THALES

SafeNet Luna Network HSM 7.3

LUNACM COMMAND REFERENCE GUIDE

Document Information

Product Version	7.3
Document Part Number	007-013576-005
Release Date	13 December 2019

Revision History

Revision	Date	Reason
Rev. A	13 December 2019	Initial release.

damages or any damages whatsoever including but not limited to damages resulting from loss of use, data, profits, revenues, or customers, arising out of or in connection with the use or performance of information contained in this document.

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

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

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

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

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

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

CONTENTS

PREFACE: About the LunaCM Command Reference Guide

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 11

> "LunaCM Commands" on page 15

This preface also includes the following information about this document:

> "Customer Release Notes" below

> "Audience" below

> "Document Conventions" below

> "Support Contacts" on page 10

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

Customer Release Notes

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

Audience

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

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

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

Document Conventions

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

Notes

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

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

Cautions

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

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

Warnings

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

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

Command Syntax and Typeface Conventions

Format	Convention
bold	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.

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

Customer Support Portal

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

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

Telephone

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

CHAPTER 1:   Using LunaCM

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

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

> "Accessing LunaCM" below
> "LunaCM Features" on page 13

Accessing LunaCM

The LunaCM utility (LunaCM) is the client-side administrative command interface for SafeNet HSMs.

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

> Internally installed SafeNet Luna PCIe HSMs (HSM card)

> Locally USB-connected SafeNet Luna USB HSMs

> Remotely located SafeNet Luna Network HSM application partitions, made available by a 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 SafeNet 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 SafeNet HSM. For a summary, type "help" and press **Enter**.

> **NOTE** For SafeNet Luna PCIe HSM and SafeNet Luna USB HSM, LunaCM is used to administer both the HSM as HSM SO, and the application partition. For SafeNet Luna Network HSM, LunaCM is used to manage application partitions (assuming an NTLS or STC link between your SafeNet Luna HSM Client computer and the SafeNet Luna Network HSM appliance). LunaCM is not used to perform HSM-wide administration by the HSM SO on SafeNet Luna Network HSM - 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.

If the Chrystoki.conf / Crystoki.ini configuration file [Presentation] setting "ShowAdminTokens=" is set to no, then the HSM administrative partition/slot is also unavailable, and LunaCM is not usable. If you know you have a working SafeNet Luna PCIe HSM or SafeNet Luna USB HSM attached to your Client computer and LunaCM shows no usable commands, then verify in your Chrystoki.conf or Crystoki.ini file that "ShowAdminTokens" is not set to no.

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	
-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.

Option	Description
-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.

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 mYpa55word!

or

 lunacm:> partition LOGIN -PASSWorD mYpa55word!

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 Trusted Path 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 SafeNet Luna Network HSM 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:

> SafeNet Luna Network HSM application partitions (if any), network-connected to the host computer via NTLS or STC channels

> SafeNet Luna PCIe HSMs (if any) installed within the host computer

> SafeNet Luna USB HSMs (if any) connected via USB to the host computer

By default, LunaCM shows the lowest-numbered slot first. Local HSMs (SafeNet Luna PCIe HSM or SafeNet Luna USB HSM) 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 current-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 17.
clientconfig	**ccfg**	Client configuration. See "clientconfig" on page 37.
file	**f**	File commands. See "file display" on page 44.
hagroup	**ha**	High Availability Group commands. See "hagroup" on page 45.
partition	**par**	Partition commands. See "partition" on page 88.
ped	**p**	Remote PED commands. See "ped" on page 127.

Argument(s)	Shortcut	Description
remotebackup	**rb**	Manage Remote Backup server. See "remotebackup start" on page 134.
role	**ro**	Role management commands. See "role" on page 135.
slot	**s**	Slot management commands. See "slot" on page 150.
stc	**stc**	Secure Trusted Channel commands. See "stc" on page 159.
stcconfig	**stcc**	Secure Trusted Channel configuration commands. See "stcconfig" on page 173.

appid

Access the **appid**-level commands to manage application IDs on the HSM. For a description of application IDs, see "Application IDs" on page 1 in the *SDK Reference Guide*.

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 19
open	o	Open a previously set access ID. See "appid open" on page 20
set	s	Set an access ID. See "appid set" on page 21

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" on page 1 in the *SDK Reference Guide*.

> **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.

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
```

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" on page 1 in the *SDK Reference Guide*.

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" on page 1 in the *SDK Reference Guide*.

> **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.

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" on page 1 in the *SDK Reference Guide*.

> **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.

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 on a SafeNet Luna PCIe HSM or SafeNet Luna Backup HSM. To access the Auditor commands on SafeNet Luna Network HSM, use LunaSH (see "audit" on page 1).

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 148 for the command syntax). 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 24.
export	**e**	Read the wrapped log secret from the HSM. See "audit export" on page 28.
import	**m**	Import the wrapped log secret to the HSM. See "audit import" on page 30.
logmsg	**logm**	Write a message to the HSM's log. See "audit logmsg" on page 31.
status	**s**	Show the status of the logging subsystem. See "audit status" on page 32.

Argument(s)	Shortcut	Description
time	**t**	Synchronize the HSM time to the host, or get the HSM time. See "audit time" on page 33.
verify	**v**	Verify a block of log messages. See "audit verify" on page 36.

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 148 for the command syntax). This step is required before setting logging parameters or the log filepath, or importing/exporting audit logs.

> **NOTE** The **audit** commands appear only when LunaCM's active slot is set to the administrative partition on a SafeNet Luna PCIe HSM or SafeNet Luna Backup HSM. To access the Auditor commands on SafeNet Luna Network HSM, use LunaSH (see "audit" on page 1).

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)
		> **[u]sage**: key usage (enc/dec/sig/ver)
		> **fi[r]st**: first 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
		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 t,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**

Argument(s)	Shortcut	Description
path <filepath>	**p**	Path on the host to which logs will be written. You will get 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.

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 148 for the command syntax). This step is required before setting logging parameters or the log filepath, or importing/exporting audit logs.

> **NOTE** The **audit** commands appear only when LunaCM's active slot is set to the administrative partition on a SafeNet Luna PCIe HSM or SafeNet Luna Backup HSM. To access the Auditor commands on SafeNet Luna Network HSM, use LunaSH (see "audit" on page 1).

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 148 for the command syntax). This step is required before setting logging parameters or the log filepath, or importing/exporting audit logs.

> **NOTE** The **audit** commands appear only when LunaCM's active slot is set to the administrative partition on a SafeNet Luna PCIe HSM or SafeNet Luna Backup HSM. To access the Auditor commands on SafeNet Luna Network HSM, use LunaSH (see "audit" on page 1).

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. The message text must be enclosed in double quotes. If the quotation marks are not provided, the text is interpreted as arguments (to a command that takes no arguments) and is rejected with an error message.

> **NOTE** The **audit** commands appear only when LunaCM's active slot is set to the administrative partition on a SafeNet Luna PCIe HSM or SafeNet Luna Backup HSM. To access the Auditor commands on SafeNet Luna Network HSM, use LunaSH (see "audit" on page 1).

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 on a SafeNet Luna PCIe HSM or SafeNet Luna Backup HSM. To access the Auditor commands on SafeNet Luna Network HSM, use LunaSH (see "audit" on page 1).

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 a USB-connected SafeNet 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 on a SafeNet Luna PCIe HSM or SafeNet Luna Backup HSM. To access the Auditor commands on SafeNet Luna Network HSM, use LunaSH (see "audit" on page 1).

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 35.

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 on a SafeNet Luna PCIe HSM or SafeNet Luna Backup HSM. To access the Auditor commands on SafeNet Luna Network HSM, use LunaSH (see "audit" on page 1).

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 on a SafeNet Luna PCIe HSM or SafeNet Luna Backup HSM. To access the Auditor commands on SafeNet Luna Network HSM, use LunaSH (see "audit" on page 1).

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.

> **NOTE** The **audit** commands appear only when LunaCM's active slot is set to the administrative partition on a SafeNet Luna PCIe HSM or SafeNet Luna Backup HSM. To access the Auditor commands on SafeNet Luna Network HSM, use LunaSH (see "audit" on page 1).

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.

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
```

clientconfig

Access the clientconfig-level commands to configure your client.

Syntax

clientconfig

> **deleteserver**
> **deploy**
> **listservers**
> **restart**
> **verify**

Argument(s)	Shortcut	Description
deleteserver	**d**	Delete a SafeNet Luna Network HSM server. See "clientconfig deleteserver" on the next page.
deploy	**dp**	Create a network Trust Link (NTL) between the client and the SafeNet Luna Network HSM in one step. See "clientconfig deploy" on page 39.
listservers	**ls**	List the SafeNet Luna Network HSM appliances that are registered to the client. See "clientconfig listservers" on page 41.
restart	**rest**	Restart LunaCM. See "clientconfig restart" on page 42.
verify	**v**	Verify the SafeNet Luna Network HSM slots/partitions that are visible to the client. See "clientconfig verify" on page 43.

clientconfig deleteserver

Delete a SafeNet Luna Network HSM 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 SafeNet Luna Network HSM appliance. This command creates a client Private Key and Certificate, and uses **scp** or **pscp** to transfer the client and server certificates to each other.

> **NOTE** If **scp** or **pscp** 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** <password>] [**-user** <username>] [**-regen**] [**-verbose**] [**-force**]

Argument(s)	Shortcut	Description
-client <client_IP>	**-c**	The client hostname or IP.
-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**	The appliance administrator's password. If this option is not included, you will be prompted for the password. Passwords entered at the prompt are hidden.
-regen	**-rg**	Including this option will regenerate and replace the client certificate. This may disrupt connections to other SafeNet Luna Network HSM servers.
-server <server_IP>	**-n**	The server hostname or IP.
-verbose	**-v**	Show more detailed logs during the procedure.
-user <username>	**-ur**	The appliance administrator's username. **Default:** admin

Example

```
lunacm:> clientconfig deploy -server 192.20.11.78 -client 192.20.11.129 -partition par1 -password
userpin2 -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 2017 from 192.20.11.129

Luna SA 7.0.0 Command Line Shell - Copyright (c) 2001-2017 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 SA Slots/Partitions were found:

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


Command Result : No Error
```

clientconfig listservers

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

Syntax

clientconfig listservers

Example

```
lunacm:> clientconfig listservers

  Server ID  Server              Channel  HTL Required
  _____

  0          192.20.11.40        STC      no

  1          192.20.11.78        NTLS     no


Command Result : No Error
```

clientconfig restart

Restart LunaCM. This command refreshes the LunaCM display to show any changes, such as new STC links.

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 SafeNet Luna Network HSM 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       JHpar0
   1       154438865312       JHpar1


Command Result : No Error
```

file display

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 SafeNet 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 47.
addstandby	**as**	Convert an HA group member to a standby member. See "hagroup addstandby" on page 49.
creategroup	**c**	Create an HA group. See "hagroup creategroup" on page 50.
deletegroup	**d**	Delete an HA group . See "hagroup deletegroup" on page 52.
halog	**hl**	Configure the HA log file. See "hagroup halog" on page 53.
haonly	**ho**	Enable "HA Only" mode. See "hagroup haonly" on page 55.
interval	**i**	Set the HA recover retry interval. See "hagroup interval" on page 56
listgroups	**l**	List the currently-configured HA groups. See "hagroup listgroups" on page 57.
recover	**re**	Recover a failed HA member. See "hagroup recover" on page 58.

Argument(s)	Shortcut	Description
recoverymode	**m**	Set HA recovery mode to "activeBasic" or "activeEnhanced". See "hagroup recoverymode" on page 59.
removemember	**rm**	Remove a member from an HA group. See "hagroup removemember" on page 60.
removestandby	**rs**	Convert a standby member to an active member of the HA group. See "hagroup removestandby" on page 61.
retry	**rt**	Set the HA recover retry count. See "hagroup retry" on page 62
synchronize	**s**	Synchronize an HA group. See "hagroup synchronize" on page 63

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 PED-authenticated HA group members must have a challenge created, and activation turned on, and all challenges must be the same.

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.

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 PED-authenticated HA group members must have a challenge created, and activation turned on, and all challenges must be the same.

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.
-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 v7.0.0-932. 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
```

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 262144 bytes.
-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" on page 1).

> **NOTE** Individual partition slots are still visible in LunaCM when HA Only mode is enabled. They are hidden only from client applications. Use **CKdemo** (Option **11**) to see the slot numbers to use with client applications.

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 62 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.

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
```

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. Network HSM 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.

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 56.

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 56.

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.

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** commands appear only when LunaCM's active slot is set to the administrative partition on a SafeNet Luna PCIe HSM or SafeNet Luna Backup HSM. To access the HSM-level commands on SafeNet Luna Network HSM, use LunaSH (see "hsm" on page 1).

Syntax

hsm

>**changehsmpolicy**
envshow
factoryreset
init
migratepedkey
monitor
restart
rollbackfw
showinfo
showmechanism
showpolicies
tamperclear
tampershow
updatecap
updatefw
zeroize

Argument(s)	Shortcut	Description
changehsmpolicy	**changehp**	Change the HSM Policy value. See "hsm changehsmpolicy" on page 66.
envshow	**es**	Display environmental status information for the card. See "hsm envshow" on page 67.
factoryreset	**f**	Factory reset the HSM. See "hsm factoryreset" on page 68.
init	**i**	Initialize the HSM. See "hsm init" on page 69.
migratepedkey	**mig**	Migrate a PED Key from a legacy HSM. See "hsm migratepedkey" on page 72.
monitor	**mon**	Get HSM utilization information. See "hsm monitor" on page 73.

Argument(s)	Shortcut	Description
restart	**rs**	Restart the HSM. See "hsm restart" on page 75.
rollbackfw	**rb**	Rollback the HSM firmware. See "hsm rollbackfw" on page 76.
showinfo	**si**	Get HSM information. See "hsm showinfo" on page 77.
showmechanism	**showm**	Show all mechanisms. See "hsm showmechanism" on page 79.
showpolicies	**sp**	Get HSM policy information. See "hsm showpolicies" on page 81.
tamperclear	**tc**	Unlock the HSM following a tamper event. See "hsm tamperclear" on page 83
tampershow	**ts**	Display the current tamper state for the HSM. See "hsm tampershow" on page 84
updatecap	**uc**	Update the HSM capabilities. See "hsm updatecap" on page 85.
updatefw	**uf**	Update the HSM firmware. See "hsm updatefw" on page 86.
zeroize	**z**	Put the HSM in a zeroized state. See "hsm zeroize" on page 87.

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** commands appear only when LunaCM's active slot is set to the administrative partition on a SafeNet Luna PCIe HSM or SafeNet Luna Backup HSM. To access the HSM-level commands on SafeNet Luna Network HSM, use LunaSH (see "hsm" on page 1).

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** commands appear only when LunaCM's active slot is set to the administrative partition on a SafeNet Luna PCIe HSM or SafeNet Luna Backup HSM. To access the HSM-level commands on SafeNet Luna Network HSM, use LunaSH (see "hsm" on page 1).

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 can be performed only at the local serial console. 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** commands appear only when LunaCM's active slot is set to the administrative partition on a SafeNet Luna PCIe HSM or SafeNet Luna Backup HSM. To access the HSM-level commands on SafeNet Luna Network HSM, use LunaSH (see "hsm" on page 1).

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

        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


Command Result : 0 (success)
```

hsm init

Initialize the 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** The **hsm** commands appear only when LunaCM's active slot is set to the administrative partition on a SafeNet Luna PCIe HSM or SafeNet Luna Backup HSM. To access the HSM-level commands on SafeNet Luna Network HSM, use LunaSH (see "hsm" on page 1).

Syntax

hsm init -label <label> [**-password** <SOpassword>] [**-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.
-auth	**-a**	Log in after the initialization.
-domain <domain>	**-d**	HSM Domain Name. This option is mutually exclusive with the **-defaultdomain** option. This option is required for a password-authenticated HSM. If you do not provide the domain string in the command, you are prompted for it, and the characters that you type are obscured by asterisks (*). This option is ignored for PED-authenticated HSMs.
-defaultdomain	**-def**	HSM Default Domain Name. This option is mutually exclusive with the **-domain** option. Deprecated. The **-defaultdomain** is not secure, and should not be used in a production environment. This option is ignored for PED-authenticated HSMs.
-force	**-f**	Force the action - no prompts. Useful for scripting.
-initwithped	**-iped**	Initialize a Backup Device with PED-Auth. This option is supported only when initializing a Backup Device that is in a zeroized state. This option is mutually exclusive with the **-initwithpwd** option.
-initwithpwd	**-ipwd**	Initialize a Backup Device with PWD-Auth. This option is supported only when initializing a Backup Device that is in a zeroized state. This option is mutually exclusive with the **-initwithped** option.

Argument(s)	Shortcut	Description
-label <label>	**-l**	The HSM label. Required.
-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 PED-authenticated HSMs.

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 SafeNet Luna Backup HSM

```
lunacm:>hsm init -label mybackuphsm -password s0mepw -domain s0med0ma1n -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 SafeNet 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 Luna PED USB iKey. This operation requires both a version 1.14 Luna PED (no earlier version will work - contact SafeNet 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** commands appear only when LunaCM's active slot is set to the administrative partition on a SafeNet Luna PCIe HSM or SafeNet Luna Backup HSM. To access the HSM-level commands on SafeNet Luna Network HSM, use LunaSH (see "hsm" on page 1).

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** commands appear only when LunaCM's active slot is set to the administrative partition on a SafeNet Luna PCIe HSM or SafeNet Luna Backup HSM. To access the HSM-level commands on SafeNet Luna Network HSM, use LunaSH (see "hsm" on page 1).

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 restart

Restart the SafeNet Luna HSM. Use this command to restart the SafeNet 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 SafeNet 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 Group, contact that company for a resolution of the problem. They know how their application is programmed to accomplish tasks that use the SafeNet 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 Group after gathering the relevant information.

> **NOTE** The **hsm** commands appear only when LunaCM's active slot is set to the administrative partition on a SafeNet Luna PCIe HSM or SafeNet Luna Backup HSM. To access the HSM-level commands on SafeNet Luna Network HSM, use LunaSH (see "hsm" on page 1).

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** commands appear only when LunaCM's active slot is set to the administrative partition on a SafeNet Luna PCIe HSM or SafeNet Luna Backup HSM. To access the HSM-level commands on SafeNet Luna Network HSM, use LunaSH (see "hsm" on page 1).

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
```

hsm showinfo

Display HSM-level information.

> **NOTE** The **hsm** commands appear only when LunaCM's active slot is set to the administrative partition on a SafeNet Luna PCIe HSM or SafeNet Luna Backup HSM. To access the HSM-level commands on SafeNet Luna Network HSM, use LunaSH (see "hsm" on page 1).

Syntax

hsm showinfo

Example

```
lunacm:>hsm showinfo

        Partition Label -> myLuna
        Partition Manufacturer -> Gemalto
        Partition Model -> Luna K7
        Partition Serial Number -> 532018
        Partition Status -> L3 Device
        HSM Part Number -> 808-000048-002
        Token Flags ->
                CKF_RESTORE_KEY_NOT_NEEDED
                CKF_PROTECTED_AUTHENTICATION_PATH
                CKF_TOKEN_INITIALIZED
        RPV Initialized -> Yes
        Slot Id -> 103
        Session State -> CKS_RW_PUBLIC_SESSION
        Role Status ->   none logged in
        Token Flags ->
                TOKEN_KCV_CREATED
        Partition OUID: 0000000000000000321e0800

        Partition Storage:
                Total Storage Space:  393216
                Used Storage Space:   2292
                Free Storage Space:   390924
                Object Count:         4
                Overhead:             9640

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

        Firmware Version -> 7.0.1
        Rollback Firmware Version -> 7.0.1

        Environmental:
                Fan 1 Status                            : standby
                Fan 2 Status                            : active
                Battery Voltage                         : 3.093 V
                Battery Warning Threshold Voltage       : 2.750 V
                System Temp                             : 39 deg. C
                System Temperature Warning Threshold    : 75 deg. C

        HSM Storage:
                Total Storage Space:  33554432
```

```
            Used Storage Space:    333744
            Free Storage Space:    33220688
            Allowed Partitions:    100
            Number of Partitions: 1

    License Count -> 8
            1. 621000153-000 K7 base configuration
            2. 621010185-003 Key backup via cloning protocol
            3. 621000046-002 Maximum 100 partitions
            4. 621000134-002 Enable 32 megabytes of object storage
            5. 621000135-002 Enable allow decommissioning
            6. 621000021-002 Performance level 15
            7. 621000145-002 Enable PED authentication with M of N
            8. 621010089-002 Enable remote PED capability


Command Result : No Error
```

hsm showmechanism

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

> **NOTE** The **hsm** commands appear only when LunaCM's active slot is set to the administrative partition on a SafeNet Luna PCIe HSM or SafeNet Luna Backup HSM. To access the HSM-level commands on SafeNet Luna Network HSM, use LunaSH (see "hsm" on page 1).

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.

> **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 Group Customer Support.

> **NOTE** The **hsm** commands appear only when LunaCM's active slot is set to the administrative partition on a SafeNet Luna PCIe HSM or SafeNet Luna Backup HSM. To access the HSM-level commands on SafeNet Luna Network HSM, use LunaSH (see "hsm" on page 1).

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.

Examples

```
lunacm:>hsm showpolicies
        HSM Capabilities
                0: Enable PIN-based authentication : 0
                1: Enable PED-based authentication : 1
                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 : 1
               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 : 1
               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

     HSM Policies
           1: PED-based authentication : 1
           7: Allow cloning : 1
          12: Allow non-FIPS algorithms : 1
          15: SO can reset partition PIN : 0
          16: Allow network replication : 0
          21: Force user PIN change after set/reset : 1
          22: Allow offboard storage : 1
          25: Allow remote PED usage : 1
          30: Allow unmasking : 1
          33: Current maximum number of partitions : 100
          37: Allow MofN : 1
          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 : 0


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 154. Use the command "hsm tampershow" on the next page to display detailed information for the tamper.

> **NOTE** The **hsm** commands appear only when LunaCM's active slot is set to the administrative partition on a SafeNet Luna PCIe HSM or SafeNet Luna Backup HSM. To access the HSM-level commands on SafeNet Luna Network HSM, use LunaSH (see "hsm" on page 1).

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** commands appear only when LunaCM's active slot is set to the administrative partition on a SafeNet Luna PCIe HSM or SafeNet Luna Backup HSM. To access the HSM-level commands on SafeNet Luna Network HSM, use LunaSH (see "hsm" on page 1).

Syntax

hsm tampershow

Example

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

Command Result : No Error
```

hsm updatecap

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

> **NOTE** The **hsm** commands appear only when LunaCM's active slot is set to the administrative partition on a SafeNet Luna PCIe HSM or SafeNet Luna Backup HSM. To access the HSM-level commands on SafeNet Luna Network HSM, use LunaSH (see "hsm" on page 1).

On SafeNet Luna Network HSM, these upgrades are obtained via the Thales Group 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 SafeNet Luna HSM. LunaCM performs an automatic restart following a firmware update.

> **NOTE** The **hsm** commands appear only when LunaCM's active slot is set to the administrative partition on a SafeNet Luna PCIe HSM or SafeNet Luna Backup HSM. To access the HSM-level commands on SafeNet Luna Network HSM, use LunaSH (see).

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** commands appear only when LunaCM's active slot is set to the administrative partition on a SafeNet Luna PCIe HSM or SafeNet Luna Backup HSM. To access the HSM-level commands on SafeNet Luna Network HSM, use LunaSH (see "hsm" on page 1).

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
```

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.

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
    clear
    clone
    contents
    createchallenge
    init
    login
    logout
    resize
    restoresim3
    setlegacydomain
    showinfo
    showmechanism
    showpolicies

Argument(s)	Shortcut	Description
addsize	**as**	Increase the size of a partition by a specific number of bytes. See "partition addsize" on page 90.
archive	**ar**	Partition archive management commands. See "partition archive" on page 92.
changelabel	**changel**	Change the specified partition's label. See "partition changelabel" on page 106.
changepolicy	**changepo**	Change the Partition Policy value. See "partition changepolicy" on page 107
clear	**clr**	Delete all of the user's token objects. See "partition clear" on page 108.
clone	**clo**	Clone user objects. See "partition clone" on page 109.

Argument(s)	Shortcut	Description
contents	**con**	Show the contents of the user partition. See "partition contents" on page 111.
init	**in**	Initialize an application partition. See "partition init" on page 112.
login	**logi**	Log in to an HA group using the common Crypto Officer password or challenge secret. See "partition login" on page 114.
logout	**logo**	Log out of an HA group. See "partition logout" on page 115.
restoresim3file	**rsim3f**	Restore user objects (using SIM3). See "partition restoresim3file" on page 118.
setlegacydomain	**sld**	Set the legacy domain. "partition setlegacydomain" on page 119.
showinfo	**si**	Display partition information. See "partition showinfo" on page 121.
showmechanism	**showm**	Show all available mechanisms. See "partition showmechanism" on page 122.
showpolicies	**sp**	Get partition policy information. See "partition showpolicies" on page 124.

partition addsize

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

This command is applicable to SafeNet 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 SafeNet Luna PCIe HSM

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 SafeNet Luna Backup HSM
When using a password-authenticated SafeNet 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 98.
delete	d	Delete the specified backup partition in a backup device in a specified slot. See "partition archive delete" on page 100.
list	l	List the backup partitions on a backup device in a specified slot. See "partition archive list" on page 102.
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 104.

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.

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.

Syntax

If backup device is a slot in the current system:
partition archive backup -slot <backup_slot> **-partition** <backup_partition> **-password** <password> [**-sopassword** <sopassword>] [**-domain** <domain> | **-defaultdomain**] [**-append**] [**-replace**] [**-debug**] [**-force**]

If backup device is in a remote workstation:
partition archive backup -slot remote -hostname <hostname> **-port** <portnumber> **-partition** <backup_partition> **-password** <password> [**-sopassword** <sopassword>] [**-commandtimeout** <seconds>] [**-domain** <domain> | **-defaultdomain**] [**-append**] [**-replace**] [**-debug**] [**-force**]

If backup device is a USB-attached HSM:
partition archive backup -slot direct -partition <backup_partition> **-password** <password> [**-sopassword** <sopassword>] [**-domain** <domain> | **-defaultdomain**] [**-append**] [**-replace**] [**-debug**] [**-force**]

Argument(s)	Shortcut	Description
-append	**-a**	Append the objects to the existing partition.
-commandtimeout <seconds>	**-ct**	The command timeout for network communication. The default timeout is 10 seconds. The maximum timeout is 3600. This option can be used to adjust the timeout value to account for network latency.
-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.
-hostname <hostname>	**-ho**	Host name of remote workstation running remote backup server. (required when **-s remote** is used)
-partition <backup_partition>	**-par**	Partition on the backup device. (maximum length of 64 characters)
-password <password>	**-pas**	Password for the specified partition.
-port <portnumber>	**-po**	Port number for remote backup server on remote workstation. (required when **-s remote** is used)
-replace	**-rep**	Allow objects with same OUID on backup device to be deleted and replaced.
-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. **>** **remote -hostname** <host name> **-port** <port number> if the backup device is in a remote work station. **>** **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**)
-sopassword <sopassword>	**-sop**	SO password for the backup device.

Example with password in command line

```
lunacm:> partition archive backup -slot 2 -partition sa78backup -domain clientdomain -password
newPa$$w0rd -sopassword backupSOpwd

        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 with password prompt

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

Option -domain was not specified. It is required.
 Enter the domain name: ***
 Re-enter the domain name: ***
 Option -password was not supplied. It is required.
 Enter the user password for the target partition: ***
 Re-enter the user password for the target partition: ***
   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 if password mistyped

```
lunacm:>partition archive backup -slot 21 -partition bkpar3

Option -domain was not specified. It is required.
 Enter the domain name: ***
```

```
 Re-enter the domain name: ***
 Option -password was not supplied. It is required.
 Enter the user password for the target partition: ***
 Re-enter the user password for the target partition: ***
The passwords are not the same.
Command aborted.
Command Result : 0xb (User Cancelled Operation)
```

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> [**-commandtimeout** <seconds>] [**-debug**

Argument(s)	Shortcut	Description
-commandtimeout <seconds>	**-ct**	The command timeout for network communication. The default timeout is 10 seconds. The maximum timeout is 3600. This option can be used to adjust the timeout value to account for network latency. (optional)
-debug	**-deb**	Turn on additional error information. (optional)
-hostname <hostname>	**-ho**	Host name of remote workstation running remote backup server (required when **-s remote** is used)
-partition <backup_partition>	**-par**	Partition on the backup device. (maximum length of 64 characters) .
-password	**-pas**	User password for the specified partition.
-port <portnumber>	**-po**	Port number for remote backup server on remote workstation (required when **-s remote** is used)
-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. > **remote -hostname** <host name> **-port** <port number> if the backup device is in a remote work station. > **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

If backup device is a slot in the current system:
partition archive delete -slot <backup_slot> **-partition** <backup_partition> **-password** <password> [**-debug**]

If backup device is in a remote workstation:
partition archive delete -slot remote -hostname <hostname> **-port** <portnumber> **-partition** <backup_partition> **-password** <password> [**-commandtimeout** <seconds>] [**-debug**]

If backup device is a USB-attached device:
partition archive delete -slot direct [**-slot** <backup_slot>] **-partition** <backup_partition> **-password** <password> [**-debug**]

Argument(s)	Shortcut	Description
-commandtimeout <seconds>	**-ct**	The command timeout for network communication. The default timeout is 10 seconds. The maximum timeout is 3600. This option can be used to adjust the timeout value to account for network latency. (optional)
-debug	**-deb**	Turn on additional error information. (optional)
-hostname <hostname>	**-ho**	Host name of remote workstation running remote backup server. (required when **-s remote** is used)
-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.
-port <portnumber>	**-po**	Port number for remote backup server on remote workstation. (required when **-s remote** is used)

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. > **remote -hostname** <host name> **-port** <port number> if the backup device is in a remote work station. > **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 SafeNet 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
```

partition archive list

Display a list of the backup partitions on a backup device in a specified slot.

Syntax

If backup device is a slot in the current system:
partition archive list -slot <backup_slot> [**-debug**]

If backup device is in a remote workstation:
partition archive list -slot remote -hostname <hostname> **-port** <portnumber> [**-commandtimeout** <seconds>] [**-debug**]

If backup device is a USB-attached device:
partition archive list -slot direct [**-slot** <backup_slot>] [**-debug**]

Argument(s)	Shortcut	Description
-commandtimeout <seconds>	**-ct**	The command timeout for network communication. The default timeout is 10 seconds. The maximum timeout is 3600. This option can be used to adjust the timeout value to account for network latency. (optional)
-debug	**-de**	Turn on additional error information. (optional)
-hostname <hostname>	**-ho**	Host name of remote workstation running remote backup server. (required when **-s remote** is used)
-port <portnumber>	**-po**	Port number for remote backup server on remote workstation. (required when **-s remote** is used)
-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. > **remote -hostname** <host name> **-port** <port number> if the backup device is in a remote work station. > **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 2

        HSM Storage Information for slot 2:
```

```
        Total HSM Storage Space: 16252928
        Used HSM Storage Space:  26432
        Free HSM Storage Space:  16226496
        Allowed Partitions:      20
        Number Of Partitions:    2

    Partition list for slot 2

        Number of partition: 2

        Name:                    sa78backup
        Total Storage Size:      9480
        Used Storage Size:       9348
        Free Storage Size:       132
        Number Of Objects:       6

        Name:                    sa40backup
        Total Storage Size:      12640
        Used Storage Size:       12464
        Free Storage Size:       176
        Number Of Objects:       8

Command Result : No Error
```

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 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.

Syntax

If backup device is a slot in the current system:
partition archive restore -slot <backup_slot> **-partition** <backup_partition> **-password** <password> [**-replace**] [**-debug**]

If backup device is in a remote workstation:
partition archive restore -slot remote -hostname <hostname> **-port** <portnumber> **-partition** <backup_partition> **-password** <password> [**-commandtimeout** <seconds>] [**-replace**] [**-debug**]

If backup device is a USB-attached device:
partition archive restore -slot direct [**-slot** <backup_slot>] **-partition** <backup_partition> **-password** <password> [**-replace**] [**-debug**]

Argument(s)	Shortcut	Description
-commandtimeout <seconds>	**-ct**	The command timeout for network communication. The default timeout is 10 seconds. The maximum timeout is 3600. This option can be used to adjust the timeout value to account for network latency. (optional)
-debug	**-deb**	Turn on additional error information. (optional)
-hostname <hostname>	**-ho**	Host name of remote workstation running remote backup server. (required when **-s remote** is used)

Argument(s)	Shortcut	Description
-partition <backup_partition>	**-par**	Partition on the backup device. (maximum length of 64 characters) .
-password <password>	**-pas**	User password for the specified partition.
-port <portnumber>	**-po**	Port number for remote backup server on remote workstation. (required when **-s remote** is used)
-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. > **remote -hostname** <host name> **-port** <port number> if the backup device is in a remote work station. > **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 restore -slot 6 -password Pa$$w0rd -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 has software and/or firmware dependencies. See "Version Dependencies by Feature" on page 1 for more information.

Syntax

partition changelabel -label <newlabel> [**-slot** <slotnumber>] [**-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.
-slot <slotnumber>	**-s**	This option is deprecated -- you can change the partition label only on the currently-active slot.

Example

```
lunacm:> partition changelabel -label "user partition 0"

        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:> slot list

        Slot Id ->              0
        Label ->                user partition 0
        Serial Number ->        1238700701509
        Model ->                LunaSA 7.2.0
        Firmware Version ->     7.2.0
        Configuration ->        Luna User Partition With SO (PW) Key Export With Cloning Mode
        Slot Description ->     Net Token Slot


        Current Slot Id: 0


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> [**-slot** <slot_number>] [**-value** <policy_value>] [**-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.
-slot <slot_number>	**-s**	Specifies the slot where the partition is located.
-value <policy_value>	**-v**	Specifies the new value for the specified policy.

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 124 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.

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
```

partition clone

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

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.

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 > zero, 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 PED-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:    79080000090000061b030100


        Number of objects:  4


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 PED-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!** When labeling HSMs or partitions, *never* use a numeral as the first, or only, character in the name/label. Token backup commands allow a slot-number OR a label as identifier, which can lead to confusion if the label is a string version of a slot number.
>
> For example, if the token is initialized with the label "1", the user cannot use the label to identify the target for backup purposes, because VTL parses "1" as the numeric ID of the first slot rather than as a text label for the target in the actual occupied slot.

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.

Partition name rules

A partition **name** or a partition **label** can include any of the following characters:

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

> No spaces, unless you wish to surround the name or label in double quotation marks every time it is used.

> No question marks, no double quotation marks within the string.

> Minimum name or label length is 1 character. Maximum is 32 characters.

Partition password and domain rules

Valid characters that can be used in a **password** or in a cloning **domain** are:

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

(the first character in that list is the space character)

Invalid or problematic characters, not to be used in passwords or cloning domains are "&';<>\`|()

Minimum password length is 7 characters; maximum is 255 characters.

Minimum domain string length is 1 character; maximum domain length is 128 characters.

Names and labels have an additional restriction, in that you should avoid a leading space.

Syntax

partition init -label <string> [**-password**<string>] [**-domain**<string>] [**-applytemplate** <filepath/filename>] [**-defaultdomain**] [**-auth**] [**-force**]

Argument(s)	Shortcut	Description
-applytemplate <filepath/filename>	**-at**	Apply a policy template located in the specified directory.
-auth	**-a**	Log in after the initialization.
-defaultdomain	**-def**	Default cloning domain name. *Deprecated.* Used only on password-authenticated HSMs, and not recommended. Kept for compatibility with previous, existing configurations; will be discontinued in a future release.
-domain	**-d**	Partition domain name. Used only on password-authenticated HSMs; ignored for PED-authenticated.
-force	**-f**	Force the action (useful for scripting).
-label	**-l**	Label for the partition.
-password	**-p**	Partition Security Officer Password. Used only on password-authenticated HSMs; ignored for PED-authenticated.

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
```

partition login

Log in to an HA group using the common Crypto Officer password or challenge secret. This command is only available in LunaCM 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 resize

Change the size of an application partition.

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:      20
          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.

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
```

partition setlegacydomain

Set the legacy cloning domain on a partition.

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 SafeNet Luna Network HSM partition.

The legacy cloning domain for PED-authenticated HSM partitions is the cloning domain secret on the red PED key for the legacy PED-authenticated HSM whose contents are to be migrated to the SafeNet Luna Network HSM 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 PED-authenticated HSM partition, and you cannot migrate objects from a PED authenticated token/HSM to a Password authenticated HSM partition. Again, this is a security provision.

See "About the Migration Guide" on page 1 in the *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.

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.

Syntax

partition showinfo

Examples

Partition Info for an application partition

```
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 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
```

```
      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 network-connected HSMs, use the LunaSH command "hsm showpolicies" on page 1 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.
-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.

Example

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

```
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
```

Verbose mode

```
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
```

ped

Access the Remote-PED configuration commands. These commands manage the use of Remote PED with your SafeNet 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 (RPK). Obviously, the commands to administer your HSM could be issued remotely as well, using SSH or remote desktop connection. See "About Remote PED" on page 1 in the *Administration Guide* for more information.

Syntax

ped

> **connect**
> **disconnect**
> **get**
> **set**
> **show**

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 130.
get	**g**	Show the PED ID and the listening slot ID. See "ped get" on page 131.
set	**se**	Set the PED ID. See "ped set" on page 132.
show	**sh**	Display the remote PED server configuration. See "ped show" on page 133.

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. See "ped set" on page 132 for more information.

Behavior when defaults are configured using ped set

The **ped set** 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. The behavior of the **ped connect** command when defaults are configured using **ped set** is as follows:

Values set with hsm ped set	Parameters specified by hsm ped connect	IP address used	Port used
IP address and port	None	IP address configured with **ped set**.	Port configured with **ped set**.
	IP address	IP address specified by **ped connect**	Port configured with **ped set**.
	Port	IP address configured with **ped set**.	Port specified by **ped connect**
	IP address and port	IP address specified by **ped connect**	Port specified by **ped connect**
IP address only	None	IP address configured with **ped set**.	Port 1503 (default).
	IP address	IP address specified by **ped connect**	Port 1503 (default).
	Port	IP address configured with **ped set**.	Port specified by **ped connect**.
	IP address and port	IP address specified by **ped connect**	Port specified by **ped connect**.

Values set with hsm ped set	Parameters specified by hsm ped connect	IP address used	Port used
Port only	None	Error. You must use the **-ip** parameter to specify an IP address.	Port configured with **ped set**.
	IP address	IP address specified by **ped connect**	Port configured with **ped set**.
	Port	Error. You must use the **-ip** parameter to specify an IP address..	Port specified by **ped connect**
	IP address and port	IP address specified by **ped connect**	Port specified by **ped connect**

Behavior when no defaults are configured using ped set

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>]

Argument(s)	Shortcut	Description
-ip <ip_address>	**-i**	Specifies the IP Address of the PED. If **-ip** is not specified, the configured ip, if any, is used.
-port <number>	**-p**	Network Port (0-65535). If **-port** is not specified, the default or the configured port is used. **Default:** 1503
-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

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.

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.

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 for more information. At least one (**-ip** or **-port**) must be specified.

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.

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
```

remotebackup start

Start the remote backup server on the current slot. Your SafeNet Luna Backup HSM must be connected to that computer and the SafeNet 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 138.
deactivate	**deact**	Deactivate role. See "role deactivate" on page 139.
init	**in**	Initialize a role on the partition. See "role init" on page 140.
list	**li**	List roles on the partition. See "role list" on page 141.
login	**logi**	Role login. See "role login" on page 142.
logout	**logo**	Role logout. See "role logout" on page 144.
recoveryinit	**ri**	Setup/configure for "Recovery Login". See "role recoveryinit" on page 145.
recoverylogin	**rl**	Login using"Recovery Login". See "role recoverylogin" on page 146.
resetpw	**r**	Reset password. See "role resetpw" on page 147.
setdomain	**d**	Set the domain for a role. See "role setdomain" on page 148.
show	**s**	Show state of a role. See "role show" on page 149.

role changepw

Change the password, PED key secret, or activation challenge password for a specified role.

Syntax

role changepw -name <role> [**-oldpw** <oldpassword>] [**-newpw** <newpassword>] [**-prompt**] [**-force**]

Argument(s)	Shortcut	Description
-name <role>	**-n**	Role to change password for.
-oldpw <oldpassword>	**-old**	Current password (for application partition on PW authenticated HSM) or current challenge secret (for application partition on PED 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 PW authenticated HSM) or new challenge secret (for application partition on PED 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 PED-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 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 userpin

        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
```

role createchallenge

Create a challenge secret for the Crypto Officer (CO) 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 PED-Authenticated Partitions" on page 1 in the *Administration Guide* 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 Crypto User. The target role must already exist. See "role init" on page 140.

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.

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 the command "role list" on the next page to see which roles are possible on the current partition/slot.

The Auditor role can exist only on the HSM's administrative partition, and shares that partition with the HSM Security Officer or SO. 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 the command **role setdomain**. See "role setdomain" on page 148.

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. Crypto User (CU). The CO initializes the CU. Audit (AU). The SO initializes the AU.
-password <password>	**-p**	The initial password for role, valid for the initial login only. **NOTE** The role must change the initial password using the command "role changepw" on page 136 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

```
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
        Crypto User         cu

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 PED-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.

> 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 107), 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 PW-authenticated.

Activation (caching of the PED key secret) persists until you explicitly deactivate (see "role deactivate" on page 139) 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 141 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)
        ========================
        Partition SO        po
        Crypto Officer      co
        Crypto User         cu

Command Result : No Error

lunacm:>role login -name po

        Please attend to the PED.

Command Result : No Error
```

role logout

This command logs the currently logged-in role out of a partition.

For PED-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. This command applies to SafeNet Luna PCIe HSM or SafeNet Luna USB HSM. Does not apply to SafeNet Luna Network HSM partitions that appear in LunaCM via NTLS or STC channel.

See also CKDemo "The HIGH AVAILABILITY RECOVERY Menu Functions" on page 1.

Syntax

role recoveryinit [**-plabel** <string>] [**-rlabel** <string>] [**-keyhandle** <number>] [**-force**]

Argument(s)	Shortcut	Description
-plabel <string>	**-pl**	RSA Public key label.
-rlabel <string>	**-rl**	RSA Private key label.
-keyhandle <number>	**-kh**	RSA Private key handle (optional).
-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. This command applies to SafeNet Luna PCIe HSM or SafeNet Luna USB HSM. Does not apply to SafeNet Luna Network HSM partitions that appear in LunaCM via NTLS or STC channel.

See also CKDemo "The HIGH AVAILABILITY RECOVERY Menu Functions" on page 1.

Syntax

role recoverylogin -user <username> **-slot** <slotnumber> **-keyhandle** <number>

Argument(s)	Shortcut	Description
-user <username>	**-pl**	User name.
-slot <slotnumber>	**-s**	Target slot.
-keyhandle <number>	**-kh**	Handle of RSA Private key to use.

Example

```
lunacm:>role recoverylogin -user somebody -slot 3 -keyhandle 46
```

role resetpw

Resets the password for a specified role. 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 partition is possible only from the administrative partition.

Syntax

role resetpw -name <role> [**-password** <password>] [**-slot** <slotnumber>]

Argument(s)	Shortcut	Description
-name <role>	**-n**	Name of role to have password reset.
-password <password>	**-p**	Password for the specified role. Use this option for password-authenticated HSMs only. PED-authenticated HSMs will return an error.
-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 of a role. Used only by the HSM's Auditor user. 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.

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 PED-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 PED-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

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 SafeNet 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 SafeNet appliance or to a SafeNet 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.

If the Chrystoki.conf / Crystoki.ini configuration file [Presentation] setting "ShowAdminTokens=" is set to no, then the HSM administrative partition/slot is also unavailable, and LunaCM is not usable. If you know you have a working SafeNet Luna PCIe HSM or SafeNet Luna USB HSM attached to your Client computer and LunaCM shows no usable commands, then verify in your Chrystoki.conf or Crystoki.ini file that "ShowAdminTokens" is not set to no.

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 the next page
configshow	**cshow**	Show the configuration for a slot . See "slot configshow" on page 153.
list	**l**	List the available slots. See "slot list" on page 154.
partitionlist	**plist**	List the partitions for a slot. See "slot partitionlist" on page 156.
set	**s**	Set the current slot. See "slot set" on page 157.
showempty	**sempt**	Show empty slots and their types. See "slot showempty" on page 158.

slot configset

Identify and set a SafeNet Luna Backup HSM partition to access at the specified slot number.

This command is used only with a SafeNet 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 SafeNet DOCK reader. It is still available, and can be used on a SafeNet 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 SafeNet Luna Backup HSM is from older editions of SafeNet 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
```

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 SafeNet Luna HSMs installed or connected, or if you have SafeNet Luna Network HSM application partitions Ethernet-connected via NTLS or STC 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.

If the Chrystoki.conf / Crystoki.ini configuration file [Presentation] setting "ShowAdminTokens=" is set to no, then the HSM administrative partition/slot is also unavailable, and LunaCM is not usable. If you know you have a working SafeNet Luna PCIe HSM or SafeNet Luna USB HSM attached to your Client computer and LunaCM shows no usable commands, then verify in your Chrystoki.conf or Crystoki.ini file that "ShowAdminTokens" is not set to no.

Syntax

slot list

Example

```
lunacm:> slot list

        Slot Id ->              0
        Label ->                par0
        Serial Number ->        1238700701521
        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 ->        1238700701522
        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 ->              2
        Label ->                par2
        Serial Number ->        154438865317
        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 ->              3
        Label ->                myRBSG5Bk
        Serial Number ->        7000329
        Model ->                G5Backup
        Firmware Version ->     6.22.0
        Configuration ->        Luna HSM Admin Partition (PW) Backup Mode
        Slot Description ->     Net Admin Token Slot
        HSM Configuration ->    Luna HSM Admin Partition (PW) Backup Device
        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" on page 1 in the *Administration Guide.*

slot partitionlist

List the partitions for the specified slot. This is of interest when a cryptographic slot might contain more than one HSM partition. In general, one slot contains one partition, but a SafeNet Luna Backup HSM, for example, might occupy one cryptographic slot while containing many partitions (see).

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 103

        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 SafeNet 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
```

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 ->   5: Luna UHD Slot
        Slot Id ->   6: Luna UHD Slot
        Slot Id ->   7: Luna UHD Slot

        Current Slot Id: 0


Command Result : No Error
```

stc

> **NOTE** STC commands are used only for configuring partitions on the SafeNet Luna Network HSM.

Access the STC (secure trusted channel) setup commands. Use these commands to set up and manage an STC network link between a client and a partition.

See also "stcconfig" on page 173 for the STC configuration commands, which you can use to specify the network and security settings for the STC link.

Syntax

stc

> **disable**
> **enable**
> **identitycreate**
> **identitydelete**
> **identityexport**
> **identityshow**
> **partitionderegister**
> **partitionregister**
> **status**
> **tokeninit**
> **tokenlist**

Argument(s)	Shortcut	Description
disable	**d**	Disable STC for the current slot. See "stc disable" on page 161.
enable	**e**	Enable STC for the current slot. See "stc enable" on page 162.
identitycreate	**idc**	Create a client identity on the STC client token. See "stc identitycreate" on page 163.
identitydelete	**idd**	Delete a client identity from the STC identity token. See "stc identitydelete" on page 164.
identityexport	**ide**	Export the STC client identify to a file. See "stc identityexport" on page 165.
identityshow	**idsh**	Display the client name, public key hash, and registered partitions for the STC client token. See "stc identityshow" on page 166.
partitionderegister	**pard**	Remove a partition identity from the STC client token. See "stc partitionderegister" on page 167.

Argument(s)	Shortcut	Description
partitionregister	**parr**	Register a partition to the STC client token. See "stc partitionregister" on page 168
status	**s**	Display status and configuration information for an STC link. See "stc status" on page 169.
tokeninit	**ti**	Initialize a client token. See "stc tokeninit" on page 170.
tokenlist	**tl**	List the available STC client identity tokens. See "stc tokenlist" on page 172.

stc disable

Disable STC for the current slot. This command changes the port for the client-partition network link from STC to NTLS and saves the change to the **ServerPort00** statement in the **Chrystoki.conf** (Linux) or **crystoki.ini** (Windows) file.

> **NOTE** Disabling the STC link will restart LunaCM. All sessions logged in through LunaCM will be closed. Sessions logged in through other applications will remain active.

Syntax

stc disable -id <server_ID> [**-force**]

Argument(s)	Shortcut	Description
-id <server_ID>	**-i**	Specifies the identifier of the SafeNet Luna Network HSM appliance to which you want to disable STC, as displayed using the command "clientconfig listservers" on page 41.
-force	**-f**	Force the action without prompting.

Example

```
lunacm:> stc disable

        You are about to disable STC to server 192.20.11.40
        The following slot will be affected:

        0,1,2,3

        This will initiate an automatic restart of this application. All sessions
        logged in through the application will be closed.
        Are you sure you wish to continue?

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

        Successfully disabled STC to connect to server 192.20.11.40.

Command Result : No Error
```

stc enable

Enable STC on the current HSM/partition. This command changes the port for the client-partition network link from NTLS to STC and saves the change to the **ServerPort00** statement in the **Chrystoki.conf** (Linux) or **crystoki.ini** (Windows) file.

This command is valid only if the STC policy is enabled on both the HSM and the partition. See "Enabling or Disabling STC on the HSM" on page 1 and "Enabling or Disabling STC on a Partition" on page 1 in the *Administration Guide*.

> **CAUTION!** Enabling the STC link terminates all existing NTLS sessions.

Syntax

stc enable -id <server_ID> [**-force**]

Argument(s)	Shortcut	Description
-force	**-f**	Force the action without prompting.
-id <server_ID>	**-i**	Specifies the identifier of the SafeNet Luna Network HSM appliance to which you want to disable STC, as displayed using the command "clientconfig listservers" on page 41.

Example

```
lunacm:> clientconfig listservers

 Server ID  Server                    Channel  HTL Required
 _____

 0          192.20.11.78              NTLS     no

 1          192.20.11.40              NTLS     no


Command Result : No Error



lunacm:> stc enable -id 1

        You are about to enable STC to server 192.20.11.40.
        This will initiate an automatic restart of this application. All sessions
        logged in through the application will be closed.

        Are you sure you wish to continue?

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

        Successfully enabled STC to connect to server 192.20.11.40.

Command Result : No Error
```

stc identitycreate

Create a client identity on the STC client token. After it is created, the client identity is exported to the following path:

<luna_client_root_dir>/**data/client_identities/**<client-name>

> **NOTE** If a client identity already exists, a warning is displayed. If you choose to create a new identity, all currently registered partition identities will be removed and will need to be registered to the new client identity.

Syntax

stc identitycreate -label <label> [**-force**]

Argument(s)	Shortcut	Description
-label <label>	**-l**	Specifies the token label.
-force	**-f**	Force the action without prompting.

Example

```
lunacm:> stc identitycreate -label client1

Client identity client1 successfully created and exported to file C:\Program
Files\SafeNet\LunaClient\data\client_identities\client1

Command Result : No Error
```

stc identitydelete

Delete a client identity from the STC identity token. This command, in conjunction with "stc identitycreate" on the previous page allows you to re-generate the token identity key pair if required for security reasons (for example, if the token is comprmised), or for administrative reasons (for example, to perform a key rotation).

This command does the following, in the order specified:

1. Deletes the client identity public key in the partition.

2. Deletes each registered partition identity.

3. Deletes the client identity.

If any of the identities fail to be deleted, the command will report the failure but will continue to delete the client identity.

> **CAUTION!** Deleting the client identity results in the loss of all partitions registered to the client. Any applications using those partitions will experience a loss of service.

Syntax

stc identitydelete [**-force**]

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

Example

```
lunacm:> stc identitydelete

Are you sure you want to delete the client identity client1?

All the partition registrations will be lost. Any applications using this
client identity will subsequently be affected.

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

Successfully deleted client identity client1.

Command Result : No Error
```

stc identityexport

Export the STC client identify to a file. This command allows you to reuse the client identity to re-establish a new STC channel in the event that the partition that originally used the channel no longer exists.

Syntax

stc identityexport [**-file** <file_path>]

Argument(s)	Shortcut	Description
-file <file_path>	**-f**	Specifies the full path of the file to which you want to export the client identity. If this parameter is not specified, the client identity is saved to the following location: <luna_client_root_dir>**/data/client_identities/**<client-name>

Example

```
lunacm:> stc identityexport

Successfully exported the client identity to C:\Program Files\SafeNet\LunaClient\data\client_
identities\client1

Command Result : No Error
```

stc identityshow

Display the following information for the STC client token:

> The client identity name

> The public key SHA1 hash for the client identity

> A list of the partitions registered with the client identity

Syntax

stc identityshow

Example

```
lunacm:> stc identityshow

Client Identity Name:           client1
Public Key SHA1 Hash:           d11c9d27884788332124d1417fffa07b8acd0c45
List of Registered Partitions:

Partition Identity      Partition          Partition Public Key SHA1 Hash
Label                   Serial Number
_____

par0                    1238700701521      5b198518dbb6146f5a0ee78a8605b24de0191601
par1                    1238700701522      3525218101b446e830464e3a39bb08bba6d0869c
par2                    1238700701523      3e486cf08dd502ac8d5d3c6d4b81f4735c72ecec
par3                    154438865321       440fe709d45ddab5833192d2ef2142a982019a7d
par4                    154438865322       988d88995e4a336f0a6d0ecee5f91de09598725d
par5                    154438865323       f4d50c439fe8159778e76c9efdde1cb1ee40dcc0


Command Result : No Error
```

stc partitionderegister

Remove the partition identity public key that is currently registered to the STC client token. Use this command if you no longer require access to a registered partition.

After invoking this command, use the command to restart LunaCM and refresh the slot list.

> **CAUTION!** Deregistering a partition disables the STC link. Any applications using the partition will lose access to the partition.

Syntax

stc partitionderegister -serial <partition_serialnum> [**-force**]

Argument(s)	Shortcut	Description
-serial <partition_serialnum>	**-s**	Specifies the serial number of the partition to deregister.
-force	**-f**	Force the action without prompting.

Example

```
lunacm:> stc partitionderegister -serial 98730559

Are you sure you want to deregister the partition 98730559?

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

Partition 98730559 successfully deregistered from the client token.

Command Result : No Error
```

stc partitionregister

Register the partition in the current slot to the STC client token.

After invoking this command, use the command to restart LunaCM and refresh the slot list.

Syntax

stc partitionregister -file <partition_ID_filepath> [**-label** <partition_ID_label>]

Argument(s)	Shortcut	Description
-file <partition_id_filepath>	**-f**	Specifies the path to the partition identity file.
-label <partition_id_label>	**-l**	Specifies a label for the partition identity.

Example

```
lunacm:> stc partitionregister par0 -file /usr/safenet/lunaclient/partition_
identities/359693009026.pid

Partition identity 359693009026 successfully registered.

Command Result : No Error
```

stc status

Display the STC status and configuration information for the current slot, or for all slots.

Syntax

stc status [**-all**]

Argument(s)	Shortcut	Description
-all	**-a**	Display the STC status for all slots.

Example

> **NOTE** The key life is displayed only if allowed by the partition security policy settings.

```
lunacm:> stc status

Enabled:            Yes
Status:             Connected
Channel ID:         1
Cipher Name:        AES 256 Bit with Cipher Block Chaining
HMAC Name:          HMAC with SHA 512 Bit


Command Result : No Error



lunacm:> stc status -all

Slot ID       Enabled      State       Channel ID    Cipher Name    HMAC name
_____

0             Yes          Connected    1            AES256_CBC     HMAC_SHA512

1             Yes          Connected    2            AES256_CBC     HMAC_SHA512

2             Yes          Connected    3            AES256_CBC     HMAC_SHA512

3             Yes          Connected    7            AES256_CBC     HMAC_SHA512

4             Yes          Connected    8            AES256_CBC     HMAC_SHA512


Command Result : No Error
```

stc tokeninit

Initialize an STC client identity token. You must run this command on a Windows client if you are initializing an eToken 7300 hard token.

Use the command to list the available tokens and to determine whether the token has been initialized.

> **NOTE** Re-initializing a token deletes all information stored in the token (client identity and the list of all registered partition identities).

Syntax

stc tokeninit -label <token_label> [**-force**]

Argument(s)	Shortcut	Description
-label <token_label>	**-l**	Specifies the label of the token.
-force	**-f**	Force the action without prompting.

Example

Uninitialized token

```
lunacm:> stc tokeninit -label token1

Successfully initialized the client token.

Command Result : No Error
```

Previously initialized token

```
lunacm:> stc tokeninit -label token1

The client token token1 is already initialized with the following client identity:

Client Identity Name:          client1
Public Key SHA1 Hash:          d11c9d27884788332124d1417fffa07b8acd0c45
List of Registered Partitions:

 Partition Identity    Partition        Partition Public Key SHA1 Hash
 Label                 Serial Number
 _____

 par0                  154438865321     440fe709d45ddab5833192d2ef2142a982019a7d
 par1                  154438865322     988d88995e4a336f0a6d0ecee5f91de09598725d
 par2                  154438865323     f4d50c439fe8159778e76c9efdde1cb1ee40dcc0

Re-initialization will delete the client identity and remove existing partition registrations.

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

Successfully initialized the client token.
```

```
Command Result : No Error
```

stc tokenlist

List the available STC client identity tokens. Use this command to determine the following:

> Which token to use when setting up a token using the command "stc tokeninit" on page 170

> Whether the token has been initialized.

> **NOTE** Only one token per client is supported.

Syntax

stc tokenlist

Example

```
lunacm:> stc tokenlist


 Token Slot ID   Token Label                     Serial Number    Initialized

 ──────────────────────────────────────────────────────────────────────────────

 1               token1                          55f3f968b2       Yes



Command Result : No Error
```

stcconfig

Access the STC configuration commands. Use these commands to specify the network and security settings for an STC link between a client and a partition.

See also "stc" on page 159 for STC setup commands, which you can use to set up and manage an STC network link.

Syntax

stcconfig

> **activationtimeoutset**
> **activationtimeoutshow**
> **cipherdisable**
> **cipherenable**
> **ciphershow**
> **clientderegister**
> **clientlist**
> **clientregister**
> **hmacdisable**
> **hmacenable**
> **hmacshow**
> **partitionidexport**
> **partitionidshow**
> **rekeythresholdset**
> **rekeythresholdshow**

Argument(s)	Shortcut	Description
activationtimeoutset	**atse**	Set the activation timeout for an STC link. See "stcconfig activationtimeoutset" on page 175.
activationtimeoutshow	**atsh**	Display the activation timeout for an STC link. See "stcconfig activationtimeoutshow" on page 176.
cipherdisable	**cid**	Disable the use of a symmetric encryption cipher algorithm for data encryption on an STC link. See "stcconfig cipherdisable" on page 177.
cipherenable	**cie**	Enable the use of a symmetric encryption cipher algorithm for data encryption on an STC link. See "stcconfig cipherenable" on page 178.
ciphershow	**cish**	List the symmetric encryption cipher algorithms you can use for data encryption on an STC link. See "stcconfig ciphershow" on page 179.

Argument(s)	Shortcut	Description
clientderegister	**cld**	Deregister a client's STC public key from a partition. See "stcconfig clientderegister" on page 180.
clientlist	**cll**	List the clients registered to a partition. See "stcconfig clientlist" on page 181.
clientregister	**clr**	Register a client's STC public key to a partition. See "stcconfig clientregister" on page 182.
hmacdisable	**hmd**	Disable the use of an HMAC message digest algorithm for message integrity verification on an STC link. See "stcconfig hmacdisable" on page 183.
hmacenable	**hme**	Enable the use of an HMAC message digest algorithm for message integrity verification on an STC link. See "stcconfig hmacenable" on page 184
hmacshow	**hsh**	List the HMAC message digest algorithms you can use for message integrity verification on an STC link. See "stcconfig hmacshow" on page 185.
partitionidexport	**pidex**	Export a partition's STC public key to a file. See "stcconfig partitionidexport" on page 186.
partitionidshow	**pish**	Display a partition's STC public key and serial number. "stcconfig partitionidshow" on page 187.
rekeythresholdset	**rkse**	Set the rekey threshold for the symmetric key used to encrypt data on an STC link. See "stcconfig rekeythresholdset" on page 188.
rekeythresholdshow	**rksh**	Display the rekey threshold for the symmetric key used to encrypt data on an STC link. See "stcconfig rekeythresholdshow" on page 189.

stcconfig activationtimeoutset

Set the activation timeout for an STC link. The activation timeout is the maximum time allowed to establish the STC link before the channel request is dropped.

Syntax

stcconfig activationtimeoutset -time <seconds> [**-slot** <slot_ID>]

Argument(s)	Shortcut	Description
-slot <slot_ID>	**-s**	Specifies the slot containing the partition for which you want to set the STC link activation timeout. This argument is available only if you are logged into the HSM's Admin partition.
-time <seconds>	**-t**	Specifies the activation timeout, in seconds. **Range:** 1-240 **Default:** 120

Example

```
lunacm:> stcconfig activationtimeoutset -time 30

Successfully changed the activation timeout for the current slot to 30 seconds.
```

stcconfig activationtimeoutshow

Display the activation timeout for an STC link. The activation timeout is the maximum time allowed to establish the STC link before the channel request is dropped.

Syntax

stcconfig activationtimeoutshow -slot <slot_ID>

Argument(s)	Shortcut	Description
-slot <slot_ID>	**-s**	Specifies the slot containing the partition for which you want to display the STC link activation timeout. This argument is available only if you are logged into the HSM's Admin partition.

Example

Current slot

```
lunacm:> stcconfig activationtimeoutshow

The activation timeout for the current slot is 30 seconds.

Command Result : No Error
```

stcconfig cipherdisable

Disable the use of a symmetric encryption cipher algorithm for data encryption on an STC link. All data transmitted over the STC link will be encrypted using the cipher that is both enabled and that offers the highest level of security. For example, if AES 192 and AES 256 are enabled, and AES 128 is disabled, AES 256 will be used. You can use the command "stcconfig ciphershow" on page 179 to show which ciphers are currently enabled and the command "stc status" on page 169 to display the cipher that is currently being used.

> **NOTE** Performance is reduced for larger ciphers.

Syntax

stcconfig cipherdisable -slot <slot_ID> **-id** <cipher_ID> [**-all**] [**-force**]

Argument(s)	Shortcut	Description
-all	**-a**	Disable all ciphers.
-force	**-f**	Force the action without prompting for confirmation.
-id <cipher_ID>	**-id**	Specifies the numerical identifier of the cipher you want to allow or disallow, as listed by "stcconfig ciphershow" on page 179
-slot <slot_ID>	**-s**	Specifies the slot containing the partition for which you want to allow or disallow a cipher algorithm. This argument is available only if you are logged into the HSM's Admin partition.

Example

```
lunacm:> stcconfig cipherdisable

This table lists the ciphers supported for STC links to the current slot.
Enabled ciphers are accepted during STC link negotiation with a client.
If all ciphers are disabled, STC links to the partition are not encrypted.

STC Encryption: On

 Cipher ID    Cipher Name                         Enabled
 _____

 1            AES 128 Bit with Cipher Block Chaining    No
 2            AES 192 Bit with Cipher Block Chaining    Yes
 3            AES 256 Bit with Cipher Block Chaining    Yes

Command Result : No Error

lunacm:> stcconfig cipherdisable -id 3

AES 256 Bit with Cipher Block Chaining is now disabled for the current slot.

Command Result : No Error
```

stcconfig cipherenable

Enable the use of a symmetric encryption cipher algorithm for data encryption on an STC link. All data transmitted over the STC link will be encrypted using the cipher that is both enabled and that offers the highest level of security. For example, if AES 192 and AES 256 are enabled, and AES 128 is disabled, AES 256 will be used. You can use the command "stcconfig ciphershow" on the next page to show which ciphers are currently enabled and the command "stc status" on page 169 to display the cipher that is currently being used.

> **NOTE** Performance is reduced for larger ciphers.

Syntax

stcconfig cipherenable -slot <slot_ID> **-id** <cipher_ID> [**-all**]

Argument(s)	Shortcut	Description
-all	**-a**	Enable all ciphers.
-id <cipher_ID>	**-id**	Specifies the numerical identifier of the cipher you want to allow or disallow, as listed by "stcconfig ciphershow" on the next page
-slot <slot_ID>	**-s**	Specifies the slot containing the partition for which you want to allow or disallow a cipher algorithm. This argument is available only if you are logged into the HSM's Admin partition.

Example

```
lunacm:> stcconfig ciphershow

This table lists the ciphers supported for STC links to the current slot.
Enabled ciphers are accepted during STC link negotiation with a client.
If all ciphers are disabled, STC links to the partition are not encrypted.

STC Encryption: On

 Cipher ID    Cipher Name                             Enabled
 _____

 1            AES 128 Bit with Cipher Block Chaining   No
 2            AES 192 Bit with Cipher Block Chaining   Yes
 3            AES 256 Bit with Cipher Block Chaining   Yes

Command Result : No Error

lunacm:> stcconfig ciphereneble -id 3

AES 256 Bit with Cipher Block Chaining is now enabled for the current slot.

Command Result : No Error
```

stcconfig ciphershow

List the symmetric encryption cipher algorithms you can use for data encryption on an STC link.

Syntax

stcconfig ciphershow

Example

```
lunacm:> stcconfig ciphershow

This table lists the ciphers supported for STC links to the current slot.
Enabled ciphers are accepted during STC link negotiation with a client.
If all ciphers are disabled, STC links to the partition are not encrypted.

STC Encryption: On

  Cipher ID   Cipher Name                             Enabled
  _____

  1           AES 128 Bit with Cipher Block Chaining  Yes

  2           AES 192 Bit with Cipher Block Chaining  Yes

  3           AES 256 Bit with Cipher Block Chaining  Yes


Command Result : No Error
```

stcconfig clientderegister

Deregister a client's STC public key from a partition. You must be logged into the partition as the SO to use this command.

> **CAUTION!** Deregistering a client's public key disables the STC link to that client.

> **CAUTION!** If you delete the client identity for the partition SO, you will lose the partition. You can only recover by restoring the partition from a backup, with the help of the HSM SO.

Syntax

stcconfig clientderegister -label <client_label> [**-force**]

Argument(s)	Shortcut	Description
-force	**-f**	Force the action without prompting for confirmation.
-label <client_label>	**-l**	A string used to identify the client being deregistered.

Example

```
lunacm:> stcconfig clientderegister -label client2

Are you sure you want to deregister the client identity client2?

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

Successfully deregistered the client client2 from the current slot.

Command Result : No Error
```

stcconfig clientlist

List the clients registered to a partition.

Syntax

stcconfig clientlist

Example

```
lunacm:> stcconfig clientlist

 Client Name                    Client Public Key SHA1 Hash
 ──────────────────────────────────────────────────────────────

 Partition SO                   3472c9423f9faf2ce431fda7f845e53c783b7303

 client2                        8be55fa0f7ad688f1fa1f243c142a04fdaa8bf39


Command Result : No Error
```

stcconfig clientregister

Register a client's STC public key to a partition. You must be logged in to the partition as the SO to use this command.

> **NOTE** Each client identity registered to a partition uses 2332 bytes of storage on the partition. Before registering a client identity to a partition, ensure that there is adequate free space.

Syntax

stcconfig clientregister -label <client_label> **-file** <client_public_key>

Argument(s)	Shortcut	Description
-label <client_label>	**-l**	A string used to identify the client being registered.
-file <client_public_key>	**-f**	Specifies the full path to the client public key file.

Example

```
lunacm:> stcconfig clientregister -label client2 -file "C:\Program
Files\SafeNet\LunaClient\data\client_identities\client2"

Successfully registered the client client2 to the current slot.

Command Result : No Error
```

stcconfig hmacdisable

Disable the use of an HMAC message digest algorithm for message integrity verification on an STC link. The HMAC algorithm that is both enabled and that offers the highest level of security is used. For example, if SHA 256 and SHA 512 are enabled, SHA 512 is used. You can use the command "stcconfig hmacshow" on page 185 to show which HMAC message digest algorithms are currently enabled/disabled and the command "stc status" on page 169 to display the HMAC message digest algorithm that is currently being used.

Syntax

stcconfig hmacdisable -id <hmac_ID> [**-slot** <slot_ID>]

Argument(s)	Shortcut	Description
-id <hmac_ID>	**-i**	Specifies the numerical identifier of the HMAC message digest algorithm you want to use, as listed using "stcconfig hmacshow" on page 185
-slot <slot_ID>	**-s**	Specifies the slot containing the partition on which you want to allow or disallow an HMAC algorithm. This argument is available only if you are logged into the HSM's Admin partition.

Example

```
lunacm:> stcconfig hmacshow

This table lists the HMAC algorithms supported for STC links to the current slot.
Enabled algorithms are accepted during STC link negotiation with a client.
At least one HMAC algorithm must be enabled.

HMAC ID       HMAC Name                         Enabled
_____
0             HMAC with SHA 256 Bit             Yes
1             HMAC with SHA 512 Bit             Yes

Command Result : 0 (Success)



lunacm:> stcconfig hmacdisable -id 0

HMAC with SHA 256 Bit for the current slot is now disabled.

Command Result : 0 (Success)
```

stcconfig hmacenable

Enable the use of an HMAC message digest algorithm for message integrity verification on an STC link.The HMAC algorithm that is both enabled and that offers the highest level of security is used. For example, if SHA 256 and SHA 512 are enabled, SHA 512 is used. You can use the command "stcconfig hmacshow" on the next page to show which HMAC message digest algorithms are currently enabled/disabled and the command "stc status" on page 169 to display the HMAC message digest algorithm that is currently being used.

Syntax

stcconfig hmacenable -slot <slot_ID> **-id** <hmac_ID>

Argument(s)	Shortcut	Description
-id <hmac_ID>	**-i**	Specifies the numerical identifier of the HMAC message digest algorithm you want to use, as listed using "stcconfig hmacshow" on the next page
-slot <slot_ID>	**-s**	Specifies the slot containing the partition on which you want to allow or disallow an HMAC algorithm. This argument is available only if you are logged into the HSM's Admin partition.

Example

```
lunacm:> stcconfig hmacshow

This table lists the HMAC algorithms supported for STC links to the current slot.
Enabled algorithms are accepted during STC link negotiation with a client.
At least one HMAC algorithm must be enabled.

HMAC ID        HMAC Name                            Enabled
_____
0              HMAC with SHA 256 Bit                No
1              HMAC with SHA 512 Bit                Yes

Command Result : 0 (Success)



lunacm:> stcconfig hmacenable -id 0

HMAC with SHA 256 Bit for the current slot is now enabled.

Command Result : 0 (Success)
```

stcconfig hmacshow

List the HMAC message digest algorithms you can use for message integrity verification on an STC link.

Syntax

stcconfig hmacshow -slot <slot_ID>

Argument(s)	Shortcut	Description
-slot <slot_ID>	**-s**	Specifies the slot containing the partition whose available HMAC algorithms you want to display. This argument is available only if you are logged into the HSM's Admin partition.

Example

```
lunacm:> stcconfig hmacshow

This table lists the HMAC algorithms supported for STC links to the current slot.
Enabled algorithms are accepted during STC link negotiation with a client.
At least one HMAC algorithm must be enabled.

HMAC ID      HMAC Name                            Enabled
_____

0            HMAC with SHA 256 Bit                Yes

1            HMAC with SHA 512 Bit                Yes


Command Result : No Error
```

stcconfig partitionidexport

Export a partition's STC public key to a file.

> **NOTE** If the HSM is zeroized while STC is enabled, the STC link between LunaCM and the admin partition will no longer authenticate, since the admin partition identity no longer exists. If this occurs, you will be unable to log into, or initialize, the HSM. To recover from this state, run the **stcconfig partitionidexport** command without any parameters. When you run the command, a new identity is created for the admin partition, and the new admin partition public key is exported to the default directory. This will restore the STC link between LunaCM and the admin partition, allowing you to re-initialize the HSM. You can only run this command, while not logged into the HSM, if the HSM is zeroized.

Syntax

stcconfig partitionidexport -slot <slot_ID> [**-file** <filepath>]

Argument(s)	Shortcut	Description
-file <filepath>	**-f**	Specifies the full path to the file to which you want to export the partition's STC public key. If you omit this parameter the key is exported by default to the following file: <luna_client_root>/**identities/**<partition_serial_number>**.pem**
-slot <slot_ID>	**-s**	Specifies the slot containing the partition whose STC public key you want to export. This argument is available only if you are logged into the HSM's Admin partition.

Example

```
lunacm:> stcconfig partitionidexport

Successfully exported partition identity for the current slot to C:\Program
Files\SafeNet\LunaClient\data\partition_identities\154438865321.pid

Command Result : No Error
```

stcconfig partitionidshow

Display a partition's STC public key and serial number.

Syntax

stcconfig partitionidshow -slot <slot_ID>

Argument(s)	Shortcut	Description
-slot <slot_ID>	**-s**	Specifies the slot for the partition for which you want to display the public key and serial number. This argument is available only if you are logged into the HSM's Admin partition.

Example

```
lunacm:> stcconfig partitionidshow

Partition Serial Number:              154438865321
Partition Identity Public Key SHA1 Hash: 440fe709d45ddab5833192d2ef2142a982019a7d

Command Result : No Error
```

stcconfig rekeythresholdset

Set the rekey threshold for the symmetric key used to encrypt data on an STC link. The symmetric key is used to encode the number of messages specified by the threshold value, after which it is regenerated and the counter is reset to 0.

The default of 400 million messages would force a rekeying operation once every 24 hours on an HSM under heavy load (processing approximately 5000 messages/second), or once a week for an HSM under light load (processing approximately 700 messages/second).

Syntax

stcconfig rekeythresholdset -slot <slot_ID> **-value** <threshold>

Argument(s)	Shortcut	Description
-slot <slot_ID>	**-s**	Specifies the slot containing the partition for which you want to set the rekey threshold. This argument is available only if you are logged into the HSM's Admin partition.
-value <threshold>	**-v**	An integer that specifies the key life (in millions of encoded messages) for the STC symmetric key. Enter a value of **0** to disable rekeying. **Range:** 0 to 4000 million messages. **Default:** 400 million messages.

Example

```
lunacm:> stcconfig rekeythresholdset -value 600

Successfully changed the rekey threshold for the current slot to 600. (in millions of messages)

Command Result : No Error
```

stcconfig rekeythresholdshow

Display the rekey threshold for the symmetric key used to encrypt data on an STC link. The symmetric key is used for the number of times specified by the threshold value, after which it is regenerated and the counter is reset to 0.

Syntax

stcconfig rekeythresholdset -slot <slot_ID>

Argument(s)	Shortcut	Description
-slot <slot_ID>	**-s**	Specifies the slot containing the partition for which you want to display the rekey threshold. This argument is available only if you are logged into the HSM's Admin partition.

Example

```
lunacm:> stcconfig rekeythresholdshow

The current rekey threshold for the current slot is 400. (in millions of messages)

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 on a SafeNet Luna PCIe HSM or SafeNet Luna Backup HSM. Note that STM is unavailable on SafeNet Luna Backup HSM. To access the STM feature on SafeNet Luna Network HSM, use LunaSH (see "hsm stm" on page 1).

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" on page 1.

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 193.
transport	**t**	Access commands that allow you to enable or disable STM. See "stm transport" on page 194

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; 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 on a SafeNet Luna PCIe HSM or SafeNet Luna Backup HSM. Note that STM is unavailable on SafeNet Luna Backup HSM. To access the STM feature on SafeNet Luna Network HSM, use LunaSH (see "hsm stm" on page 1).

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

If you are confident the HSM has not been tampered with, you can still enter "**proceed**" to recover from STM. See "Secure Transport Mode" on page 1 for more information.

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 on a SafeNet Luna PCIe HSM or SafeNet Luna Backup HSM. Note that STM is unavailable on SafeNet Luna Backup HSM. To access the STM feature on SafeNet Luna Network HSM, use LunaSH (see "hsm stm" on page 1).

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 191 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 need to be logged in as the HSM SO to issue this command.

> **NOTE** The **stm** commands appear only when LunaCM's active slot is set to the administrative partition on a SafeNet Luna PCIe HSM or SafeNet Luna Backup HSM. Note that STM is unavailable on SafeNet Luna Backup HSM. To access the STM feature on SafeNet Luna Network HSM, use LunaSH (see "hsm stm" on page 1).

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 191).

To enter transport mode on a PED-authenticated HSM, provide the black PED key when prompted.

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
```