On      Yes       No
  34  Allow CBC-PAD (un)wrap keys of any size          On      Yes       No
  37  Force Secure Trusted Channel                     Off     No        Yes
  39  Allow Start/End Date Attributes                  Off     No        Yes

Command Result : No Error
```

V0 Partition Example

```
lunacm:> partition showpolicies -verbose
        Partition Capabilities
                 0: Enable private key cloning : 1
                 1: Enable private key wrapping : 1
                 2: Enable private key unwrapping : 1
                 3: Enable private key masking : 1
                 4: Enable secret key cloning : 1
                 5: Enable secret key wrapping : 1
                 6: Enable secret key unwrapping : 1
                 7: Enable secret key masking : 1
                 9: Enable DigestKey : 1
                10: Enable multipurpose keys : 1
                11: Enable changing key attributes : 1
                15: Allow failed challenge responses : 1
                16: Enable operation without RSA blinding : 1
                17: Enable signing with non-local keys : 1
                18: Enable raw RSA operations : 1
                20: Max failed user logins allowed : 10
                21: Enable high availability recovery : 1
                22: Enable activation : 0
                23: Enable auto-activation : 0
                25: Minimum pin length (inverted: 255 - min) : 248
                26: Maximum pin length : 255
                28: Enable Key Management Functions : 1
                29: Enable RSA signing without confirmation : 1
```

```
31: Enable private key unmasking : 1
32: Enable secret key unmasking : 1
33: Enable RSA PKCS mechanism : 1
34: Enable CBC-PAD (un)wrap keys of any size : 1
37: Enable enforcing Secure Trusted Channel : 1
39: Enable Start/End Date Attributes : 1
40: Enable Per-Key Authorization Data : 1
41: Enable Partition Version : 1
```

Partition Policies

Code	Description	Value	Destructive Off-To-On	Destructive On-To-Off
0	Allow private key cloning	On	Yes	No
1	Allow private key wrapping	Off	Yes	No
2	Allow private key unwrapping	On	No	No
3	Allow private key masking	Off	Yes	No
4	Allow secret key cloning	On	Yes	No
5	Allow secret key wrapping	On	Yes	No
6	Allow secret key unwrapping	On	No	No
7	Allow secret key masking	Off	Yes	No
9	Allow DigestKey	Off	Yes	No
10	Allow multipurpose keys	On	Yes	No
11	Allow changing key attributes	On	Yes	No
15	Ignore failed challenge responses	On	Yes	No
16	Operate without RSA blinding	On	Yes	No
17	Allow signing with non-local keys	On	No	No
18	Allow raw RSA operations	On	Yes	No
20	Max failed user logins allowed	10	N/A	N/A
21	Allow high availability recovery	On	No	No
25	Minimum pin length (inverted: 255 - min)	248	N/A	N/A
26	Maximum pin length	255	N/A	N/A
28	Allow Key Management Functions	On	Yes	No
29	Perform RSA signing without confirmation	On	Yes	No
31	Allow private key unmasking	Off	No	No
32	Allow secret key unmasking	Off	No	No
33	Allow RSA PKCS mechanism	On	Yes	No
34	Allow CBC-PAD (un)wrap keys of any size	On	Yes	No
37	Force Secure Trusted Channel	Off	No	Yes
39	Allow Start/End Date Attributes	Off	No	Yes
40	Require Per-Key Authorization Data	Off	Yes	Yes
41	Partition Version	0	No	Yes

```
Command Result : No Error
```

V1 Partition Example

```
lunacm:> partition showpolicies -verbose
        Partition Capabilities
```

```
 0: Enable private key cloning : 1
 1: Enable private key wrapping : 1
 2: Enable private key unwrapping : 1
 3: Enable private key masking : 1
 4: Enable secret key cloning : 1
 5: Enable secret key wrapping : 1
 6: Enable secret key unwrapping : 1
 7: Enable secret key masking : 1
10: Enable multipurpose keys : 1
11: Enable changing key attributes : 1
15: Allow failed challenge responses : 1
16: Enable operation without RSA blinding : 1
17: Enable signing with non-local keys : 1
18: Enable raw RSA operations : 1
20: Max failed user logins allowed : 10
21: Enable high availability recovery : 1
22: Enable activation : 0
23: Enable auto-activation : 0
25: Minimum pin length (inverted: 255 - min) : 247
26: Maximum pin length : 255
28: Enable Key Management Functions : 1
29: Enable RSA signing without confirmation : 1
31: Enable private key unmasking : 1
32: Enable secret key unmasking : 1
33: Enable RSA PKCS mechanism : 1
34: Enable CBC-PAD (un)wrap keys of any size : 1
37: Enable enforcing Secure Trusted Channel : 1
39: Enable Start/End Date Attributes : 1
40: Enable Per-Key Authorization Data : 1
41: Enable Partition Version : 1
42: Enable CPv1 : 1
43: Enable non-FIPS algorithms : 1
```

Partition Policies

Code	Description	Value	Destructive Off-To-On	Destructive On-To-Off
0	Allow private key cloning	On	Yes	No
1	Allow private key wrapping	Off	Yes	No
2	Allow private key unwrapping	On	No	No
3	Allow private key masking	On	Yes	No
4	Allow secret key cloning	On	Yes	No
5	Allow secret key wrapping	On	Yes	No
6	Allow secret key unwrapping	On	No	No
7	Allow secret key masking	On	Yes	No
10	Allow multipurpose keys	On	Yes	No
11	Allow changing key attributes	On	Yes	No
15	Ignore failed challenge responses	On	Yes	No
16	Operate without RSA blinding	On	Yes	No
17	Allow signing with non-local keys	On	No	No
18	Allow raw RSA operations	On	Yes	No
20	Max failed user logins allowed	10	N/A	N/A
21	Allow high availability recovery	On	No	No
25	Minimum pin length (inverted: 255 - min)	248	N/A	N/A
26	Maximum pin length	255	N/A	N/A
28	Allow Key Management Functions	On	Yes	No

```
                29  Perform RSA signing without confirmation       On      Yes       No
                31  Allow private key unmasking                    On      No        No
                32  Allow secret key unmasking                     On      No        No
                33  Allow RSA PKCS mechanism                       On      Yes       No
                34  Allow CBC-PAD (un)wrap keys of any size        On      Yes       No
                37  Force Secure Trusted Channel                   Off     No        Yes
                39  Allow Start/End Date Attributes                Off     No        Yes
                40  Require Per-Key Authorization Data             On      Yes       Yes
                41  Partition Version                               1      No        Yes
                42: Allow CPv1                                      1      Yes       No
                43: Allow non-FIPS algorithms :                     1      Yes       No



Command Result : No Error
```

Firmware 7.8.0

```
lunacm:> partition showpolicies
        Partition Capabilities
                 0: Enable private key cloning : 1
                 1: Enable private key wrapping : 1
                 2: Enable private key unwrapping : 1
                 3: Enable private key masking : 1
                 4: Enable secret key cloning : 1
                 5: Enable secret key wrapping : 1
                 6: Enable secret key unwrapping : 1
                 7: Enable secret key masking : 1
                10: Enable multipurpose keys : 1
                11: Enable changing key attributes : 1
                15: Allow failed challenge responses : 1
                16: Enable operation without RSA blinding : 1
                17: Enable signing with non-local keys : 1
                18: Enable raw RSA operations : 1
                20: Max failed user logins allowed : 10
                21: Enable high availability recovery : 1
                22: Enable activation : 0
                23: Enable auto-activation : 0
                25: Minimum pin length (inverted: 255 - min) : 247
                26: Maximum pin length : 255
                28: Enable Key Management Functions : 1
                29: Enable RSA signing without confirmation : 1
                31: Enable private key unmasking : 1
                32: Enable secret key unmasking : 1
                33: Enable RSA PKCS mechanism : 1
                34: Enable CBC-PAD (un)wrap keys of any size : 1
                37: Enable enforcing Secure Trusted Channel : 1
                39: Enable Start/End Date Attributes : 1
                40: Enable Per-Key Authorization Data : 1
                41: Enable Partition Version : 1
                42: Enable CPv1 : 1
                43: Enable non-FIPS algorithms : 1
                44: Enable Extended Domain Management : 1

        Partition Policies
                 0: Allow private key cloning : 1
```

```
 1: Allow private key wrapping : 0
 2: Allow private key unwrapping : 1
 3: Allow private key masking : 0
 4: Allow secret key cloning : 1
 5: Allow secret key wrapping : 1
 6: Allow secret key unwrapping : 1
 7: Allow secret key masking : 0
10: Allow multipurpose keys : 1
11: Allow changing key attributes : 1
15: Ignore failed challenge responses : 1
16: Operate without RSA blinding : 1
17: Allow signing with non-local keys : 1
18: Allow raw RSA operations : 1
20: Max failed user logins allowed : 10
21: Allow high availability recovery : 1
25: Minimum pin length (inverted: 255 - min) : 247
26: Maximum pin length : 255
28: Allow Key Management Functions : 1
29: Perform RSA signing without confirmation : 1
31: Allow private key unmasking : 0
32: Allow secret key unmasking : 0
33: Allow RSA PKCS mechanism : 1
34: Allow CBC-PAD (un)wrap keys of any size : 1
37: Force Secure Trusted Channel : 0
39: Allow Start/End Date Attributes : 0
40: Require Per-Key Authorization Data : 0
41: Partition Version : 0
42: Allow CPv1 : 1
43: Allow non-FIPS algorithms : 1
44: Allow Extended Domain Management : 0


Command Result : No Error
```

Firmware 7.9.0

```
lunacm:> partition showpolicies
        Partition Capabilities
                 0: Enable private key cloning : 1
                 1: Enable private key wrapping : 1
                 2: Enable private key unwrapping : 1
                 3: Enable private key masking : 1
                 4: Enable secret key cloning : 1
                 5: Enable secret key wrapping : 1
                 6: Enable secret key unwrapping : 1
                 7: Enable secret key masking : 1
                10: Enable multipurpose keys : 1
                11: Enable changing key attributes : 1
                15: Allow failed challenge responses : 1
                16: Enable operation without RSA blinding : 1
                17: Enable signing with non-local keys : 1
                18: Enable raw RSA operations : 1
                20: Max failed user logins allowed : 10
                21: Enable high availability recovery : 1
                22: Enable activation : 0
                23: Enable auto-activation : 0
                25: Minimum pin length (inverted: 255 - min) : 247
                26: Maximum pin length : 255
```

```
            28: Enable Key Management Functions : 1
            29: Enable RSA signing without confirmation : 1
            31: Enable private key unmasking : 1
            32: Enable secret key unmasking : 1
            33: Enable RSA PKCS mechanism : 1
            34: Enable CBC-PAD (un)wrap keys of any size : 1
            37: Enable enforcing Secure Trusted Channel : 1
            39: Enable Start/End Date Attributes : 1
            40: Enable Per-Key Authorization Data : 1
            41: Enable Partition Version : 1
            42: Enable CPv1 : 1
            43: Enable non-FIPS algorithms : 1
            44: Enable Extended Domain Management : 1
            45: Enable ECDSA/RSA Prehash SigVer : 1

    Partition Policies
             0: Allow private key cloning : 1
             1: Allow private key wrapping : 0
             2: Allow private key unwrapping : 1
             3: Allow private key masking : 0
             4: Allow secret key cloning : 1
             5: Allow secret key wrapping : 1
             6: Allow secret key unwrapping : 1
             7: Allow secret key masking : 0
            10: Allow multipurpose keys : 1
            11: Allow changing key attributes : 1
            15: Ignore failed challenge responses : 1
            16: Operate without RSA blinding : 1
            17: Allow signing with non-local keys : 1
            18: Allow raw RSA operations : 1
            20: Max failed user logins allowed : 10
            21: Allow high availability recovery : 1
            25: Minimum pin length (inverted: 255 - min) : 247
            26: Maximum pin length : 255
            28: Allow Key Management Functions : 1
            29: Perform RSA signing without confirmation : 1
            31: Allow private key unmasking : 0
            32: Allow secret key unmasking : 0
            33: Allow RSA PKCS mechanism : 1
            34: Allow CBC-PAD (un)wrap keys of any size : 1
            37: Force Secure Trusted Channel : 0
            39: Allow Start/End Date Attributes : 0
            40: Require Per-Key Authorization Data : 0
            41: Partition Version : 1
            42: Allow CPv1 : 1
            43: Allow non-FIPS algorithms : 1
            44: Allow Extended Domain Management : 0
            45: Allow ECDSA/RSA Prehash SigVer : 1

Command Result : No Error
```

partition smkclone

Clone the Scalable Key Storage Masking Key (SMK) from the current slot to the target slot.

Always back up any SMK that you have created (with partition archive backup to an SKS Backup HSM), before performing an action that would overwrite that SMK, like partition smkClone or like partition archive restore from an SKS partition on an SKS Backup HSM. Failure to do so risks permanently losing any objects that are encrypted with that original SMK.

> **CAUTION!** This command overwrites the SMK in the target partition with the SMK from the source. If you have exported any objects using a particular SMK, that SMK must be backed up to a Backup HSM before you overwrite it with smkclone, or those exported objects become unusable and can never be recovered.

An SMK secret that is cloned from a source V1 HSM partition to a target V1 partition overwrites any pre-existing V1 SMK on the target partition. SMK secrets cloned from V0 partitions do not overwrite V1 SMK secrets, but are stored separately.

If you invoked scalable key storage (SKS) for your applications to create and store large numbers of keys, then the partition is V1. If you perform cloning operations (including HA) or Backup and Restore, see Cloning or Backup / Restore with SKS.

The following table shows possible migration paths for existing SMKs -- the leftmost column is possible sources, while the heading row across the top lists possible destinations, and the intersecting table cells are the possible result for each source-to-destination scenario.

Destination **Source**	**FM6 SKS appliance**	**FW6 SKS G5 Backup (6.25)**	**FW7.7 eIDAS G5 Backup (6.28)**	**FW<7.7 HSM**	**FW>=7.7**	**FM HSM FW>=7.7 Non-FM HSM**
FW6 SKS appliance	FW6 SMKs	FW6 SMKs	FW6 SMKs	No SMK support on target	Target has FM cert only	FW6 SMKs
FW6 SKS G5 Backup (6.25)	FW6 SMKs	FW6 SMKs	FW6 SMKs	No SMK support on target	Target has FM cert only	FW6 SMKs
FW7.7 eIDAS G5 Backup (6.28)	FW6 SMKs	FW6 SMKs	All SMKs (cloning protocol used by V1 partitions)	No SMK support on source/target	All SMKs (cloning protocol used by V1 partitions)	All SMKs (cloning protocol used by V1 partitions)
FW<7.7 HSM	No SMK support on source	No SMK support on source	No SMK support on source	No SMK support on target	No SMK support on source	No SMK support on source

Destination Source	FM6 SKS appliance	FW6 SKS G5 Backup (6.25)	FW7.7 eIDAS G5 Backup (6.28)	FW<7.7 HSM	FW>=7.7	FM HSM FW>=7.7 Non-FM HSM
FW7.7 FM HSM	Source has FM cert only	Source has FM cert only	All SMKs (cloning protocol used by V1 partitions)	No SMK support on target	All SMKs (cloning protocol used by V1 partitions)	All SMKs (FW7.7-Primary -> FW7.7-FM, FW7.7-Rollover dropped) (V1 partition)
FW7.7 Non-FM SKS HSM	Required cloning protocol not on target	Required cloning protocol not on target	All SMKs (cloning protocol used by V1 partitions)	No SMK support on target	Blocked by V1 cloning protocol	All SMKs (cloning protocol used by V1 partitions)

(**FW>=7.7** means Luna HSM Firmware 7.7.0 or newer)

> **NOTE** If a remote partition is involved (Network HSM) on either side of the SMK cloning operation, the HSM that contains the remote partition must have Network Replication enabled. See **HSM policy 16:** Allow network replication.

Syntax

partition smkClone -slot <slot number> **[-force] -password** <password>

Argument	Shortcut	Description
-force	**-f**	Force the action without prompting for confirmation (useful when scripting commands).
-password <password>	**-p**	Password of the target slot.
-slot <number>	**-sl**	Target slot to which the source SMK is to be cloned (overwriting any SMK that might already be in the target slot).

Example

```
lunacm:> partition smkclone -slot 4 -password <your_unique_password_for_co>
Logging in to target slot 4

Cloning the SMK.

The SMK was cloned successfully.
Command Result : No Error
```

partition smkrollover

This command, with the **-start** option, moves the current primary SMK to the Rollover location, and generates a new Primary SMK.

If you just wanted to generate a fresh SMK, and no external SKS blobs are encrypted with the previous SMK, then you can issue the comand again with the **-end** option, and the task is finished.

If you are performing a rollover of an active SMK (as you might do, in compliance with your organization's key-rotation policy), then - immediately after **partition smkrollover -start** - you would insert and re-extract all SKS blobs that are encrypted by the old SMK. The HSM recognizes which SMK was used to encrypt a blob, and if it is the rollover SMK (or an SMK from a previous HSM generation, currently in the appropriate 'legacy' SMK location), it uses that SMK for the insertion. [Re-]extraction always uses the Primary SMK.

When all desired blobs have been re-extracted, the **partition smkrollover -end** command finishes the process.

> **CAUTION!** The **partition smkrollover -end** command deletes the SMK from the Rollover space of the current partition, leaving only the new SMK in the Primary space. If you have exported any SKS blobs using the old SMK, that you have not re-extracted with the new Primary SMK, then those blobs can never be inserted again, unless you have retained a backup of the old SMK.

Syntax

partition smkrollover [**-start**] [**-end**] [**-force**]

Argument	Shortcut	Description
-end	**-e**	End SMK rollover and delete the Rollover SMK.
-force	**-f**	Force the action without prompting for confirmation (useful when scripting commands).
-start	**-s**	Start SMK rollover, moving the pre-existing SMK to the Rollover space, and creating a new SMK in the Primary SMK space.

Example

```
lunacm:> partition smkrollover -start

        You are about to rollover the SMK.
        Are you sure you wish to continue?

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

Command Result : No Error
```

Between issuing the **-start** and **-end** commands, insert and re-extract any SKS blobs that were encrypted/extracted with the old SMK, so that they are now encrypted with the new (Primary) SMK and stored externally.

```
lunacm:> partition smkrollover -end

        You are about to rollover the SMK.
        Are you sure you wish to continue?

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

Command Result : No Error
```

ped

Access the Remote-PED configuration commands. These commands manage the use of Remote PED with your Luna HSM. You can use a PED connected to a distant computer to provide authentication when running HSM and partition commands.

Secure use of Remote PED is mediated by the Remote PED Vector (RPV) on the HSM and on orange Remote PED keys. Obviously, the commands to administer your HSM could be issued remotely as well, using SSH or remote desktop connection. See About Remote PED for more information.

> **NOTE** This command is not applicable on DPoD Luna Cloud HSM services.

Syntax

ped

connect
disconnect
get
set
show
vector

Argument(s)	Shortcut	Description
connect	**c**	Connect to the remote PED. See "ped connect" on the next page.
disconnect	**d**	Disconnect from the remote PED. See "ped disconnect" on page 198.
get	**g**	Show the PED ID and the listening slot ID. See "ped get" on page 199.
set	**se**	Set the PED ID. See "ped set" on page 200.
show	**sh**	Display the remote PED server configuration. See "ped show" on page 201.
vector	**v**	Create or delete a Remote PED Vector (RPV). See "ped vector" on page 202.

ped connect

Connect to a remote PED. This command instructs PEDclient to attempt to connect to the remote PEDserver at the IP address and port specified on the command line, or configured using the **ped set** command.

> **NOTE** This command is not applicable on DPoD Luna Cloud HSM services.

Using ped set to Configure the ped connect Defaults

The "ped set" on page 200 command allows you to configure a default IP address and/or port for the remote PEDserver. These values are used if they are not specified when you issue the **ped connect** command. If no defaults are configured using **ped set**, you must specify at least an IP address. If no port is specified, the default port (1503) is used.

Syntax

ped connect [**-ip** <ip_address>] [**-port** <number>] [**-slot** <slot_number>] [**-pwd**]

Argument(s)	Shortcut	Description
-ip <ip_address>	**-i**	Specifies the IP Address of the PED. If **-ip** is not specified, the IP address configured with **ped set** is used.
-port <number>	**-po**	Network Port (0-65535). If **-port** is not specified, the default or the port configured with **ped set** is used. **Default:** 1503
-password	**-pwd**	Used to set up a one-time password-protected secure channel between an uninitialized HSM and the PED, allowing you to securely initialize the orange (Remote PED Vector) key.
-slot <slot_number>	**-s**	Specifies the slot for the remote PED. If **-slot** is not specified, the current slot number is used.

Example

```
lunacm:> ped connect -ip 123.45.6.78

Command Result : No Error
```

ped disconnect

Disconnect the current/active remote PED. No address information is required since only one remote PED connection can exist at one time.

> **NOTE** This command is not applicable on DPoD Luna Cloud HSM services.

Syntax

ped disconnect [**-slot** <slotnum>] [**-force**]

Argument(s)	Shortcut	Description
-force	**-f**	Force the action without prompting.
-slot	**-s**	The slot on which to disconnect from the remote PED server. If this is not specified, the current slot is used.

Example

```
lunacm:> ped disconnect

        Are you sure you wish to disconnect the remote ped?

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

Command Result : No Error
```

ped get

Show the PED connection type for current slot. This command displays the type of PED input which is expected ('local' or 'remote') on the current slot.

> **NOTE** This command is not applicable on DPoD Luna Cloud HSM services.

Syntax

ped get

Example

```
lunacm:> ped get

HSM slot 1 listening to remote PED (id 1).

Command Result : No Error


lunacm:> ped set id 0 slot 2

Command Result : No Error


lunacm:> ped get

HSM slot 2 listening to local PED (id 0).

Command Result : No Error
```

ped set

Configure an IP address and/or port that are used by the **ped connect** command when establishing a connection to a Remote PED Server. See "ped connect" on page 197 for more information. At least one (**-ip** or **-port**) must be specified.

> **NOTE** This command is not applicable on DPoD Luna Cloud HSM services.

Syntax

ped set [**-ip** <ped_server_ip> | **-port** <ped_server_port>]

Argument(s)	Shortcut	Description
-ip <ped_server_ip>	**-i**	Specifies the IP Address used by the **ped connect** command.
-port <ped_server_port	**-p**	Specifies the port used by the **ped connect** command. **Range:** 0-65535 **Default:** 1503

Example

```
lunacm:> ped set -ip 192.20.11.64 -port 1503

Command Result : No Error
```

ped show

Display information for the current HSM PED connection. This command is not applicable on DPoD Luna Cloud HSM services.

Syntax

ped show

Example

```
lunacm:> ped show

Configured Remote PED Server information

Remote PED Server IP address:   192.20.11.64
Remote PED Server Port:         1503

Command Result : No Error
```

ped vector

Create or delete a Remote PED Vector (RPV). Use this command to:

- Create a Remote PED Vector (RPV) and imprint it onto the HSM and an orange PED key.
- Delete an RPV from the HSM.

The options **init** and **delete** cannot be used together.

> **NOTE** This command is not applicable on DPoD Luna Cloud HSM services.

Syntax

ped vector [**init** | **delete**] [**-force**]

Argument(s)	Shortcut	Description
delete	**d**	Delete a Remote PED Vector (RPV) from the HSM. This does not affect RPV on orange PED key(s). No PED action required.
-force	**-f**	Force the action without prompting.
init	**i**	Create a Remote PED Vector (RPV) and imprint it on an orange PED key, or accept a pre-existing RPV from an orange PED key. PED action required.

Example

```
lunacm:>ped vector init

        You are about to initialize the Remote PED Vector
        Are you sure you wish to continue?

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

        RPV was successfully initialized.

Command Result : No Error



lunacm:>ped vector delete

        You are about to delete the Remote PED Vector
        Are you sure you wish to continue?

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

        RPV was successfully deleted.

Command Result : No Error
```

remotebackup start

Start the remote backup server on the current slot. Your Luna Backup HSM must be connected to that computer and the Luna HSM Client software must be installed, including the library and the Backup HSM driver. Use the **slot set -slot** <number> command to set the backup HSM as the current slot for use by the remote backup server.

Syntax

remotebackup start [**-port** <portnum>] [**-timeout** <seconds>] [**-commandtimeout** <seconds>] [**-debug**]

Argument(s)	Shortcut	Description
-commandtimeout <seconds>	**-ct**	The command timeout for network communication. This option can be used to adjust the timeout value to account for network latency. **Default:** 10 seconds **Range:**1 to 3600
-debug	**-de**	Display additional error information.
-port <portnum>	**-po**	Port number the server will listen on. If no port number is provided, the default port number is used. **Default:** 2222
-timeout <seconds>	**-t**	The time in seconds that the server will wait for a client connection. The maximum allowed value is 18000. After every client connection, the timeout value is restarted. **Default:** 18000 seconds **Range:**1 to 18000

Example

```
lunacm:> remotebackup start

        Remote Backup Server started for slot 1 on port 2222.

        It will run for 18000 seconds. To stop it sooner, hit 'ctl^c".

        Stopping Remote Backup Server.

Command Result : No Error
```

role

Perform administrative commands related to HSM and partition roles - list roles, log in and log out, initialize a role on a partition, create a challenge secret, change or reset password for a role, etc.

Syntax

role

changepw
createchallenge
deactivate
init
list
login
logout
recoveryinit
recoverylogin
resetpw
setdomain
show

Argument(s)	Shortcut	Description
changepw	**cp**	Change password. See "role changepw" on the next page.
createchallenge	**cc**	Challenge create. See "role createchallenge" on page 208.
deactivate	**deact**	Deactivate role. See "role deactivate" on page 210.
init	**in**	Initialize a role on the partition. See "role init" on page 211.
list	**li**	List roles on the partition. See "role list" on page 213.
login	**logi**	Role login. See "role login" on page 214.
logout	**logo**	Role logout. See "role logout" on page 216.
recoveryinit	**ri**	Setup/configure for "Recovery Login". See "role recoveryinit" on page 217.
recoverylogin	**rl**	Login using"Recovery Login". See "role recoverylogin" on page 218.
resetpw	**rp**	Reset password. See "role resetpw" on page 219.
setdomain	**d**	Set the domain for a role. See "role setdomain" on page 221.
show	**s**	Show state of a role. See "role show" on page 222.

 Copyright 2001-2026 Thales Group

role changepw

Change the password, PED key secret, or activation challenge password for the currently logged-in role.

From time to time, it might be necessary to change the secret associated with a role on a cryptographic module (HSM) or a partition of an HSM, or a cloning domain secret. Reasons for changing credentials include:

- Regular credential rotation as part of your organization's security policy
- Compromise of a role or secret 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, PINs, or shared secrets)

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

The following characters are allowed:

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

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

Syntax

role changepw -name <role> [**-oldpw** <oldpassword>] [**-newpw** <your_unique_new_password_for_the_role>] [**-prompt**] [**-logoutOther**] [**-force**]

Argument(s)	Shortcut	Description
-logoutOther	**-l**	Log out the role with the given name from other applications. *Include* the **-logoutOther** option if there is an immediate security concern, and you want all applications' access to be terminated immediately, to minimize damage due to a compromised credential. Issue the command *without* this option for relaxed situations like scheduled password roll-over, or personnel departing on good terms, or other non-urgent reasons, where you want the applications using the partition, with the current role credential, to have time to finish current tasks and end their sessions. When they resume activity, and need to create new sessions, they will do so only under the new credential for the role.
-name <role>	**-n**	Role to change password for. This must be the currently logged-in role.

Argument(s)	Shortcut	Description
-oldpw <oldpassword>	**-old**	Current password (for application partition on PW authenticated HSM) or current challenge secret (for application partition on multifactor quorum-authenticated HSM). If you include option **-oldpw** the HSM assumes that you wish to change the challenge secret, which is the "secondary credential". This applies to Crypto Officer and Crypto User, which each have primary and secondary credentials, but not to Partition SO, which has only primary credential. If you omit option **-oldpw** the HSM assumes that you wish to change the "primary credential" or PED key secret. Required if you wish to change the secondary credential.
-newpw <newpassword>	**-new**	New password (for application partition on password-authenticated HSM) or new challenge secret (for application partition on multifactor quorum-authenticated HSM). Required if you have already provided an **-oldpw**.
-prompt	**-p**	Prompt for challenges (challenges will be hidden by *)
-force	**-f**	Force the action. Use this option to bypass the warning about primary/secondary credentials on a multifactor quorum-authenticated HSM, as shown in the example.

Examples

Change credential on the HSM's Admin partition

```
lunacm:> role login -name SO

        Please attend to the PED.

Command Result : No Error



lunacm:> role changepw -name SO -prompt

        Warning: this role has no secondary credentials.
                -prompt parameter will be ignored.

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

        Please attend to the PED.

Command Result : No Error
```

Change Crypto Officer's password

```
lunacm:> role changepw -name co -oldpw PASSWORD -newpw <your_unique_password_for_co>

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

Command Result : No Error
```

Change the Crypto Officer's primary credential (PED key secret)

```
lunacm:> role changepw -name co

        This role has secondary credentials.
        You are about to change the primary credentials.
        Are you sure you wish to continue?

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


Command Result : No Error
```

Change Crypto Officer's secondary credential (challenge secret)

```
lunacm:> role changepw -name co -oldpw PASSWORD -newpw <your_unique_password_for_co>

        This role has secondary credentials.
        You are about to change the secondary credentials.
        Are you sure you wish to continue?


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


Command Result : No Error
```

 Copyright 2001-2026 Thales Group

role createchallenge

Create a challenge secret for the Crypto Officer (CO) or Limited Crypto Officer (LCO) or Crypto User (CU) role on the current partition (slot). This command applies to PED-authenticated partitions only.

The challenge secret is a text string (password) that provides an additional level of authentication for PED-authenticated partitions. If you create a challenge secret for a role, the role authenticates to the partition as follows:

- If the role is not activated on the partition, the role must provide both the PED key and challenge secret to gain access to the partition.
- If the role is activated on the partition, the role is able to access the partition using the challenge secret only.

See Activation and Auto-activation on Multi-factor- (PED-) Authenticated Partitions for more information.

You must be logged in as the Partition SO to create a challenge for the Crypto Officer. You must be logged in as the Crypto Officer to create a challenge for the Limited Crypto Officer. You must be logged in as the Crypto Officer to create a challenge for the Crypto User. The target role must already exist. See "role init" on page 211.

> **NOTE** This command is not applicable on DPoD Luna Cloud HSM services.

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

The following characters are allowed:

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

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

Syntax

role createchallenge -name <role> [**-challengesecret** <string>]

Argument(s)	Shortcut	Description
-name <role>	**-n**	Name of role for which the challenge is to be created
-challengesecret	**-c**	The challenge secret (password) you wish to create for this role. If this option is not included, you will be prompted to enter a challenge secret, masked by asterisks (*).

Example

```
lunacm:> role createchallenge -name co

        Please attend to the PED.

        enter new challenge secret: ********
```

```
        re-enter new challenge secret: ********

Command Result : No Error
```

role deactivate

Deactivates a role on a partition.

If the "Allow activation" policy is set, then activation/re-activation happens with login for the CO and CU roles. Use this command to disable activation for a specific role.

> **NOTE** This command is not applicable on DPoD Luna Cloud HSM services.

Syntax

role deactivate -name <role>

Argument(s)	Shortcut	Description
-name <role>	**-n**	Name of role to be deactivated.

Example

```
lunacm:> role login -name po

        Please attend to the PED.

Command Result : No Error


lunacm:> role deactivate -name co

Command Result : No Error
```

role init

Initializes (creates) the named role on the current partition / slot, if applicable.

Use lunacm:> **"role list" on page 213** to see which roles are available on the current partition/slot.

The Auditor role can exist only on the Luna PCIe HSM 7's administrative partition, and shares that partition with the HSM Security Officer. The Auditor role cannot be initialized by another role. Therefore, if the HSM SO is currently logged in, the SO must log out before you run **role init** to create the Auditor.

When the Auditor role is created, it has no domain set. To allow Auditor to clone, you must log in as Auditor and run lunacm:> **"role setdomain" on page 221**.

Syntax

role init -name <role> [**-password** <password>]

Argument(s)	Shortcut	Description
-name <role>	**-n**	Name of role to be initialized. You can type the entire string, or use the shortcut shown in parentheses (not case-sensitive). **Valid roles:** Crypto Officer (CO). The PO initializes the CO. Limited Crypto Officer (LCO). The CO initializes the LCO. Crypto User (CU). The CO initializes the CU. Audit (AU).

-password <password>	**-p**	The initial password for role, valid for the initial login only.
		Passwords and activation challenge secrets must be 8-255 characters in length. Spaces are allowed; to specify a password with spaces using command-line options, enclose the password in double quotation marks. The space character may not be used as the first character in a password.
		The following characters are allowed:
		`!#$%'`
		`()*+,-./0123456789:=? @ABCDEFGHIJKLMNOPQRSTUVWXYZ`
		`[]^_abcdefghijklmnopqrstuvwxyz{}~`
		This character set is enforced when using Luna HSM Client 10.8.0 or newer, and recommended for all previous versions. Previously-set passwords and challenge secrets are unaffected, but the new character set is enforced when these passwords are changed.
		NOTE The role must change the initial password using the command "role changepw" on page 205 during the initial login session, or when they attempt a subsequent login.

Example

Initializing the Crypto Officer role

```
lunacm:>role init -name co

        Please attend to the PED.

Command Result : No Error
```

Initializing the Auditor role

```
lunacm:>role init -name au

        Please attend to the PED.

Command Result : No Error
```

role list

List the roles available on the current partition/slot.

Syntax

role list

Example

When current slot is set to a User Partition:

```
lunacm:>slot set slot 0

        Current Slot Id:    0     (Luna User Slot 7.0.1 (PED) Signing With Cloning Mode)

Command Result : No Error



lunacm:>role list
        Roles                  (short)
        ============================
        Partition SO            po
        Crypto Officer          co
        Limited Crypto Officer  lco
        Crypto User             cu

Command Result : No Error
```

When current slot is set to the Admin Partition:

```
lunacm:>slot set slot 4

        Current Slot Id:    4     (Luna Admin Slot 7.0.1 (PED) Signing With Cloning Mode)

Command Result : No Error



lunacm:>role list
        Roles            (short)
        ======================
        SO                 so
        Administrator      ad
        Auditor            au

Command Result : No Error
```

role login

Logs the named user into the partition at the current slot.

For password-authenticated HSMs, the entire credential is the password. You can enter your password visibly on-screen with the **-password** option, or wait to be prompted after pressing enter. Passwords entered at the prompt are masked by asterisks (*). This is the administrative password (Crypto Officer or Crypto User), and it is also the same password that is presented by your application program when it performs cryptographic operations on the application partition.

For multifactor quorum-authenticated HSMs, the authentication is the black PED key and the password/challenge for Crypto Officer, or the gray PED key and the password/challenge for Crypto User.

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

- If Partition Policy 22: Allow activation is not set (value = 0), then the black PED key and the password/challenge are both required for each login, including those initiated by your application program.
- If Partition Policy 22: Allow activation is set (value = 1 see "partition changepolicy" on page 128), then the PED key secret is cached, and only the password/challenge string is required for each subsequent login. That is, if the partition is activated, you are not prompted to respond to the PED. At that point, your application program can authenticate with just the password/challenge string, as if the HSM was password-authenticated.

Activation (caching of the PED key secret) persists until you explicitly deactivate (see "role deactivate" on page 210) or until the HSM is restarted or loses power.

> **CAUTION!** If too many bad login attempts are made against a role, the appropriate security policy for that role is enacted. For example, three bad attempts to log into the HSM SO role causes all HSM contents to be zeroized. Too many attempts on the Crypto Officer role causes that role to be locked out until reset by the Partition Security Officer. The bad-login count is reset by a successful login. For the Auditor role, if the bad login attempt threshold is exceeded, the HSM locks out that role for 60 seconds. The output of **role show**, during that time, gives a status of "Locked out". However, **role show** continues to show a state of "Locked out" even after the lockout time has expired; the displayed status does not reset until after a successful login.

PKCS#11 permits one role to be logged into a slot, per session. If a role is logged in, and you attempt to log in as a different role, the HSM presents an error message like USER_ALREADY_LOGGED_IN, indicating that some other user role is logged into the current slot via the current session. If you need to log in, your options are:

> Log out the other user and log in as the desired user, in the current session,

or

> Launch another session (lunacm or other tool), select the slot, and log in from there.

Syntax

role login -name <role> [**-password** <password>]

Argument(s)	Shortcut	Description
-name <role>	**-n**	Specifies the name of the role that is logging in. Use the command "role list" on page 213 to see the roles available on the partition. **Note:** If you specify multiple users (for example **role login -n Crypto Officer -n Partition SO**, the last one entered (in this example, **Partition SO**), is used.
-password <password>	**-p**	Specifies the password for the role. Omit this parameter to be prompted for a password, which will be obscured by * characters when entered.

Example

```
lunacm:> role list
        Roles            (short)
        ========================
        SO                 so
        Administrator      ad
        Auditor            au

Command Result : No Error



lunacm:> role login -name SO

        Please attend to the PED.

Command Result : No Error
```

role logout

This command logs the currently logged-in role out of a partition.

For multifactor quorum-authenticated HSMs, if the activation policy is set, then logout does not uncache the PED key data, so the next login will require only the password/challenge for success - no PED prompt appears.

Syntax

role logout

Example

```
lunacm:> role logout

Command Result : No Error
```

role recoveryinit

Initialize the current role for Recovery Login by creating an HA RSA key pair.

See also CKDemo HIGH AVAILABILITY RECOVERY Menu Functions.

> **NOTE** Labels are required only to create a RecoveryLogin RSA key pair, which is the default action if [keyhandle] is not supplied.
>
> If an allowed user role name is not specified and Partition is version zero (v0), then HA Login v 1.1 is set up, otherwise HA Login version 2.0 is set up.

> **NOTE** This command is not applicable on DPoD Luna Cloud HSM services.

Syntax

role recoveryinit [**-revoke**] [**-plabel** <string>] [**-rlabel** <string>] [**-keyhandle** <number>] [**-publicKeyCertificate** <number>] [**-name** <string>[,<string>]] [**-force**]

Argument(s)	Shortcut	Description
-revoke	**-r**	Revoke recovery credential.
-plabel <string>	**-pl**	RSA Public key label.
-rlabel <string>	**-rl**	RSA Private key label.
-keyhandle <number>	**-kh**	RSA Private key handle (optional).
-publicKeyCertificate <number>	**-pkc**	[Slot#] containing RSA private key handle against which to generate PKC. Current slot or given slot#.
-name <name string>	**-n**	User's role name allowed to log in the secondary Token).
-force	**-f**	Force action (useful for scripting).

Example

```
lunacm:>role recoveryinit -plabel SOpub -rlabel SOpriv

        Generating RSA Key pair for Recovery Init...

        'SO' in slot 103 has been Recovery Initialized
        with key handle 37.

Command Result : No Error
```

role recoverylogin

Perform an HA recovery login on the specified target slot.

See also CKDemo HIGH AVAILABILITY RECOVERY Menu Functions.

> **NOTE** This command is not applicable on DPoD Luna Cloud HSM services.

Syntax

role recoverylogin -name <string> **-slot** <slotnumber> **-keyhandle** <number>

Argument(s)	Shortcut	Description
-name <string>	**-n**	Role name.
-slot <slotnumber>	**-s**	Target slot.
-keyhandle <number>	**-kh**	Handle of RSA Private key to use.

Example for the Crypto Officer role

```
lunacm:>role recoverylogin -name co -slot 3 -keyhandle 46
```

role resetpw

Resets the password for a specified role. On Luna HSMs, the Partition SO can reset the Crypto Officer password or black PED key only 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 the target role is not on the current partition, you must specify the target role's partition's slot.

> **NOTE** Resetting passwords for roles on partitions other than the current active partition is possible only from the administrative partition.

Syntax

role resetpw -name <role> [**-password** <password>] [**-slot** <slotnumber>] [**-logoutOther**]

Argument(s)	Shortcut	Description
-logoutOther	**-l**	Log out the role with the given name from other applications. *Include* the **-logoutOther** option if there is an immediate security concern, and you want all applications' access to be terminated immediately, to minimize damage due to a compromised credential. Issue the command *without* this option for relaxed situations like scheduled password roll-over, or personnel departing on good terms, or other non-urgent reasons, where you want the applications using the partition, with the current role credential, to have time to finish current tasks and end their sessions. When they resume activity, and need to create new sessions, they will do so only under the new credential for the role.
-name <role>	**-n**	Name of role to have password reset.

Argument(s)	Shortcut	Description

-password <password>	**-p**	Password for the specified role. Use this option for password-authenticated HSMs only. Multifactor Quorum-authenticated HSMs will return an error.
		Passwords and activation challenge secrets must be 8-255 characters in length. Spaces are allowed; to specify a password with spaces using command-line options, enclose the password in double quotation marks. The space character may not be used as the first character in a password.
		The following characters are allowed:
		`!#$%'`
		`()*+,-./0123456789:=? @ABCDEFGHIJKLMNOPQRSTUVWXYZ`
		`[]^_abcdefghijklmnopqrstuvwxyz{}~`
		This character set is enforced when using Luna HSM Client 10.8.0 or newer, and recommended for all previous versions. Previously-set passwords and challenge secrets are unaffected, but the new character set is enforced when these passwords are changed.

-slot <slotnumber>	**-s**	Target slot.

Example

```
lunacm:> role resetpw -name co
        Please attend to the PED.

Command Result : No Error
```

role setdomain

Sets the domain for the HSM's Auditor user on the Luna PCIe HSM 7's admin partition (not applicable to other roles). The Auditor role must have been initialized previously, and must be logged in, in order to set the domain. On password-authenticated HSMs, this step is required before setting logging parameters or the log filepath, or importing/exporting audit logs.

> **NOTE** This command is not applicable on DPoD Luna Cloud HSM services.

Syntax

role setdomain [**-domain** <domain> | **-defaultdomain**] [**-force**]

Argument(s)	Shortcut	Description
-domain <domain>	**-d**	Set the role Cloning Domain string for password-authenticated HSM only; ignored for multifactor quorum-authenticated HSM) **Note: -domain** and **-defaultdomain** are mutually exclusive parameters - attempting to use both causes the command to fail with an error message.
-defaultdomain	**-def**	Set the default domain on a password-authenticated HSM; ignored for multifactor quorum-authenticated HSM. (Deprecated - not recommended unless needed to clone with older HSMs that had default domain set.) **Note: -domain** and **-defaultdomain** are mutually exclusive parameters - attempting to use both causes the command to fail with an error message.
-force	**-f**	Force the action (useful for scripting)

Example

```
lunacm:> role login -name au
        Please attend to the PED.

Command Result : No Error



lunacm:> role setdomain

        You are about to set a new domain for the role.
        Are you sure you wish to continue?

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

        Please attend to the PED.

Command Result : No Error
```

role show

Shows the state of the named role.

> **NOTE** For the Auditor role, if the bad login attempt threshold is exceeded, the HSM locks out that role for 60 seconds. The output of **role show**, during that time, gives a status of "Locked out".
>
> However, **role show** continues to show a state of "Locked out" even after the lockout time has expired; the displayed status does not reset until after a successful login.

Syntax

role show -name <role>

Argument(s)	Shortcut	Description
-name <role>	**-n**	The name of the role to show.

Example

```
lunacm:> role show -name co

        State of role 'Crypto Officer':
                Primary authentication type:          PED
                Secondary authentication type:        PIN
                Failed login attempts before lockout: 10
                Failed change password attempts before lockout: 10

Command Result : No Error



lunacm:> role show -name Crypto User

        State of role 'Crypto User':
        Not initialized.

Command Result : No Error
```

slot

Access the slot commands.

Slots originated as a cryptographic software concept, later overlaid onto HSM function, and originally corresponded to individual removable cryptographic "token" HSMs. In general, a physical "slot" correlates to a PKCS#11 crypto slot. However, to allow for cases where more than one HSM, or where physical Luna HSMs containing multiple virtual HSMs can be connected, we declare placeholder slots that might or might not be occupied by a physical device, but which are seen by the library as ready for a device to be connected.

This allows (for example) a USB-connected HSM to be connected to a Luna Network HSM 7 appliance or to a Luna HSM Client computer during a cryptographic session without requiring a restart. Similarly, it allows HA operation, where client activity is directed toward the HA virtual slot, but the client must be able to see all physical slots, in addition to that HA virtual slot, in order to coordinate the function of the HA group.

LunaCM depends on the availability of HSM partitions in order to be useful. If no application partition has been created, then only the HSM SO (administrative) partition is available, against which to run commands.

> **CAUTION!** If the **Chrystoki.conf** / **Crystoki.ini** configuration file [Presentation] setting "ShowAdminTokens=" is set to **no**, then the HSM administrative partition/slot for any attached HSMs are not available. If you also have not created any application partitions, LunaCM is not usable. If you know you have a working Luna PCIe HSM 7 attached to your Client computer and LunaCM shows no usable commands, or you cannot see the Admin slots, then verify in your **Chrystoki.conf** or **Crystoki.ini** file that "ShowAdminTokens" is not set to **no**. See Configuration File Summary for more information.

Syntax

slot

configset
configshow
list
partitionlist
set
showempty

Argument(s)	Shortcut	Description
configset	**cset**	Set a configuration item for the slot. See ."slot configset" on page 225
configshow	**cshow**	Show the configuration for a slot . See "slot configshow" on page 227.
list	**l**	List the available slots. See "slot list" on page 228.
partitionlist	**plist**	List the partitions for a slot. See "slot partitionlist" on page 230.

Argument(s)	Shortcut	Description
set	**s**	Set the current slot. See "slot set" on page 231.
showempty	**sempt**	Show empty slots and their types. See "slot showempty" on page 232.

slot configset

Identify and set a Luna Backup HSM partition to access at the specified slot number.

This command is used only with a Luna Backup HSM at firmware version earlier than 6.22.0, and allows an archive partition on the Backup HSM to be accessed in a manner similar to an application partition on a general-purpose HSM. This command was originally developed for purposes of object migration from older PCMCIA-type HSMs in a Luna DOCK reader. It is still available, and can be used on a Luna Backup HSM, if you have a use for it. For a Backup HSM partition that is exposed by the **slot configset** command, the following limitations apply:

- Keys cannot be used for cryptographic objects.
- Keys cannot be modified.

The benefit of applying the **slot configset** command to a Backup HSM is that, on an identified archive partition:

- Keys can be deleted, individually/selectively.
- Keys can be cloned to other HSM partitions.

Partitions are named as they are created on a Backup HSM to accept archived objects during backup operations. If more than one backup partition exists on a Backup HSM, they are not exposed when you perform the lunacm command **slot list**. Generally the only backup partition that is referenced by default when the slot listing shows a slot as containing a Luna Backup HSM is from older editions of Luna HSMs, and is called "Cryptoki User". To choose which, of potentially several, archive partitions within a Backup HSM is the active partition, and to make it accessible, you need to identify that archive partition by name.

The process is to list/view the partitions while the Backup HSM is the current slot in LunaCM, using **partition list**, in order to see their partition names. Then run **slot configset -slot** <slot#-of-the-backup-hsm> **-partitionname** <name-of-desired-partition-on-backup-hsm> Then, for example, use **partition clone** to clone selected objects to other HSM partition slots.

> **NOTE** The configuration set with this command exists for the current LunaCM session only. If you log out of your LunaCM session, your **slot configset** configuration is erased.

Syntax

slot configset -slot <slot_number> **-partitionname** <partition_name>

Argument(s)	Shortcut	Description
-partitionname <partition_name>	**-p**	The partition name of the slot.
-slot <slot_number>	**-s**	Specifies the number of the slot for which you wish to set configuration settings.

Example

```
lunacm:> slot configset -slot 1 -partitionname backuppar3

        Slot configuration was successfully updated.
```

```
Command Result : No Error
```

slot configshow

Show the configuration information for the specified slot number.

Syntax

slot configshow -slot <slot_number>

Argument(s)	Shortcut	Description
-slot <slot_number>	**-s**	The number of the slot for which you want to show the configuration information.

Example

```
lunacm:> slot configshow -slot 2

        Slot Configuration:

                Slot ID:                2

                User Partition Name:    Cryptoki User

Command Result : No Error
```

 Copyright 2001-2026 Thales Group

slot list

List the available slots on the system. The HSM administrative partition and any application partition are distinct and appear individually in a LunaCM slot list, so at least two slots. Similarly, if you have several local Luna HSMs installed or connected, or if you have Luna Network HSM 7 application partitions Ethernet-connected via NTLS links, then you can have multiple slots represented in a LunaCM slot list.

LunaCM depends on the availability of HSM partitions in order to be useful. If no application partition has been created, then only the HSM SO (administrative) partition is available, against which to run commands.

> **CAUTION!** If the **Chrystoki.conf** / **Crystoki.ini** configuration file [Presentation] setting "ShowAdminTokens=" is set to **no**, then the HSM administrative partition/slot for any attached HSMs are not available. If you also have not created any application partitions, LunaCM is not usable. If you know you have a working Luna PCIe HSM 7 attached to your Client computer and LunaCM shows no usable commands, or you cannot see the Admin slots, then verify in your **Chrystoki.conf** or **Crystoki.ini** file that "ShowAdminTokens" is not set to **no**. See Configuration File Summary for more information.

Listing backup partitions

Depending on the type of backup HSM and its firmware version, the **slot list** command may list all of the backup partitions on the backup HSM, or may only list the backup HSM Admin partition:

- For Luna Backup HSM G5s running older firmware, the **slot list** command lists all of the backup partitions on any attached backup HSMs.
- For Luna Backup HSM 7s and for Luna Backup HSM G5s running newer firmware, the **slot list** command lists only the Admin partition (which contains the backup partitions) on any attached backup HSMs.

If **slot list** does not list the backup partitions, use **"slot set" on page 231** to set the current slot to the backup HSM Admin partition, and then use **"partition archive list" on page 121** to list the backup partitions contained in the Admin partition.

Syntax

slot list

Example

```
lunacm:> slot list
        Slot Id ->              0
        Tunnel Slot Id ->       2
        Label ->
        Serial Number ->        349297122736
        Model ->                Luna K7
        Firmware Version ->     7.0.1
        Configuration ->        Luna User Partition With SO (PED) Signing With Cloning Mode
        Slot Description ->     User Token Slot

        Slot Id ->              1
        Tunnel Slot Id ->       2
        Label ->                mypcie7
        Serial Number ->        150022
```

```
        Model ->                Luna K7
        Firmware Version ->     7.0.1
        Configuration ->        Luna HSM Admin Partition (PED) Signing With Cloning Mode
        Slot Description ->     Admin Token Slot
        HSM Configuration ->    Luna HSM Admin Partition (PED)
        HSM Status ->           OK

        Slot Id ->              3
        HSM Label ->            myG5pw
        HSM Serial Number ->    7001312
        HSM Model ->            G5Base
        HSM Firmware Version -> 6.10.4
        HSM Configuration ->    Luna USB HSM (PW) Signing With Cloning Mode
        HSM Status ->           OK
        Current Slot ID:  3


Command Result : No Error
```

NOTE Each HSM administrative partition in a slot list includes "HSM Status". The possible values are listed, along with expanded descriptions and possible responses, at HSM Status Values.

 Copyright 2001-2026 Thales Group

slot partitionlist

List the partitions for the specified slot. This applies only when a cryptographic slot might contain more than one HSM partition. A Luna Backup HSM, for example, occupies one cryptographic slot while containing many partitions (see "slot configset" on page 225).

Syntax

slot partitionlist -slot <slot_number>

Argument(s)	Shortcut	Description
-slot <slot_number>	**-s**	The slot for which you want to list the partitions.

Example

```
lunacm:> slot partitionlist -slot 20

        Number of Partitions: 3

                Partition #: 1
                Partition Name: par0

                Partition #: 2
                Partition Name: par1

                Partition #: 3
                Partition Name: par2

Command Result : No Error
```

slot set

Set the current slot number. The current slot is the slot to which you want LunaCM commands to apply.

LunaCM commands work on the current slot. If there is only one slot, then it is always the current slot. If there is more than one slot, then use the **slot set** command to direct the focus at the desired slot/partition, so that you can use LunaCM commands against whatever HSM admin partition or application partition occupies the indicated slot.

This command is useful where you have more than one Luna module installed in or connected to your computer, or when you have a single HSM where the HSM administrative slot is separate from the application partition slot. In those cases, you can use the **slot list** command to see which slot numbers have been assigned, and then use **slot set** to specify which of the available HSM partitions (in their slots) you wish to address with LunaCM commands.

Syntax

slot set -slot <slot_number>

Argument(s)	Shortcut	Description
-slot <slot_number>	**-s**	The number of the slot that you wish to assign as the current slot for other LunaCM utility commands to work with.

Example

```
lunacm:> slot set -slot 4

Command Result : No Error
```

 Copyright 2001-2026 Thales Group

slot showempty

This command will list the available empty slots on the system and their types.

Syntax

slot showempty

Example

```
lunacm:> slot showempty

        Slot Id ->   2: Luna UHD Slot
        Slot Id ->   3: Luna UHD Slot
        Slot Id ->   4: Luna UHD Slot
        Slot Id ->   7: Luna G7 Slot
        Slot Id ->   8: Luna G7 Slot
        Slot Id ->   9: Luna G7 Slot

        Current Slot Id: 0


Command Result : No Error
```

srk

Access the Secure Recovery commands to configure and manage the Backup HSM tamper and secure recovery key (SRK) behavior and the setting and recovery from Secure Transport Mode.SeeBackup HSM Secure Transport and Tamper Recovery for details.

The **srk** commands apply to the Luna Backup HSM G5 only.

Syntax

srk

disable
enable
generate
recover
show
transport

Argument(s)	Shortcut	Description
disable	**d**	Disable Secure Transport Mode functionality. See "srk disable" on the next page.
enable	**e**	Enable Secure Transport Mode functionality. See "srk enable" on page 235.
generate	**g**	Generate a new SRK on the Backup HSM. See "srk generate" on page 236.
recover	**r**	Recover from tamper or exit transport mode. See "srk recover" on page 237.
show	**s**	Show the Secure Recovery state. See "srk show" on page 238.
transport	**t**	Set the HSM into transport mode. See "srk transport" on page 239.

srk disable

Disable external tamper keys. This command disables the use of external split(s) of the SRV (secure recovery vector) on purple PED keys (SRK). The external split is brought from the purple key, back into the HSM. When SRK is disabled:

- Secure Transport Mode cannot be set.
- Any tamper event that is detected by the HSM stops the HSM only until you restart. The MTK is destroyed by a tamper, but is immediately recreated at the restart if both splits are internally available (i.e., when SRK is disabled).

The Backup HSM SO must be logged in to the HSM to issue this command.

The **srk** commands apply to the Luna Backup HSM G5 only.

Syntax

srk disable

Example

```
lunacm:> srk disable

        Secure Transport functionality was successfully disabled.

Command Result : No Error
```

srk enable

Enable external tamper keys. This command enables the use of external split(s) of the SRV (secure recovery vector) on purple PED keys (SRK). The external split is brought from the HSM to a purple key, and erased from the HSM, leaving only one split on the HSM. When SRK is enabled:

- Secure Transport Mode can be set.
- Any tamper event that is detected by the HSM stops the HSM until you restart and perform "srk recover". The "srk recover" operation makes the externally provided split (from the purple key) available to combine with the internal split, allowing the MTK to be recreated. The MTK is destroyed by a tamper (or by setting STM), and cannot be recreated until both splits are available (if SRK is enabled).

The Backup HSM SO must be logged in to the HSM to issue this command.

The PED must be connected, and you must present "new" purple PED keys when prompted. "New" in this case, means a purple PED key that is literally new, or a PED key that has been used for another purpose - as long as it does not contain the current valid external SRK split, before the new generating operation. For safety reasons, the HSM and Luna PED detect and refuse to overwrite the current purple PED key(s).

The **srk** commands apply to the Luna Backup HSM G5 only.

Syntax

srk enable

Example

```
lunacm:> srk enable

        Secure Transport functionality was successfully enabled.

Command Result : No Error
```

srk generate

Resplit the Secure Recovery Key. This command generates new splits of the Secure Recovery Key. The internal split is stored in a secure memory area on the HSM. The external split is imprinted on a purple PED key (or multiple purple keys if you invoke MofN), using "srk enable" on the previous page.

The **srk** commands apply to the Luna Backup HSM G5 only.

Syntax

srk generate

Example

```
lunacm:> srk generate
        New SRK successfully generated.

Command Result : 0 (Success)
```

srk recover

Exit transport or tamper mode. This command reconstitutes the SRV on the HSM, using the SRK split(s) on the purple SRK PED Key(s), which in turn recreates the HSM's Master Key, allowing the HSM and its contents to be accessed and used again, following Transport Mode or a tamper event. The Luna PED must be connected, and you must present the correct purple PED keys when prompted.

The **srk** commands apply to the Luna Backup HSM G5 only.

Syntax

srk recover

Example

```
lunacm:> srk recover
        Successfully recovered from Transport Mode/Tamper.

Command Result : No Error
```

srk show

Display the current SRK state on the Luna Backup HSM.

The **srk** commands apply to the Luna Backup HSM G5 only.

Syntax

srk show

Example

```
lunacm:> srk show

        Secure Transport Functionality is supported and enabled.

        Secure Recovery State Flags ->
                SRK Regeneration Required:  0
                Hardware (tamper) Zeroized: 0
                Transport Mode:             0
                Locked:                     1   *


Command Result : No Error
```

> **NOTE** * The flag "Locked:" was set during manufacturing and testing at the factory and indicates that the MTK is locked into the HSM and cannot be modified for the life of the HSM. No action.

srk transport

Enter Secure Transport Mode. This command places the HSM in transport mode, destroying the SRK split of the Master Key and causing all HSM content to be unusable. The use of external split(s) of the SRK (secure recovery key) on purple PED keys must already be enabled.

The Backup HSM SO need not be logged in to the HSM to issue this command.

The **srk** commands apply to the Luna Backup HSM G5 only.

Syntax

srk transport

Example

```
lunacm:> srk transport

        You are about configure the HSM in transport mode.
        If you proceed, Secure Recovery keys will be created
        and the HSM will be tampered.
        Are you sure you wish to continue?

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

        Configuring the HSM for transport...

        HSM was successfully configured for transport.

Command Result : No Error
```

stm

Configure, or display information about Secure Transport Mode (STM).

> **NOTE** The **stm** commands appear only when LunaCM's active slot is set to the administrative partition

STM allows you to verify that an HSM has not been tampered while in transit or storage. STM is optional. When invoked, STM provides comparison strings that you can visually verify, and imposes a pause during the STM recover operation where you indicate that you have seen the command output and decided to resume using the HSM, or to leave the HSM in Secure Transport Mode pending further investigation. For more information, see Secure Transport Mode.

Syntax

stm

recover
show
transport

Argument(s)	Shortcut	Description
recover	**r**	Recover an HSM that has been placed in STM. See "stm recover" on the next page.
show	**s**	Displays the current STM state. See "stm show" on page 243.
transport	**t**	Access commands that allow you to enable or disable STM. See "stm transport" on page 244

 Copyright 2001-2026 Thales Group

stm recover

Recover the HSM from Secure Transport Mode (STM).

If the HSM is in initialized state, you must be logged in as HSM SO to recover from STM.

- for multifactor quorum authenticated HSMs the blue HSM SO PED key is required;
- for password authentication have the HSM SO password ready.

If the HSM is zeroized, no login is required.

> **NOTE** The **stm** commands appear only when LunaCM's active slot is set to the administrative partition

When you enter this command, include the random user string that was generated when the HSM was put into STM. A verification string will be displayed:

- If the verification string generated matches the string that was displayed when the HSM was put into STM (see "stm transport" on page 244), the HSM was not tampered with while in STM.
- If the verification string generated does not match the verification string generated when you placed the HSM in STM, this might indicate that the HSM has been tampered while in STM, or that an incorrect random user string has been entered..

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

If you are confident the HSM has not been tampered with, you can still enter "**proceed**" to recover from STM. See Secure Transport Mode for more information.

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

Syntax

stm recover -randomuserstring <string>

Argument(s)	Shortcut	Description
-randomuserstring <string>	**-r**	To confirm that the HSM was not tampered with while in STM, enter the random user string generated when it was placed in STM, in the format XXXX-XXXX-XXXX-XXXX.

Example

```
lunacm:>stm recover -randomuserstring Gxbx-dXFM-x4bW-bMWN

        Calculating the verification string (may take a few seconds)...

        Verification String: SL7P-GWtA-JFKt-psCH

        Please verify the string before you continue...
        Are you sure you wish to continue?

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

        Recovering the HSM from transport...
        Successfully recovered from Transport Mode.

Command Result : No Error
```

stm show

Display the current Secure Transport Mode state.

> **NOTE** The **stm** commands appear only when LunaCM's active slot is set to the administrative partition

The state is 0 or 1, as follows:

0	The HSM is not in transport mode, and is ready for use.
1	The HSM is in transport mode. You must use the command "stm recover" on page 241 to exit transport mode before you can use the HSM.

Syntax

stm show

Example

```
lunacm:> stm show

         STM State Flags ->
                 Transport Mode:           0


Command Result : No Error
```

stm transport

Place the HSM in Secure Transport Mode (STM).

You must be logged in as HSM SO to invoke Secure Transport Mode.

> for multifactor quorum authenticated HSMs, the blue HSM SO PED key is required

> for password authentication have the HSM SO password ready

> **NOTE** The **stm** commands appear only when LunaCM's active slot is set to the administrative partition

When you enter this command, two strings are displayed: a verification string and a random user string. Record both of these to confirm later that the HSM was not tampered with while in STM. When you recover from STM, enter the random user string and compare the generated verification string to the original one you received. If the strings match, the HSM has not been tampered while in STM (see "stm recover" on page 241).

> **CAUTION!** Using a multifactor quorum-authenticated HSM with Luna HSM Firmware 7.7.1-20 or older, ensure that CO, LCO and CU roles are deactivated *on all partitions* before placing the HSM in Secure Transport Mode (see Deactivating a Role). If any roles are still activated when STM is set, this can result in mismatched verification strings during STM recovery.
>
> This is not necessary using Luna HSM Firmware 7.7.2 or newer; placing the HSM in STM automatically logs out and deactivates these roles.
>
> The roles can be logged in and reactivated manually after STM recovery.

Syntax

stm transport

Example

```
lunacm:>stm transport

        You are about to configure the HSM in STM.
        Are you sure you wish to continue?

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

        Configuring the HSM for transport (may take a few seconds)...

        HSM was successfully configured for transport.

        Please record the displayed verification & random user strings.
        These are required to recover from Secure Transport Mode.


        Verification String: SL7P-GWtA-JFKt-psCH

        Random User  String: Gxbx-dXFM-x4bW-bMWN

Command Result : No Error
```