Luna G5

LunaCM Command Reference Guide

Document Information

Product Version	5.4.1
Document Part Number	007-011302-009
Release Date	04 July 2014

Revision History

Revision	Date	Reason
A	26 February 2014	Initial release.
B	17 April 2014	Updates to the SFF Backup feature.
C	04 July 2014	Solaris client support.

Trademarks

Disclaimer

SafeNet makes no representations or warranties with respect to the contents of this document and specifically disclaims any implied warranties of merchantability or fitness for any particular purpose. Furthermore, SafeNet reserves the right to revise this publication and to make changes from time to time in the content hereof without the obligation upon SafeNet to notify any person or organization of any such revisions or changes.

We have attempted to make these documents complete, accurate, and useful, but we cannot guarantee them to be perfect. When we discover errors or omissions, or they are brought to our attention, we endeavor to correct them in succeeding releases of the product.

SafeNet invites constructive comments on the contents of this document. Send your comments, together with your personal and/or company details to the address below.

Contact Method	Contact Information
Mail	SafeNet, Inc. 4690 Millennium Drive Belcamp, Maryland 21017 USA
Email	techpubs@safenet-inc.com

CONTENTS

PREFACE

About the LunaCM Command Reference Guide

This document describes how to do something (insert a brief description). It contains the following chapters:

This preface also includes the following information about this document:

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. It is strongly recommended that you 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 for this release at the following location:

- http://www.securedbysafenet.com/releasenotes/luna/crn_luna_hsm_5-4.pdf

Audience

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

All products manufactured and distributed by SafeNet, Inc. 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.
{**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.

Format	Convention
[**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 make sure that you have read the documentation. If you cannot resolve the issue, please contact your supplier or SafeNet support. SafeNet 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 SafeNet and your organization. Please consult this support plan for further information about your entitlements, including the hours when telephone support is available to you.

Table 1: Technical support contacts

Contact method	Contact	
Address	SafeNet, Inc. 4690 Millennium Drive Belcamp, Maryland 21017 USA	
Phone	United States	(800) 545-6608, (410) 931-7520
	Australia and New Zealand	+1 410-931-7520
	China	(86) 10 8851 9191
	France	0825 341000
	Germany	01803 7246269
	India	+1 410-931-7520
	United Kingdom	0870 7529200, +1 410-931-7520
Web	www.safenet-inc.com	
Support and Downloads	www.safenet-inc.com/support Provides access to the SafeNet Knowledge Base and quick downloads for various products.	
Technical Support Customer Portal	https://serviceportal.safenet-inc.com Existing customers with a Technical Support Customer Portal account can log in to manage incidents, get the latest software upgrades, and access the SafeNet Knowledge Base.	

CHAPTER 1
Using LunaCM

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

Accessing LunaCM

The LunaCM utility (lunacm) is the Client-side administrative command interface for Luna HSMs.

Previously, LunaCM's reach was confined to locally connected Luna HSMs - either an installed Luna PCI-E 5.x (K6 HSM card), or a USB-connected Luna G5 HSM. From Luna HSM 5.2 onward, LunaCM is now able to interact and perform operations on distantly located Luna HSM appliances (Luna SA).

Open a Command Prompt or console window.

Go to the LunaClient software directory and start the LunaCM utility.

Windows

c:\ cd c:\Program Files\SafeNet\LunaClient

c:\Program Files\SafeNet\LunaClient\> lunacm

Linux and Solaris

> cd /usr/safenet/lunaclient/bin

./lunacm

General Operation

Some preliminary status information appears, followed by the LunaCM command-line prompt.

You can now issue any lunacm utility command, to manage your Luna HSM.
For a summary, type "help" and press [Enter].

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: The above example is for Password Authenticated Luna HSMs. For Trusted Path Authenticated HSM, do not type the password - you are directed to the Luna PED, which prompts for the required PED Key.

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

The following list provides links to the top level commands in the hierarchy. Select a link to display the command syntax or to help you to navigate to the sub-command you need:

appid

Access the appid-level commands to manage application IDs on the HSM.

Syntax

appid

open
close
set
info

Parameter	Shortcut	Description
open	**o**	Open a previously set access ID. See "appid open" on page 15
close	**c**	Close a previously set access ID. See "appid close" on page 13
set	**s**	Set an access ID. See "appid set" on page 16
info	**i**	Display information for the access IDs. See "appid info" on page 14

Example

```
lunacm:> help appid
The following sub commands are available:
Command         Short    Description
-------------------------------------
open            o        Open an Application Id for the User
close           c        Close an Application Id for the User
set             s        Set the Application Id
info            i        Display current Application Id information
Syntax: appid <sub command>
Command Result : No Error
```


appid close

Close 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".

> **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 <integer_value> **-minor** <integer_value>

Parameter	Shortcut	Description
-major	**-ma**	The major appid.
-minor	**-mi**	The minor appid.

Example

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

Command Result : No Error
lunacm:>
```

appid info

Display current application ID information

Syntax

appid info

appid open

Open 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".

> **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 <integer_value> **-minor** <integer_value>

Parameter	Shortcut	Description
-major	**-ma**	The major appid.
-minor	**-mi**	The minor appid.

Example

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

Command Result : No Error
lunacm:>
```


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".

> **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 <integer_value> **-minor** <integer_value>

Parameter	Shortcut	Description
-major	**-ma**	The major appid.
-minor	**-mi**	The minor appid.

Example

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

Command Result : No Error
lunacm:>
```


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.

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.

Syntax

audit

- **changepw**
- **config**
- **export**
- **import**
- **init**
- **login**
- **logmsg**
- **logout**
- **status**
- **time**
- **verify**

Parameter	Shortcut	Description
changepw	**changepw**	Change the Audit user password or PED key. See "audit changepw" on page 18.
config	**co**	Configure the audit parameters. See "audit config" on page 19.
export	**e**	Read the wrapped log secret from the HSM. See "audit export" on page 21.
import	**m**	Import the wrapped log secret to the HSM. See "audit import" on page 22.
init	**i**	Initialize the HSM Audit user. See "audit init" on page 23.
login	**logi**	Login to the HSM as the Audit user. See "audit login" on page 24.
logmsg	**logm**	Write a message to the HSM's log. See "audit logmsg" on page 25.
logout	**logo**	Logout from the HSM as the Audit user. See "audit logout" on page 26.
status	**s**	Show the status of the logging subsystem. See "audit status" on page 27.
time	**t**	Synchronize the HSM time to the host, or get the HSM time. See "audit time" on page 28.
verify	**v**	Verify a block of log messages. See "audit verify" on page 29.

audit changepw

Change the password or PED Key contents for the HSM Audit role. Both the old and the new PED Key are required for Luna HSM with PED Authentication. In the case of multiple HSMs in the host computer, the command works on the current slot.

Syntax

audit changepw

Example

```
lunacm:>audit changePw
Please enter the old password:
> *******
Please enter the new password:
> ********
Please re-enter the new password:
> ********
Command Result : No Error
```

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.

Syntax

audit config -parameter <parameter> **-value** <value> **-serial** <serialnum>

Parameter	Shortcut	Description
- parameter	-p	The parameter you want to configure. Valid parameters are as follows. The value enclosed in [ ] indicates the shortcut character for the parameter: [**e**]**vent**. Follow this parameter with the values for the events you want to include in the log, as described below. [**r**]**otation**. Follow this parameter with the value for the log rotation interval you want to use, as described below.
- value	-v	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 -p e -v u,s,f'. **Valid values for the rotation parameter** Enter one of the following options for the log rotation interval: • **[h]ourly** • **[d]aily** • **[w]eekly**

Parameter	Shortcut	Description
		• **[m]onthly** • **[n]ever**
- serial		Specify that the HSM Audit configuration is to be set for the appliance's onboard HSM, or for a USB-connected Luna G5 or Luna Backup HSM. Enter the serial number for the HSM you want to configure.

Example

```
audit config -p e -v all        log everything
audit config -p e -v none       log nothing
audit config -p e -v f          log all command failures
audit config -p e -v u,f,s      log all key usage requests, both success and failure
audit config -p r -v daily      rotate log daily
audit config -p r -v w          rotate log weekly

lunacm:>audit config -p e -v all
Warning:: 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.
```


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.

Syntax

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

Parameter	Shortcut	Description
file	**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.bin 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 file 2013-04-01nextlog.bin overwrite

Now that you have exported your log secret, if you wish to verify your logs
on another HSM see the 'audit import' command.
```

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.

Syntax

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

Parameter	Shortcut	Description
file	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 init

Initialize the Audit role on the HSM. This command attaches an audit domain and a role password for Password-authenticated HSMs, and creates a white Audit PED key for PED-authenticated HSMs. For PED-authenticated HSMs **audit init** also creates an audit domain, or receives an existing domain, so that selected HSMs are able to validate each others' HSM Audit Log files.

Because this command destroys any existing Audit role on the HSM, the user is asked to “proceed” unless the -force switch is provided at the command line.

Syntax

audit init [**-auth**] [**-force**]

Parameter	Shortcut	Description
-auth	**-a**	This option starts a login after the initialization completes.
-force	**-f**	If this option is included in the list, the audit role initialization action is forced without prompting the user for confirmation.

Example

```
lunacm:>audit init

The AUDIT role will be initialized.
Are you sure you wish to continue?
Type proceed to continue, or quit to quit now -> proceed

Please enter the domain to use for initializing the
Audit role (press <enter> to use the default domain):
> myauditdomain

Please enter the password:
> *******

Please re-enter password to confirm:
> *******

Command Result : No Error
```

Note: For PED-authenticated HSMs, after you type "proceed" you are referred to the PED (which must be connected and 'Awaiting command...') which prompts you for domain (red PED Key) and Audit authentication (white PED Key).

audit login

Login to the HSM as the Audit role.

Syntax

audit login [**-serial** <serialnum>] [**-password** <password>]

Parameter	Shortcut	Description
-serial	**-s** <serialnum>	HSM Serial Number - identifies which HSM is to accept the login, if you have a multiple Luna PCI-E modules installed, or a Backup HSM or a Luna G5 HSM locally connected to your host.
-password	**-p** <password>	The password of the HSM you are logging into. Used for Password-authenticated HSMs. If you prefer not to write the password, in the clear, on the command line, leave it out and you are prompted for it. Ignored for PED-authenticated HSMs. If the audit log area in the HSM becomes full, the HSM stops accepting most commands, and does not prompt for password when login is requested. In that case, provide the password with the command, and the login is accepted. Audit log full does not affect login for PED-auth HSMs.

Example

PED-authenticated HSM

```
lunacm:>audit login
Luna PED operation required to login as HSM Auditor - use Audit user (white) PED key.
'audit
Command Result : No Error
[myluna] lunacm:>
```

Password-authenticated HSM

```
[myluna]lunacm:>audit login
Please enter the password:
> ********
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.

Syntax

audit logmsg "<message>"

Example

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

Command Result : No Error
```


audit logout

Logout the the HSM Audit user.

Syntax

audit logout

Example

```
lunacm:>audit logout

'audit logout' successful.

Command Result : No Error
```

audit status

Displays the Audit logging info for the indicated HSM.

Syntax

audit status [-serial <serialnum>]

Parameter	Shortcut	Description
-serial	**-s**	Specifies the serial number of the HSM for which you want to display the HSM Audit configuration. This can be the appliance's onboard HSM, or a USB-connected Luna G5 or Luna Backup HSM.

Example

```
audit status

HSM Logging Status:

HSM found logging daemon
Logging has been configured
HSM is currently storing 0 log records.

HSM Audit Role: logged in
HSM Time  : Mon Dec 17 17:50:35 2012
HOST Time : Mon Dec 17 17:51:07 2012

Current Logging Configuration
-----------------------------
event mask        : Log everything
rotation interval : daily

Command Result : 0 (Success)
```


audit time

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.

Syntax

audit time [**sync** | **get**]

Parameter	Shortcut	Description
sync	**-s**	Synchronize the HSM time to the host time.
get	**-g**	Display the current HSM time.

Example

```
lunacm:> audit time sync
```


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.

Syntax

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

Parameter	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 f test.log s 21 e 56

Verified messages 21 to 56

Command Result : No Error
```

file display

Display the contents of a backup file.

Syntax

file display -filename <filename>

Parameter	Shortcut	Description
-filename	**-f**	Specify the name of the backup file to display. Enter this keyword followed by the name of an existing backup file..

Example

```
lunacm:> > file display -filename somepartfile

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

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


hagroup

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

Syntax

hagroup

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

Parameter	Shortcut	Description
addmember	**am**	Add a member to an HA group. See "hagroup addmember" on page 32.
addstandby	**as**	Add a standby member to an HA group. See "hagroup addstandby" on page 33.
creategroup	**c**	Create an HA group. See "hagroup creategroup" on page 34.
deletegroup	**d**	Delete an HA group . See "hagroup deletegroup" on page 35.
halog	**hl**	Configure the HA log file. See "hagroup halog" on page 36.
haonly	**ho**	Enable "HA Only" mode. See "hagroup haonly" on page 37.
interval	**i**	Set the HA recover retry interval. See "hagroup interval" on page 43
listgroups	**l**	List the currently-configured HA groups. See "hagroup listgroups" on page 38.
recover	**re**	Recover a failed HA member. See "hagroup recover" on page 39.
removemember	**rm**	Remove a member from an HA group. See "hagroup removemember" on page 40.
removestandby	**rs**	Remove a standby member from an HA group. See "hagroup removestandby" on page 41.
retry	**rt**	Set the HA recover retry count. See "hagroup retry" on page 42
synchronize	**s**	Synchronize an HA group. See "hagroup synchronize" on page 44

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 <serial_number> -l <label> -p <password> [-force]
-slot <slot_number> -l <label> -p <password> [-force]

Parameter	Shortcut	Description
-serialNumber	-se	Serial number of primary member. This parameter is mandatory if **-slotnumber** is not used. the serial number that identifies the HSM being added to the HA group.
-slot	-sl	Slot number of primary member - [mandatory if -serialnumber not used] a slot number to identify the HSM being added to the HA group.
-group	-g	Label for the group being joined - [mandatory] a label for the HA group being created.
-password	-p	Password for the HSM to add - [mandatory if Password-authenticated/ignored if PED] The password or challenge secret shared by group members.
-force	-f	Force the action - no prompting (useful for scripting).

Example

```
lunacm:> hagroup addmember -serialnumber 12345679 -label mygroup

Command Result : No Error
```


hagroup addstandby

Add a standby member to an HA group. Use the "-slot" option or the "-serialNumber" option to specify which HSM to add to the group. All PED authenticated HA group members must have a challenge created, and activation turned on, and all challenges must be the same.

Syntax

hagroup addstandby -serialnumber <serial number> **-group** <label>

Parameter	Shortcut	Description
-serialNumber	**-se**	Serial number of new standby member - the serial number that identifies the standby HSM being added to the HA group.
-group	**-g**	Label for the group being joined - a label for the HA group being created.

Example

```
lunacm:> hagroup addstandby -serialnumber 12345679 -group mygroup

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 <serial number> **-l** <label> **-p** <password>
-slot <slot number> **-l** <label> **-p** <password>

Parameter	Shortcut	Description
-serialNumber	**-se**	Serial number of primary member - [mandatory if **-slotnumber** not used] the serial number that identifies the primary member of the HA group.
-slot	**-sl**	Slot number of primary member - [mandatory if **-serialnumber** not used] a slot number to identify the primary member of the HA group.
-label	**-l**	Label for the new group - [mandatory] a label for the HA group being created.
-password	**-p**	Password for the primary member. The password is the text password and is mandatory for Password authenticated HSMs, or is the challenge secret for PED authenticated HSMs, shared by group members. If an HSM is intended to join an existing HA group, that HSM's password or challenge secret must be changed to match the password or secret used by the group, before the new member is added.

Example

```
lunacm:> hagroup createGroup -serialnumber 12345678 -label mygroup -password some-obscure-string

Command Result : No Error
```


hagroup deletegroup

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

Syntax

hagroup deletegroup -l <label>

Command	Short	Description
-label	**-l**	Label for the group being deleted - [mandatory] a label for the HA group being deleted.

Example

```
lunacm:> hagroup deleteGroup -label mygroup

Command Result : No Error
```


hagroup halog

Configure the HA log.

Syntax

haGroup halog

-disable
-enable
-maxlength <max_log_file_length>
-path <log_filepath>
-show

Parameter	Shortcut	Description
-disable	**-d**	Disable HA logging.
-enable	**-e**	Enable HA logging.
-maxlength	**-m**	Set the maximum length for the HA log file The default and minimum size is 256000.
-path	**-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 2560000

HA Log maximum file size was successfully set to 2560000.

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
```


hagroup haonly

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

Syntax

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

Command	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

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 myHA,
    please enter the password for the group members. Sync info
    not available in HA Only mode.

Enter the password: *******

    HA Group Label:  myHA
    HA Group Number:  150032
    Group Members:  150032, 951327
    Needs sync:  yes

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>

Command	Shortcut	Description
-group	**-g**	Specifies the label for the group to recover.

Example

```
lunacm:> hagroup recover -group myHAgroup

Command Result : No Error
```


hagroup removemember

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

Syntax

haGroup removeMember

-serialNumber <serial number> **-l** <label> **-p** <password> [**-force**]
-slot <slot number> **-l** <label> **-p** <password> [**-force**]

Parameter	Shortcut	Description
-serialNumber	**-se**	Serial number of primary member - [mandatory if -slotnumber not used] the serial number that identifies the primary member of the HA group.
-slot	**-sl**	Slot number of primary member - [mandatory if -serialnumber not used] a slot number to identify the primary member of the HA group.
-group	**-g**	Label for the new group - [mandatory] a label for the HA group being created.
-password	**-p**	Password for the HSM to remove - [mandatory if Password-authenticated/ignored if PED] The password or challenge secret shared by group members.

Example

```
lunacm:> hagroup removemember -serialnumber 12345679 -label mygroup -password 3nd13$$$uMM3r

Command Result : No Error
```


hagroup removestandby

Remove a standby member from an HA group. Use the **-serialnumber** option to specify which HSM to remove from the group specified by the **-group** option.

Syntax

hagroup removestandby -serialnumber <serial number> **-g** <group>

Parameter	Shortcut	Description
-serialnumber	**-se**	Serial number of HSM to remove - [mandatory if -slotnumber not used] the serial number that identifies the standby member to remove from the named HA group.
-group	**-g**	Label for the group - [mandatory] a label for the HA group being modified.

Example

```
lunacm:> hagroup removestandby -serialnumber 12345679 -group mygroup

Command Result : No Error
```

hagroup retry

Modify the HA Recover retry count.

Syntax

hagroup retry -count <-1 or 0 or positive integer>

Command	Shortcut	Description
-interval	**-i**	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 enable auto-recover for HA. **Default:** 0 **Range:** 1 to 500

Example

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

Command Result : No Error
```


hagroup interval

Modify the HA Recover retry interval.

Syntax

haGroup interval -interval <-1 or 0 or positive integer>

Command	Shortcut	Description
-interval	**-i**	Sets the number of seconds between attempts to recover a failed HA group member. Enter a value of -1 to specify unlimited retries. Enter a value of 0 to disable retries. **Default:** 60 seconds **Range:** 1 to 1200 seconds

Example

```
lunacm:> hagroup interval -i 120

Command Result : No Error
```


hagroup synchronize

Synchronize an HA group.

Syntax

hagroup synchronize -p <password> **-group** <label_or_serial-number_of_group>

Parameter	Shortcut	Description
-group	**-g**	Label or serial number for the HA group being synchronized.
-password	**-p**	Password for the group.

Example

```
lunacm:> hagroup synchronize -group  mygroup -password 1F331$ecur3N0w

Command Result : No Error
```

hsm

Access the hsm-level commands.

> **Note:** The lunacm hsm commands appear only when the current slot selected in lunacm is for a locally-installed HSM, such as a Luna PCI-E. When lunacm is directed at a slot corresponding to a remote Luna SA, the hsm-level commands do not appear, since lunacm has a client-only connection to a remote HSM and therefore cannot log in as SO to a remote HSM. To access HSM commands on the Luna SA appliance, you must use the Luna Shell (lunash).

Syntax

hsm

- **changehsmpolicy**
- **changepw**
- **changesopolicy**
- **clear**
- **clone**
- **contents**
- **factoryreset**
- **init**
- **login**
- **logout**
- **migratepedkey**
- **recoveryinit**
- **recoverylogin**
- **reset**
- **restoresim2**
- **restoreuser**
- **rollbackfw**
- **setlegacydomain**
- **showinfo**
- **showmechanism**
- **showpolicies**
- **smkclone**
- **updatefw**

Parameter	Shortcut	Description
changehsmpolicy	**changehp**	Change the HSM Policy value. See "hsm changehsmpolicy" on page 47.
changepw	**changepw**	Change the HSM SO password. See "hsm changepw" on page 48.
changesopolicy	**changesp**	Change the SO Policy value. See "hsm changesopolicy" on page 49.
clear	**clr**	Delete all of the SO's token objects. See "hsm clear" on page 50.
clone	**clo**	Clone SO objects. See "hsm clone" on page 51.
contents	**con**	Show the contents of the SO partition. See "hsm contents" on page 52.

Parameter	Shortcut	Description
factoryreset	**f**	Factory reset the HSM. See "hsm factoryreset" on page 53.
init	**i**	Initialize the HSM. See "hsm init" on page 54.
login	**logi**	Login to the HSM as SO. See "hsm login" on page 56.
logout	**logo**	Logout from the HSM as SO. See "hsm logout" on page 58.
migratepedkey	**mig**	Migrate a PED Key from a legacy HSM. See "hsm migratepedkey" on page 59.
recoveryinit	**ri**	High Availability Initialize HSM (not related to load balancing). See "hsm recoveryinit" on page 60.
recoverylogin	**rl**	High Availability Login (not related to load balancing) . See "hsm recoverylogin" on page 61.
reset	**rese**	Reset the HSM. See "hsm reset" on page 62.
restoresim2	**rsim2**	Restore SO objects (using SIM2). See "hsm restoresim2" on page 64.
restoreuser	**ru**	Restore a user. See "hsm restoreuser" on page 63.
rollbackfw	**rb**	Rollback the HSM firmware. See "hsm rollbackfw" on page 65.
setlegacydomain	**sld**	Set the legacy domain. See "hsm setlagacydomain" on page 66.
showinfo	**si**	Get HSM information. See "hsm showinfo" on page 67.
showmechanism	**showm**	Show all mechanisms. See "hsm showmechanism" on page 69.
showpolicies	**sp**	Get HSM policy information. See "hsm showpolicies" on page 70.
smkclone	**smk**	Clone the SMK object. See "hsm smkclone" on page 73.
updatecap	**uc**	Update the HSM capabilities. See "hsm updatecap" on page 74.
updatefw	**uf**	Update the HSM firmware. See "hsm updatefw" on page 75.

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 lunacm hsm commands appear only when the current slot selected in lunacm is for a locally-installed HSM, such as a Luna PCI-E. When lunacm is directed at a slot corresponding to a remote Luna SA, the hsm-level commands do not appear, since lunacm has a client-only connection to a remote HSM and therefore cannot log in as SO to a remote HSM. To access HSM commands on the Luna SA appliance, you must use the Luna Shell (lunash).

Syntax

hsm changeHSMPolicy - policy <policy_number> **-value** <new_policy_value> [**-force**]

Parameter	Shortcut	Description
-policy	**-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	**-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.
-force	**-f**	Force the change without further prompting.

Example

```
lunacm:> hsm changeHSMPolicy -policy 12 -value 1

You are about to implement a destructive policy change which will zeroize the HSM.
The User will be deleted and all data will be erased.
Are you sure you wish to continue?

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

Command Result : No Error
```


hsm changepw

Change HSM Security Officer password. Use this command to change the password that authenticates the HSM Security Officer (SO) to the HSM.

Note: The lunacm hsm commands appear only when the current slot selected in lunacm is for a locally-installed HSM, such as a Luna PCI-E. When lunacm is directed at a slot corresponding to a remote Luna SA, the hsm-level commands do not appear, since lunacm has a client-only connection to a remote HSM and therefore cannot log in as SO to a remote HSM. To access HSM commands on the Luna SA appliance, you must use the Luna Shell (lunash).

Syntax

hsm changePw -newpw <new_SO_password> **-oldpw** <old_SO_password>

Parameter	Shortcut	Description
-newpw	**-n**	The new SO password.
-oldpw	**-o**	The old SO password.

Example

```
lunacm:> hsm changePw -newpw NewPa$$w0rd -oldpw 0ldPa$$w0rd

Command Result : No Error
```


hsm changesopolicy

Change the Security Officer policies. Use this command to change the specified SO Policy from the current value to the new, specified value, if the corresponding SO Capability setting permits the change.

Note: The lunacm hsm commands appear only when the current slot selected in lunacm is for a locally-installed HSM, such as a Luna PCI-E. When lunacm is directed at a slot corresponding to a remote Luna SA, the hsm-level commands do not appear, since lunacm has a client-only connection to a remote HSM and therefore cannot log in as SO to a remote HSM. To access HSM commands on the Luna SA appliance, you must use the Luna Shell (lunash).

Syntax

hsm changesopolicy - policy <policy_number> **-value** <new_policy_value>

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

Example

```
lunacm:> hsm changeSOPolicy -policy 25 -value 246

Command Result : No Error
```


hsm clear

Delete contents of the SO space. If the SO is logged in, this command deletes all token objects in the SO partition.

Note: The lunacm hsm commands appear only when the current slot selected in lunacm is for a locally-installed HSM, such as a Luna PCI-E. When lunacm is directed at a slot corresponding to a remote Luna SA, the hsm-level commands do not appear, since lunacm has a client-only connection to a remote HSM and therefore cannot log in as SO to a remote HSM. To access HSM commands on the Luna SA appliance, you must use the Luna Shell (lunash).

Syntax

hsm clear

Example

```
lunacm:> hsm clear

Command Result : No Error
```


hsm clone

Clone HSM SO objects. Use this command to clone SO objects from the HSM into another HSM installed in the same computer.

Note: The lunacm hsm commands appear only when the current slot selected in lunacm is for a locally-installed HSM, such as a Luna PCI-E. When lunacm is directed at a slot corresponding to a remote Luna SA, the hsm-level commands do not appear, since lunacm has a client-only connection to a remote HSM and therefore cannot log in as SO to a remote HSM. To access HSM commands on the Luna SA appliance, you must use the Luna Shell (lunash).

Syntax

hsm clone -objects <handles> [**-force**] **-password** <password> **-slot** <slot number>

Parameter	Shortcut	Description
-objects	**-o**	The object handles to extract
-slot	**-s**	The target slot.
-password	**-p**	The target slot password.
-force	**-f**	Force the action without prompting.

Example

```
lunacm:> hsm clone -objects 0 -slot 2

Command Result : No Error
```


hsm contents

Show the contents of the SO space. If the SO is logged in, this command displays the contents of the SO space (exclusive of user partition contents). If the SO is not logged in, this command displays all SO objects that are available from a public session.

Note: The lunacm hsm commands appear only when the current slot selected in lunacm is for a locally-installed HSM, such as a Luna PCI-E. When lunacm is directed at a slot corresponding to a remote Luna SA, the hsm-level commands do not appear, since lunacm has a client-only connection to a remote HSM and therefore cannot log in as SO to a remote HSM. To access HSM commands on the Luna SA appliance, you must use the Luna Shell (lunash).

Syntax

hsm contents

Example

```
lunacm:> hsm contents
You are not logged in. Looking for objects in a public session.
No objects are currently viewable from a public session.

Command Result : No Error

lunacm:>
lunacm:> hsm login
If you are not activated, please attend to the PED.
Command Result : No Error

lunacm:> hsm contents
The SO is currently logged in. Looking for objects in the SO's partition.
No objects are currently viewable.

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.

Note: This command resets settings and configuration, but does not perform firmware rollback and does not uninstall Capability Updates that have been installed since the HSM came from the factory.

Syntax

hsm factoryReset [**-force**]

Parameter	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

CAUTION:  Are you sure you wish to reset this HSM to factory
default settings? All partitions and data will be erased
and HSM policies will be reverted to factory settings.

Type 'proceed' to return the HSM to factory default, or
'quit' to quit now.

> proceed

Command Result : 0 (success)
```

hsm init

Initialize the HSM. Initializing the HSM erases all existing data on the key card, including any HSM Partition and its data. 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 lunacm hsm commands appear only when the current slot selected in lunacm is for a locally-installed HSM, such as a Luna PCI-E. When lunacm is directed at a slot corresponding to a remote Luna SA, the hsm-level commands do not appear, since lunacm has a client-only connection to a remote HSM and therefore cannot log in as SO to a remote HSM. To access HSM commands on the Luna SA appliance, you must use the Luna Shell (lunash).

Syntax

hsm init -label <hsmlabel> **-password** <hsmsopassword> **[-force]**

Parameter	Shortcut	Description
-label	**-l**	The HSM label.
-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.
-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.
-auth	**-a**	Log in after the initialization.
-force	**-f**	Force the action - no prompts.

Example

"Soft" init (no factory reset)

```
lunacm:> hsm init -label myLuna

You are about to initialize the HSM that is NOT in the
factory reset (zeroized) state.
All objects will be destroyed.
The User will be destroyed.
You are required to provide the current SO PED key.
The domain will NOT be destroyed.

Are you sure you wish to continue?
Type 'proceed' to continue, or 'quit' to quit now -> proceed

Command Result : No Error
lunacm:>
```

"Hard" init (with factory reset first)

```
lunacm:> hsm factoryReset

You are about to factory reset the HSM.
All contents of the HSM will be destroyed.
```



```
The user will be destroyed.
The SO will be destroyed.
The domain will be destroyed.

Are you sure you wish to continue?
Type 'proceed' to continue, or 'quit' to quit now -> proceed

Resetting HSM

Command Result : No Error
lunacm:>

lunacm:> hsm init -label myLuna

You are about to initialize the HSM that is in the
factory reset (zeroized) state.
All objects will be destroyed.
The User will be destroyed.
You are required to provide the current SO PED key.
The domain will NOT be destroyed.

Are you sure you wish to continue?
Type 'proceed' to continue, or 'quit' to quit now -> proceed

Command Result : No Error
```

hsm login

Login to the HSM as the security officer (SO).

> **Note:** The lunacm hsm commands appear only when the current slot selected in lunacm is for a locally-installed HSM, such as a Luna PCI-E. When lunacm is directed at a slot corresponding to a remote Luna SA, the hsm-level commands do not appear, since lunacm has a client-only connection to a remote HSM and therefore cannot log in as SO to a remote HSM. To access HSM commands on the Luna SA appliance, you must use the Luna Shell (lunash).

Syntax

hsm login [**-password** <hsm_SO_password>] [**-ped** <ped Id>]

Parameter	Shortcut	Description
-password	**-pa**	Applies to Password-authenticated HSMs; ignored for PED-authenticated HSMs. Specifies the HSM Admin password. The password to be used as login credential by the Security Officer (SO). As shown, you can supply the password at the command line (useful for scripting). Normally, however, you should leave out the password when issuing the command. If the password is not provided, you are prompted for it, and your response is obscured by asterisk (****) symbols. This a more secure method of providing the password.
-ped	**-pe**	Applies to PED-authenticated HSMs, only. This option is a temporary way to override PED ID settings or default. The PED Id parameter is optional. (0=local,1...65535=remote) If '0' is specified, the locally attached PED is used. If a value between 1 and 65535 is specified, the remote PED corresponding to that PED Id is used. If nothing is specified, then the value stored in the library for this slot is used. Unless the value stored in the library has been changed by using the 'ped set' command, or the 'PEDId' parameter in the 'Luna' section of cryptoki.ini, the value in the library is '0'. NOTE: The '-ped' option asserts for the duration of this login command, only. After the login completes, any PED ID that was set by the '-ped' option then reverts to whatever value was in effect before "hsm login -ped <PED Id>".

Example

HSM login using the -password option (not recommended)

lunacm:> hsm login -password SOpa55word!

Command Result : No Error

HSM login without the -password option

lunacm:> hsm login

Option -password was not supplied. It is required.

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

Command Result : No Error

hsm logout

Logout the security officer (SO) from the HSM.

Note: The lunacm hsm commands appear only when the current slot selected in lunacm is for a locally-installed HSM, such as a Luna PCI-E. When lunacm is directed at a slot corresponding to a remote Luna SA, the hsm-level commands do not appear, since lunacm has a client-only connection to a remote HSM and therefore cannot log in as SO to a remote HSM. To access HSM commands on the Luna SA appliance, you must use the Luna Shell (lunash).

Syntax

hsm logout

Example

```
lunacm:> hsm logout

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 (looks like a colorful toy 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 lunacm hsm commands appear only when the current slot selected in lunacm is for a locally-installed HSM, such as a Luna PCI-E. When lunacm is directed at a slot corresponding to a remote Luna SA, the hsm-level commands do not appear, since lunacm has a client-only connection to a remote HSM and therefore cannot log in as SO to a remote HSM. To access HSM commands on the Luna SA appliance, you must use the Luna Shell (lunash).

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 recoveryinit

Rerforms a recovery (formerly High Availability) initialization on the current active session.

Syntax

hsm recoveryinit [**-plabel** <rsapublickeylabel> **-rlabel** <rsaprivatekeylabel> **-keyhandle** <rsaprivatekeyhandle>] [**-force**] **-password**

Parameter	Shortcut	Description
-plabel	**-pl**	RSA Public key label.
-rlabel	**-rl**	RSA Private key label.
-keyhandle	**-kh**	RSA Private Key handle (optional).
-force	**-f**	Force the action (no prompts).

Note: Labels are required only to create custom-named RecoveryInit RSA key pair, which is the default action if [keyhandle] is not supplied.

Example

```
lunacm:> hsm recoveryinit

Generating RSA Key pair for Recovery Init...

No label were supplied for the RSA key pair. Default labels
will be used.
Are you sure you wish to continue?

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

Command Result : Success
```


hsm recoverylogin

Perform a High Availability login on the current active session.

Note: The lunacm hsm commands appear only when the current slot selected in lunacm is for a locally-installed HSM, such as a Luna PCI-E. When lunacm is directed at a slot corresponding to a remote Luna SA, the hsm-level commands do not appear, since lunacm has a client-only connection to a remote HSM and therefore cannot log in as SO to a remote HSM. To access HSM commands on the Luna SA appliance, you must use the Luna Shell (lunash).

Syntax

hsm recoverylogin

Example

```
lunacm:> hsm recoverylogin

Command Result : Success
```


hsm reset

Reset the Luna HSM. Use this command to reset the Luna HSM if it has 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 SafeNet, contact that company for a resolution of the problem. They know how their application is programmed to accomplish tasks that use the Luna HSM, and they can determine possible workarounds or fixes. If the third-party supplier determines that there is an actual implementation fault with the Luna, they will contact SafeNet after gathering the relevant information.

Note: The lunacm hsm commands appear only when the current slot selected in lunacm is for a locally-installed HSM, such as a Luna PCI-E. When lunacm is directed at a slot corresponding to a remote Luna SA, the hsm-level commands do not appear, since lunacm has a client-only connection to a remote HSM and therefore cannot log in as SO to a remote HSM. To access HSM commands on the Luna SA appliance, you must use the Luna Shell (lunash).

Syntax

hsm reset

Example

```
lunacm:> hsm reset

Command Result : No Error
```


hsm restoreuser

Insert a backed-up user partition into the HSM.

Note: The lunacm hsm commands appear only when the current slot selected in lunacm is for a locally-installed HSM, such as a Luna PCI-E. When lunacm is directed at a slot corresponding to a remote Luna SA, the hsm-level commands do not appear, since lunacm has a client-only connection to a remote HSM and therefore cannot log in as SO to a remote HSM. To access HSM commands on the Luna SA appliance, you must use the Luna Shell (lunash).

Syntax

hsm restoreuser -filename <input filename>

Parameter	Shortcut	Description
-filename	-fi	The name of the file (SIM2-portable blob) to be imported.
-force	-fo	Force the action without prompting.

Example

```
lunacm:> hsm restoreuser -filename mypartitionblob

Command Result : No Error
```


hsm restoresim2

Insert backed-up SO objects into the HSM. When a SIM2-portable blob is created, the options to protect it are:

- none
- an authentication text string.

Therefore, this restore/import operation offers the option to supply an unlocking/authentication text string in case one was used to secure the blob.

Note: The lunacm hsm commands appear only when the current slot selected in lunacm is for a locally-installed HSM, such as a Luna PCI-E. When lunacm is directed at a slot corresponding to a remote Luna SA, the hsm-level commands do not appear, since lunacm has a client-only connection to a remote HSM and therefore cannot log in as SO to a remote HSM. To access HSM commands on the Luna SA appliance, you must use the Luna Shell (lunash).

Syntax

hsm restoresim2 [**-auth** <auth_passwd>] **-filename** <input_filename> **-partition** <partition>

Parameter	Shortcut	Description
-auth	-a	The authorization password. If "-auth" is specified, the CKA_SIM_PORTABLE_PASSWORD SIM Form will be used. Otherwise the CKA_SIM_PORTABLE_NO_AUTHORIZATION SIM Form will be used. The same SIM Form that was used for the backup command must be used for the restore command.
-filename	-fi	The input file name. This is the name of the file (SIM2-portable blob) to be imported.
-partition	-par	Partition into which objects are restored.

Example

```
lunacm:> hsm restoreSIM2 -auth someauthenticationsecret -filename mySIM2portableblob

Command Result : No Error
```


hsm rollbackfw

Rollback 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 (**hsm updatefw**) without permanently committing to the new version.

Note: You must re-initialize the HSM after rolling back the firmware rollback. since re-initialization is a destructive action, ensure that you back up any important materials before running this command.

Note: The lunacm hsm commands appear only when the current slot selected in lunacm is for a locally-installed HSM, such as a Luna PCI-E. When lunacm is directed at a slot corresponding to a remote Luna SA, the hsm-level commands do not appear, since lunacm has a client-only connection to a remote HSM and therefore cannot log in as SO to a remote HSM. To access HSM commands on the Luna SA appliance, you must use the Luna Shell (lunash).

Syntax

hsm rollbackfw

Example

```
lunacm:> hsm login

Please attend to the PED.

Command Result : No Error

lunacm:> hsm rollbackFW

You are about to rollback the firmware.
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 setlagacydomain

Set the legacy cloning domain on the HSM. You must set the legacy cloning domain to migrate the contents of a legacy Luna HSM to a release 5.x Luna HSM.

- The legacy cloning domain for password-authenticated HSM partitions is the text string that was used as a cloning domain on the legacy token HSM or Luna PCI HSM or Luna SA HSM whose contents are to be migrated to the Luna 5.x HSM SO space (a separate command, **partition setlegacydomain** is used for partitions).
- The legacy cloning domain for PED-authenticated HSMs is the cloning domain secret on the red PED key for the legacy PED authenticated HSM whose contents are to be migrated to the Luna 5.x HSM SO space.

You cannot migrate objects from a password-authenticated token/HSM to a PED authenticated Luna 5.x HSM, and you cannot migrate objects from a PED authenticated token/HSM to a password-authenticated Luna 5.x HSM.

Your target Luna 5.x HSM has, and retains, whatever modern HSM cloning domain was imprinted (on a red PED Key) when the HSM was initialized. The **hsm setlegacydomain** command takes the domain value from your legacy HSM's red PED Key and associates that with the modern-format domain of the new HSM, to allow the HSM's SO space to be the cloning (restore...) recipient of objects from the legacy (token) HSM.

Once the first legacy domain has been associated with your new Luna HSM, that legacy domain is attached until the HSM is reinitialized.

The ability to set the legacy cloning domain does not allow you to defeat the security provision that prevents cloning of objects across different domains.

See "Legacy Domains and Migration" for a description and summary of the possible combinations of source (legacy) tokens/HSMs and target (modern) HSMs and the disposition of token objects from one to the other.

Note: The lunacm hsm commands appear only when the current slot selected in lunacm is for a locally-installed HSM, such as a Luna PCI-E. When lunacm is directed at a slot corresponding to a remote Luna SA, the hsm-level commands do not appear, since lunacm has a client-only connection to a remote HSM and therefore cannot log in as SO to a remote HSM. To access HSM commands on the Luna SA appliance, you must use the Luna Shell (lunash).

Syntax

hsm setLegacyDomain [**-domain** <domain>]

Parameter	Shortcut	Description
-password	**-pas**	The HSM password.
-domain	**-d**	The name of the legacy cloning domain.

Example

```
lunacm:> hsm setLegacyDomain
```

The PED prompts for the legacy red domain PED Key (notice mention of "raw data" in the PED message).

```
Command result: Success!
```

hsm showinfo

Display HSM-level information.

Note: The lunacm hsm commands appear only when the current slot selected in lunacm is for a locally-installed HSM, such as a Luna PCI-E. When lunacm is directed at a slot corresponding to a remote Luna SA, the hsm-level commands do not appear, since lunacm has a client-only connection to a remote HSM and therefore cannot log in as SO to a remote HSM. To access HSM commands on the Luna SA appliance, you must use the Luna Shell (lunash).

Syntax

hsm showinfo

Example

```
lunacm:> hsm showinfo

HSM Label -> myLuna
HSM Manufacturer -> Safenet, Inc.
HSM Model -> K6 Base
HSM Serial Number -> 150022
HSM Status -> OK

Token Flags ->
     CKF_RNG
     CKF_LOGIN_REQUIRED
     CKF_USER_PIN_INITIALIZED
     CKF_RESTORE_KEY_NOT_NEEDED
     CKF_TOKEN_INITIALIZED

Firmware Version -> 6.2.1
Rollback Firmware Version -> Not Available
Slot Id -> 1
Tunnel Slot Id -> 2
Session State -> CKS_RW_PUBLIC_SESSION

SO Status-> Not Logged In
SO Failed Logins-> 0
SO Flags ->

CONTAINER_KCV_CREATED

HSM Storage:
     Total Storage Space: 2097152
     Used Storage Space: 2097152
     Free Storage Space: 0
     Allowed Partitions: 1
     Number of Partitions: 1

SO Storage:
     Total Storage Space: 262144
     Used Storage Space: 0
     Free Storage Space: 262144
     Object Count: 0
```



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

License Count -> 7
   1. 621000026-000 621-000026-000 K6 BASE CONFIGURATION FILE,HSM UNMASKING
   2. 620127-000 ECC
   3. 620114-001 Cloning
   4. 620109-000 FIPS3
   5. 621010358-001 621-010358-001 External MTK - STM disabled
   6. 621010089-001 621-010089-001 Remote PED
   7. 621000021-001 SCU K5/K6 Performance 15

Command Result : No Error
```


hsm showmechanism

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

Note: The lunacm hsm commands appear only when the current slot selected in lunacm is for a locally-installed HSM, such as a Luna PCI-E. When lunacm is directed at a slot corresponding to a remote Luna SA, the hsm-level commands do not appear, since lunacm has a client-only connection to a remote HSM and therefore cannot log in as SO to a remote HSM. To access HSM commands on the Luna SA appliance, you must use the Luna Shell (lunash).

Syntax

hsm showmechanism

Example

```
lunacm:> hsm showinfo

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

Command Result : No Error
```


hsm showpolicies

Displays the HSM-level capability and policy settings for the HSM and SO.

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 for your Luna HSM, contact SafeNet Support.

Note: The lunacm hsm commands appear only when the current slot selected in lunacm is for a locally-installed HSM, such as a Luna PCI-E. When lunacm is directed at a slot corresponding to a remote Luna SA, the hsm-level commands do not appear, since lunacm has a client-only connection to a remote HSM and therefore cannot log in as SO to a remote HSM. To access HSM commands on the Luna SA appliance, you must use the Luna Shell (lunash).

Syntax

hsm showpolicies

Example

```
lunacm:> hsm showplicies

        HSM Capabilities
0: Enable PIN-based authentication : 1
1: Enable PED-based authentication : 0
2: Performance level : 9
3: Enable M of N : 0
4: Enable domestic mechanisms & key sizes : 1
6: Enable masking : 0
7: Enable cloning : 0
8: Enable special cloning certificate : 0
9: Enable full (non-backup) functionality : 1
11: Enable ECC mechanisms : 0
12: Enable non-FIPS algorithms : 1
13: Enable MofN auto-activation : 0
15: Enable SO reset of partition PIN : 1
16: Enable network replication : 0
17: Enable Korean Algorithms : 0
18: FIPS evaluated : 0
19: Manufacturing Token : 0
20: Enable Remote Authentication : 1
21: Enable forcing user PIN change : 0
22: Enable offboard storage : 1
23: Enable partition groups : 0

        HSM Policies
0: PIN-based authentication : 1
1: PED-based authentication : 0
3: Require M of N : 0
6: Allow masking : 0
7: Allow cloning : 0
12: Allow non-FIPS algorithms : 1
13: Allow MofN auto-activation : 0
```



```
15: SO can reset partition PIN : 1
16: Allow network replication : 0
20: Allow Remote Authentication : 1
21: Force user PIN change after set/reset : 0
22: Allow offboard storage : 1
23: Allow partition groups : 0

        SO Capabilities
0: Enable private key cloning : 0
1: Enable private key wrapping : 0
2: Enable private key unwrapping : 1
3: Enable private key masking : 0
4: Enable secret key cloning : 0
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
14: Enable PED use without challenge : 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
19: Max non-volatile storage space : 3
20: Max failed user logins allowed : 3
21: Enable high availability recovery : 1
22: Enable activation : 0
23: Enable auto-activation : 0
25: Minimum pin length (inverted: 255 - min) : 248
26: Maximum pin length : 255
28: Enable Key Management Functions : 1
29: Enable RSA signing without confirmation : 1
30: Enable Remote Authentication : 1

        SO Policies
0: Enable private key cloning : 0
1: Enable private key wrapping : 0
2: Enable private key unwrapping : 1
3: Enable private key masking : 0
4: Enable secret key cloning : 0
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
14: Enable PED use without challenge : 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
19: Max non-volatile storage space : 3
20: Max failed user logins allowed : 3
21: Enable high availability recovery : 1
22: Enable activation : 0
23: Enable auto-activation : 0
25: Minimum pin length (inverted: 255 - min) : 248
26: Maximum pin length : 255
28: Enable Key Management Functions : 1
29: Enable RSA signing without confirmation : 1
30: Enable Remote Authentication : 1
```



```
Command Result : No Error
```

hsm smkclone

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

CAUTION: This command overwrites the SMK of the target slot.

Note: The lunacm hsm commands appear only when the current slot selected in lunacm is for a locally-installed HSM, such as a Luna PCI-E. When lunacm is directed at a slot corresponding to a remote Luna SA, the hsm-level commands do not appear, since lunacm has a client-only connection to a remote HSM and therefore cannot log in as SO to a remote HSM. To access HSM commands on the Luna SA appliance, you must use the Luna Shell (lunash).

Syntax

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

Parameter	Shortcut	Description
-slot	**-s**	The target slot.
-password	**-p**	The password for the target slot.
-force	**-f**	Force the action without prompting.

Example

```
lunacm:> hsm smkclone -slot 2 -password $ome-Pa55word

Command Result : No Error
```


hsm updatecap

Perform an update of the HSM capabilities on the Luna HSM. When updatable features and capabilities are made available from SafeNet, from time to time, this command is the means to implement such features on your existing Luna HSM. That is, if you purchase an advanced capability upgrade, this is the command to update the HSM capability from the standard factory version.

This command, and all the lunacm hsm commands, appear only when the current slot selected in lunacm is for a local HSM, like an installed Luna PCI-E.

HSM commands do not appear in the lunacm command menu when lunacm is directed at a slot corresponding to a remote Luna SA - lunacm has a client-only connection to a remote HSM and therefore cannot log in as SO to a remote HSM.

For Luna SA, the HSM commands are available via the Luna appliance's Luna Shell (lunash:>), which can be accessed via ssh if you have the required authentication.

Syntax

hsm updatecap -cuf <capability_update_filename> **-authcode** <authorization_code_filename> [**-force**]

Parameter	Shortcut	Description
-cuf	**-u**	Specifies the capability update file that you want to apply.
-authcode	**-a**	Specifies the file containing the authorization code for the capability update.
-force	**-f**	Force the action without prompting.

Example

```
lunacm:> hsm updateCap -cuf <capupdateK3_431.FUF> -authcode <authcodeK3_431.TXT>
Command Result : No Error
```

Note: The filenames that are shown above are just examples, for purposes of illustration. Yours will differ.

hsm updatefw

Update the firmware on the Luna HSM.

Note: The lunacm hsm commands appear only when the current slot selected in lunacm is for a locally-installed HSM, such as a Luna PCI-E. When lunacm is directed at a slot corresponding to a remote Luna SA, the hsm-level commands do not appear, since lunacm has a client-only connection to a remote HSM and therefore cannot log in as SO to a remote HSM. To access HSM commands on the Luna SA appliance, you must use the Luna Shell (lunash).

Note: For PED-authenticated HSMs, you must disable SRK before you can update the firmware. Use the **srk show** command to determine whether SRK is enabled on your HSM. If it is, the first line of the output of the **srk show** command reads **Secure Transport Functionality is supported and enabled**. If this is the case, run the **srk disable**command to disable SRK on the HSM. You must have the appropriate purple PED Key to disable SRK. If you attempt to update the firmware update while SRK is enabled, the system responds with an error: 0x80000030 (CKR_OPERATION_NOT_ALLOWED).

Syntax

hsm updateFW -fuf <fwupdate_filename> **-authcode** <authorization_code_filename>

Parameter	Shortcut	Description
-fuf	**-u**	Specifies the firmware update file.
-authcode	**-a**	Specifies the file containing the authorization code for the firmware update.
-force	**-f**	Force the action without prompting.

Example

```
lunacm:> hsm updateFW -fuf fwupdateK6_6.1.3_RC7_w_BB_1.3.FUF -authcode authcodeK6_6.1.3_RC7.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
```


partition

Access the hsm-level commands.

> **Note:** The lunacm hsm commands appear only when the current slot selected in lunacm is for a locally-installed HSM, such as a Luna PCI-E. When lunacm is directed at a slot corresponding to a remote Luna SA, the hsm-level commands do not appear, since lunacm has a client-only connection to a remote HSM and therefore cannot log in as SO to a remote HSM. To access HSM commands on the Luna SA appliance, you must use the Luna Shell (lunash).

Syntax

partition

- **activate**
- **archive**
- **changepolicy**
- **changepw**
- **clear**
- **clone**
- **contents**
- **create**
- **createchallenge**
- **createuser**
- **deactivate**
- **login**
- **logout**
- **recoveryinit**
- **recoverylogin**
- **resetpw**
- **restoresim2**
- **restoresim3**
- **setlegacydomain**
- **showinfo**
- **showpolicies**
- **smkclone**

Parameter	Shortcut	Description
activate	**ac**	Change the HSM Policy value. See "partition activate" on page 78.
archive	**ar**	Backup/restore objects to/from backup devices. See "partition archive" on page 80.
changepolicy	**changepo**	Change the SO Policy value. See "partition changepolicy" on page 88
changepw	**changepw**	Change the partition password. See "partition changepw" on page 89.
clear	**clr**	Delete all of the user's token objects. See "partition clear" on page 91.
clone	**clo**	Clone user objects. See "partition clone" on page 92.

Parameter	Shortcut	Description
contents	**con**	Show the contents of the user partition. See "partition contents" on page 93.
create	**f**	Create the user partition. See "partition create" on page 94.
createchallenge	**i**	Create the user challenge. See "partition createchallenge" on page 95.
createuser	**cru**	Create a Crypto-User challenge. See "partition createuser" on page 96.
deactivate	**dea**	De-cache the user's PED Key data. See "partition deactivate" on page 97.
login	**logi**	Login to the HSM as user. See "partition login" on page 98.
logout	**logo**	Logout from the HSM as user. See "partition logout" on page 99.
recoveryinit	**ri**	Setup/configure User for "Recovery Login" (formerly "HA Init", not related to load balancing). See "partition recoveryinit" on page 100.
recoverylogin	**rl**	Login as the User using "Recovery Login" (formerly "HA Login", not related to load balancing). See "partition recoverylogin" on page 101.
resetpw	**resetpw**	Reset the partition password. See "partition resetpw" on page 102.
restoresim2	**rsim2**	Restore user objects (using SIM2). See "partition restoresim2" on page 103.
restoresim3	**rsim3**	Restore user objects (using SIM3). See "partition restoresim3" on page 104.
setlegacydomain	**sld**	Set the legacy domain. "partition setlegacydomain" on page 105.
showinfo	**si**	Display partition information. See "partition showinfo" on page 106.
showmechanism	**showm**	Show all available mechanisms. See "partition showpolicies" on page 107.
showpolicies	**sp**	Get partition policy information. See "partition showpolicies" on page 107.
smkclone	**smk**	Clone the SMK object. See "partition smkclone" on page 109.

partition activate

Cache Partition PED Key data [Luna PCI-E with PED (Trusted Path) Authentication only]. Use this command to caches a Partition's PED Key data. Clients can then connect, authenticate with their Partition password (challenge secret), and perform operations with Partition objects, without need for hands-on PED operations each time. Activation/caching endures until explicitly terminated with "partition deactivate" or host computer power off. If a Partition has not been activated, then each access attempt by a Client causes a login call which initiates a Luna PED operation (requiring the appropriate black PED Key). Unattended operation is possible while the Partition is activated.

Note: If you wish to activate a Partition, then Partition policy number 22 "Allow activation" must be set to "On" for the named partition. Use "partition showPolicies" to view the current settings and use "partition changePolicy" to change the setting. The policy shows as "Off" or "On", but to change the policy you must give a numeric value of "0" or "1".

Note: If you wish to activate a Partition, then Partition policy number 23 "Allow auto-activation" can be set to "On" for the partition. Use "partition showPolicies" to view the current settings and use "partition changePolicy" to change the setting.
The policy shows as "Off" or "On", but to change the policy you must give a numeric value of "0" or "1".
Autoactivation caches the activation authentication data in battery-backed memory so that activation can persist/recover following a shutdown/restart or a power outage up to 2 hours duration. If Partition Policy 23 is set, then partition activation includes autoactivation. If Partition Policy 23 is not set, then partition activation persists only while the host computer is powered on, and requires your intervention to reinstate activation following a shutdown or power outage.

Syntax

partition activate -password <partition_user_password>

Parameter	Shortcut	Description
-password	**-p**	The password to be used as login credential by the Partition User. As shown, you can supply the password at the command line (useful for scripting). Normally, however, you should leave out the password when issuing the command. If the password is not provided, you are prompted for it, and your response is obscured by asterisk (****) symbols. This a more secure method of providing the password. NOT USED for PED-authenticated HSMs, which need the data from the black PED Key instead, however the challenge-secret/password is still needed by the client application.
-cu	**-c**	Selects to perform the login as Crypto-User, which has a limited subset of "User". Use this option only if your security scheme makes use of the Crypto-Officer/Crypto-User distinction.
-ped	**-ped**	This parameter is optional. If it is not specified, then the value of the

Parameter	Shortcut	Description
		"PEDId" parameter in the "Luna" section of Chrystoki.conf (cryptoki.ini) is used. Otherwise the default is "0" or local PED.

Example

Password-authentication

```
lunacm:> partition activate -password Userpa55word!

Command Result : No Error
```

PED-authentication

```
lunacm:> partition activate

Option -password was not supplied. It is required.
Enter the password: ***************
User is not activated, please attend to the PED.

Command Result : No Error
```


partition archive

Access the partition archive commands.

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

- an HSM in another slot in the current system.
- a backup HSM connected to a remote workstation.
- a USB-attached HSM connected directly to a Luna PCI-E HSM.
- a SFF backup token (SafeNet iKey e7300) USB device connected to a Luna PED. The Luna PED can be locally or remotely connected (via PedServer) to the HSM you want to backup.

Device configuraton

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.

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**).

To specify a SFF backup (eToken 7300) inserted into a Luna PED connected to the local HSM or connected by USB to a host computer running PedServer, use the **-s** option and include the keyword **etoken**.

Password-authenticated Luna Remote Backup HSM

When using a password-authenticated Luna Remote 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 will be 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

Parameter	Shortcut	Description
backup	**b**	Backup objects from the current slot to a backup partition in a backup device in a specified slot. See "partition archive backup" on page 82.
contents	**c**	List the contents of a backup partition in a backup device in a specified slot. See "partition archive contents" on page 84.
delete	**d**	Delete the specified backup partition in a backup device in a specified slot. See "partition archive delete" on page 85.
list	**l**	List the backup partitions on a backup device in a specified slot. See "partition archive list" on page 86.
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 87.

partition archive backup

Backup partition objects. Use this command to backup objects from the current user partition to a partition on a backup device.

Syntax

partition archive backup -slot <slot> **-pas** <password> **-par** <backup partition>

Parameter	Shortcut	Description
-append	**-a**	Append the objects to the existing partition.
-commandtimeout	**-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	**-de**	Turn on additional error information. (optional)
-domain	**-do**	Domain for the specified partition.
-force	**-f**	Force action with no prompting.
-hostname	**-ho**	Host name of remote workstation running remote backup server. (required when **-s remote** is used)
-partition	**-par**	Partition on the backup device. (maximum length of 64 characters)
-password	**-pas**	Password for the specified partition.
-port	**-po**	Port number for remote backup server on remote workstation. (required when **-s remote** is used)
-replace	**-re**	Allow objects with same OUID on backup device to be deleted and replaced.
-slot	**-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**) • **etoken** to specify a SFF backup (eToken 7300) inserted into a Luna PED connected to the local HSM or connected by USB to a host computer running PedServer.
-sopassword	**-sop**	SO password for the backup device.

Example

```
lunacm:> partition aarchive -objects 0 -filename somepartfile
```



```
You have not specified a password.  The default SIM Form
CKA_SIM_PORTABLE_NO_AUTHORIZATION will be used.
Are you sure you wish to continue?

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

All objects will be backed up.
The backed up objects have been written to the file somepartfile.

Command Result : No Error
```


partition archive contents

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

Syntax

partition archive c -s <slot> **-par** <partition name> **-pas** <password>

Parameter	Shortcut	Description
-commandtimeout	**-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	**-ho**	Host name of remote workstation running remote backup server (required when **-s remote** is used)
-partition	**-par**	Partition on the backup device. (maximum length of 64 characters) .
-password	**-pas**	User password for the specified partition.
-port	**-po**	Port number for remote backup server on remote workstation (required when **-s remote** is used)
-slot	**-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**) • **etoken** to specify a SFF backup (eToken 7300) inserted into a Luna PED connected to the local HSM or connected by USB to a host computer running PedServer.

Example

```
lunacm:> partition archive contents -slot 5

Command Result : No Error
```


partition archive delete

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

Syntax

partition archive d -s <slot> **-par** <partition name> **-pas** <password>

Parameter	Shortcut	Description
-commandtimeout	**-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	**-ho**	Host name of remote workstation running remote backup server. (required when **-s remote** is used)
-partition	**-par**	Partition to delete on the backup device. (maximum length of 64 characters) .
-password	**-pas**	User password for the specified partition.
-port	**-po**	Port number for remote backup server on remote workstation. (required when **-s remote** is used)
-slot	**-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**) • **etoken** to specify a SFF backup (eToken 7300) inserted into a Luna PED connected to the local HSM or connected by USB to a host computer running PedServer.

Example

```
lunacm:> partition archive delete -slot 5 -partition mypar1 -password Pa$$w0rd

Command Result : No Error
```


partition archive list

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

Syntax

partition archive list -slot <slot>

Parameter	Shortcut	Description
-commandtimeout	**-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	**-ho**	Host name of remote workstation running remote backup server. (required when **-s remote** is used)
-port	**-po**	Port number for remote backup server on remote workstation. (required when **-s remote** is used)
-slot	**-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**) • **etoken** to specify a SFF backup (eToken 7300) inserted into a Luna PED connected to the local HSM or connected by USB to a host computer running PedServer.

Example

```
lunacm:> partition archive -slot 5

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.

Syntax

partition archive restore -slot <slot> **-pas** <password> **-par** <backup partition>

Parameter	Shortcut	Description
-commandtimeout	**-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	**-ho**	Host name of remote workstation running remote backup server. (required when **-s remote** is used)
-partition	**-par**	Partition on the backup device. (maximum length of 64 characters) .
-password	**-pas**	User password for the specified partition.
-port	**-po**	Port number for remote backup server on remote workstation. (required when **-s remote** is used)
-slot	**-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**) • **etoken** to specify a SFF backup (eToken 7300) inserted into a Luna PED connected to the local HSM or connected by USB to a host computer running PedServer.

Example

```
lunacm:> partition archive restore -slot 2 -password <somepassword> -partition mybackupPar

Command Result : No Error
```


partition changepolicy

Change a user policy on the partition.

Syntax

partition changepolicy -policy <policy_id> **-value** <policy_value>

Parameter	Shortcut	Description
-policy	**-p**	Specifies the ID of the policy you want to change.
-value	**-v**	Specifies the new value for the specified policy.

partition changepw

Change Partition User password. Use this command to changes the password that authenticates the User and/or the client to the Partition. You, as User, need to know the current password in order to change it.

Contrast this command with the **partition resetpw** command, used by the SO, where the SO does not need to know the current partition User password in order to reset it.

Password authentication

For Password authenticated Luna HSM, the partition password needed by the administrator (Partition Owner/User) is also the challenge secret needed by the client.

PED authentication

For PED authenticated Luna HSM, the data on the black PED Key is the administrative authentication (used by the Partition Owner/User to log in or to activate the partition), and the challenge secret is a separate text secret used by the client before performing cryptographic operations.

If you run the partition changPw command without additional arguments, the HSM offers to change only the black PED Key secret.

To change the challenge secret, you must run the command with the -newpw and -oldpw options - OR use the -p option instead, which tells the HSM to prompt for old and new challenge secrets.

Syntax

partition changepw [**- newpw** <new_user_password> **-oldpw** <old_user_password>] [**-prompt**]

Parameter	Shortcut	Description
-newpw	**-n**	The new password for the partition User.
-oldpw	**-o**	The old partition User password that is being replaced.
-prompt	**-p**	The system prompts for old and new passwords (for password-authenticated HSM) or challenge secrets (for PED-authenticated HSM) and obscures your typing with asterisks, so an unauthorized person cannot see the passwords onscreen, and the scroll-back log of your terminal would not show what you had typed.

Example

Password-authenticated HSM partition, with the passwords typed visibly at the command line.

```
lunacm:> partition changePw -newpw <new_user_password> -oldpw <old_user_password>

Command Result : No Error
```

PED-authenticated HSM partition with the challenge typed visibly at the command line.

```
lunacm:> partition changePw -newpw <new_user_password> -oldpw <old_user_password>

User is not activated, please attend to the PED.

Command Result : No Error
```


Password-authenticated HSM partition, with the passwords prompted by the HSM and obscured by asterisks.

```
lunacm:> partition changepw -p

Option -oldpw was not supplied. It is required.
Enter the old password: ***********
Option -newpw was not supplied. It is required.
Enter the new password: ***********
Re-enter the new password: ***********

Command Result : No Error
```

PED-authenticated HSM partition with the passwords prompted by the HSM and obscured by asterisks.

```
lunacm:> partition changePw -p

Option -oldpw was not supplied. It is required.
Enter the old challenge: ***********
Option -newpw was not supplied. It is required.
Enter the new challenge: ***********
Re-enter the new password: ***********
User is not activated, please attend to the PED.

Command Result : No Error
```

Changing the black key secret on a PED-authenticated HSM partition without changing the challenge secret.

```
lunacm:> partition changePw

User is not activated, please attend to the PED.

Command Result : No Error
```


partition clear

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

> ⚠ **CAUTION:** The objects are deleted as soon as the command is executed, without requesting confirmation.

Syntax

partition clear

Example

```
lunacm:> partition clear

Command Result : No Error
```

partition clone

Clone User partition objects from the HSM into another HSM installed in the same computer.

Syntax

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

Parameter	Shortcut	Description
-force	**-fo**	Force the action without prompting.
-objects	**-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	**-p**	The target slot password. This option does not apply to PED-authenticated HSMs/tokens.
-slot	**-s**	The target slot.

Example

```
lunacm:> partition clone -objects 0 -slot 2

Verifying that the specified objects can be cloned.

All objects will be cloned.

Logging in to target slot 2.

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

The cloned objects have been written to the token in slot 2.

Command Result : No Error
```


partition contents

Display a list of the objects on the partition. If the User is logged in, this command will display the contents of the User's partition. If the User is not logged in, this command will display all of the objects that are available from a public session. The partition name, serial number and total object count is displayed. For each object that is found, the label and object type are displayed.

Syntax

partition contents

Example

```
lunacm:> partition contents

The User is currently logged in.  Looking for objects in the
User's partition.

Number objects:  2
Handle: 7       Label:  Known
Handle: 8       Label:  Generated DES3 Key

Command Result : No Error
```


partition create

Create a user partition.

Syntax

partition create

Example

```
# par create

The existing Partition will be destroyed.
Are you sure you wish ot continue?
```

partition createchallenge

Create the partition User challenge. The partition createChallenge command creates a partition User challenge for the current partition. If you also create a challenge for Crypto-User, then "User" becomes Crypto-Officer and uses the challenge that you create here, while Crypto-User gets a separate challenge.

You must run this command before you can run the **partition createuser** command.

It is recommended that you record the 16-character text string displayed by the PED using a text editor to avoid transcription errors.

Syntax

partition createchallenge

Example

```
lunacm:> partition createChallenge

Please attend to the PED.

Command Result : No Error
```


partition createuser

Create the Crypto-User challenge for the current partition. The command **partition createchallenge** must have already been run for this partition. If **partition createuser** is run (creating the Crypto-User and giving that user its own challenge), then the challenge created for the partition User becomes the challenge for Crypto-Officer.

Syntax

partition createuser

Example

```
lunacm:> partition createUser

Please attend to the PED.

Command Result : No Error
```

partition deactivate

De-cache partition PED-key data. This command applies to Luna PCI-E with PED (trusted path) authentication only.

Syntax

partition deactivate

Example

```
lunacm:> partition deactivate

Command Result : No Error
```

partition login

Login to the partition.

Syntax

partition login [**-password** <password-or-challenge>] [-cu] [**-ped** <ped Id>]

Parameter	Shortcut	Description
-password	**-pa**	Applies to Password-authenticated HSMs; ignored for PED-authenticated HSMs. Specifies the Partition Owner or Crypto Officer password, to be used as login credential. As shown, you can supply the password at the command line (useful for scripting). Normally, however, you should leave out the password when issuing the command. If the password is not provided, you are prompted for it, and your response is obscured by asterisk (****) symbols. This a more secure method of providing the password.
-cu	**-c**	Perform the operation as Crypto User.
-ped	**-pe**	Applies to PED-authenticated HSMs, only. This option is a temporary way to override PED ID settings or default. The PED Id parameter is optional. (0=local,1...65535=remote) If '0' is specified, the locally attached PED is used. If a value between 1 and 65535 is specified, the remote PED corresponding to that PED Id is used. If nothing is specified, then the value stored in the library for this slot is used. Unless the value stored in the library has been changed by using the 'ped set' command, or the 'PEDId' parameter in the 'Luna' section of cryptoki.ini, the value in the library is '0'. NOTE: The '-ped' option asserts for the duration of this login command, only. After the login completes, any PED ID that was set by the '-ped' option then reverts to whatever value was in effect before "partition login -ped <PED Id>".

Example

partition logout

Logout of the partition.

Syntax

partition logout

partition recoveryinit

Performs a High Availability Initialization of the current active session.

This lunacm command is provided as a demonstration of an operation that you would actually perform within your own application. Consider this command along with **lunacm partition -halogin** command, and the material in the SDK "High Availability Indirect Login Functions" .

Syntax

partition hainit -plabel <rsa_public_key_label> **-rlabel** <rsa_private_key_label> [**-keyhandle** <private_key_handle>]

Parameter	Shortcut	Description
-keyhandle	**-k**	If this option is included then the HA function is initialized with an already existing RSA keypair, indicated by the handle that you provide.
-plabel	**-pl**	Specifies a label for the RSA Public Key. Must be supplied if you do not provide a keyhandle pointing to an existing RSA Private Key.
-rlabel	**-rl**	Specifies a label for the RSA Private Key. Must be supplied if you do not provide a keyhandle pointing to an existing RSA Private Key.

Example

Creating a new RSA keypair to HA initialize the partition

```
lunacm:> partition hai -plabel myrsapub -rlabel myrsapriv

Generating RSA Key pair for HAInit...
User in slot 1 has been HA Initialised
with key handle 11.

Command Result : No Error
```

Initializing the partition when a suitable RSA keypair already exists

```
lunacm:> partition hai -keyhandle 11

User in slot 1 has been HA Initialised
with key handle 11.

Command Result : No Error
```


partition recoverylogin

Perform a Recovery Login on the target slot. This command is provided as a demonstration of an operation that you would actually perform within your own application. Consider this command along with the **partition -recoveryinit** command, and the material in the SDK "High Availability Indirect Login Functions".

Syntax

command parameter <variable> [**optional_parameter** <variable>]

Parameter	Shortcut	Description
-keyhandle	-kh	RSA Private Key handle to use on the current token (as specified by the slot number).
-slot	-s	Specifies the slot number assigned to the token/HSM Partition.
-user	-u	An integer that specifies the user type. The user type can be one of the following: • 0 - Security Officer • 1 - User • 1 - Crypto Officer

Example

```
lunacm:> partition recoverylogin -user 1 -slot 1 -keyhandle 11

This command will perform a Recovery Login
on the specified target slot.

Command Result : No Error
```


partition resetpw

Reset the partition password.

Syntax

partition resetpw

Example

```
lunacm> partition resetpw
```

partition restoresim2

Restore/insert HSM information from a SIM2 backup file. All objects in the file are restored to the HSM.

Syntax

partition restoreSIM2 [**-auth** <authorization password>] **-filename** <input file>

Parameter	Shortcut	Description
-auth	**-a**	The password that was used to protect the generated file, and now unlocks that file for restoring onto the partition. This parameter is required if the file is locked.
-filename	**-fi**	The name of the backup file on your computer, from which the restore operation is performed.

Example

```
partition restoresim2 -filename somepartfile -auth $omePa55word

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 restoresim3

Restore/insert HSM information from a SIM3 backup file. All objects in the file are restored to the HSM.

Syntax

partition restoresim3 [**-auth** <authorization password>] **-filename** <input file>

Parameter	Shortcut	Description
-auth	**-a**	The password that was used to protect the generated file, and now unlocks that file for restoring onto the partition. This parameter is required if the file is locked.
-filename	**-fi**	The name of the backup file on your computer, from which the restore operation is performed.

Example

```
partition restoresim3 -filename somepartfile -auth $omePa55word

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 token HSM or Luna PCI HSM whose contents are to be migrated to the Luna PCI 5.x 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 Luna PCI 5.x HSM partition.

Your target Luna PCI 5.x HSM partition has, and retains, whatever modern partition cloning domain was imprinted (on a red PED Key) when the partition was created. The partition setLegacyDomain 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.

Once the first legacy domain has been associated with your Luna PCI 5.x HSM Partition, that legacy domain is attached until the partition is deleted.

The ability to "partition setLegacyDomain" does not allow you to defeat the security provision that prevents cloning of objects across different domains.

As well, you cannot migrate objects from a Password authenticated token/HSM to a PED authenticated Luna PCI 5.x HSM partition, and you cannot migrate objects from a PED authenticated token/HSM to a Password authenticated Luna PCI 5.x HSM partition. Again, this is a security provision.

Please see "Legacy domains" for a description and summary of the possible combinations of source (legacy) tokens/HSMs and target (modern) HSM partitions and the disposition of token objects from one to the other.

Syntax

partition setLegacyDomain [**-legacydomain** <legacystring>] [**-force**]

Parameter	Shortcut	Description
-force	**-f**	Force action without prompting.
-legacydomain	**-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 -partition <name>

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.

Syntax

partition showinfo

Example

```
lunacm:> partition showinfo

HSM Serial Number -> 321312

Token Flags ->
     CKF_RNG
     CKF_LOGIN_REQUIRED
     CKF_USER_PIN_INITIALIZED
     CKF_RESTORE_KEY_NOT_NEEDED
     CKF_TOKEN_INITIALIZED

Slot Id -> 1

Session State -> CKS_RW_USER_FUNCTIONS

User Status: Logged In

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

Command Result : No Error
```


partition showpolicies

Displays the partition-level capability and policy settings for the partition and User.

Syntax

partition showpolicies

Example

```
lunacm:> partition showpolicies

Partition Capabilities
0: Enable private key cloning : 0
1: Enable private key wrapping : 0
2: Enable private key unwrapping : 1
3: Enable private key masking : 0
4: Enable secret key cloning : 0
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
14: Enable PED use without challenge : 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
19: Max non-volatile storage space : 3
20: Max failed user logins allowed : 10
21: Enable high availability recovery : 1
22: Enable activation : 0
23: Enable auto-activation : 0
25: Minimum pin length (inverted: 255 - min) : 248
26: Maximum pin length : 255
28: Enable Key Management Functions : 1
29: Enable RSA signing without confirmation : 1
30: Enable Remote Authentication : 1

Partition Policies
0: Allow private key cloning : 0
1: Allow private key wrapping : 0
2: Allow private key unwrapping : 1
3: Allow private key masking : 0
4: Allow secret key cloning : 0
5: Allow secret key wrapping : 1
6: Allow secret key unwrapping : 1
7: Allow secret key masking : 0
10: Allow multipurpose keys : 1
11: Allow changing key attributes : 1
14: Challenge for authentication not needed : 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
19: Max non-volatile storage space : 3
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
30: Allow Remote Authentication : 0
Command Result : No Error
```


partition smkclone

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

Syntax

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

Parameter	Shortcut	Description
-force	**-fo**	Force the action without prompting.
-password	**-p**	Target slot password.
-slot	**-s**	Target slot.

Example

```
lunacm:> partition smkclone -slot 2 -password $ome-Pa55word

Command Result : No Error
```


ped

Access the ped-level commands. These commands manage the use of Remote PED with your Luna HSM. You can use a PED connected to a distant computer to provide authentication when running HSM and partition commands.

Secure use of Remote PED is mediated by the Remote PED Vector (RPV) on the HSM and on orange Remote PED Keys (RPK). Obviously, the commands to administer your HSM could be issued remotely as well, using SSH or remote desktop connection. See "Remote PED and PEDClient" and "Remote PED - using".

Syntax

ped

connect
disconnect
get
set
show
vector

Parameter	Shortcut	Description
connect	**c**	Connect to the remote PED. See
disconnect	**d**	Disconnect from the remote PED. See
get	**g**	Show the PED ID and the listening slot ID. See "ped get" on page 114.
set	**se**	Set the PED ID. See "ped set" on page 115.
show	**sh**	Display the remote PED server configuration. See
vector	**v**	Initialize or delete the remote PED vector. See "ped vector" on page 117.

ped connect

Connect to a remote PED. This command instructs PedClient to attempt to connect to the Remote PED Server at the IP address and port specified on the command line, or configured using the **ped set** command. See "ped set" on page 115 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 PED Server. 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**.
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 specifiy at least an IP address. If no port is specified, the default port (1503) is used.

Syntax

ped connect [**-ip** <ip_address>] [**-port** <port>] [**-serial** <serial_num>] [**-force**]

Parameter	Shortcut	Description
-force	**-f**	Force the action without prompting.
-ip	**-i**	Specifies the IP Address of the
-port	**-p**	Network Port (0-65535). **Default:** 1503
-serial	**-s**	Token Serial Number

Example

```
lunacm:>ped connect -ip 172.20.10.155

Luna PED operation required to connect to Remote PED - use orange PED key(s).
Ped Client Version 1.0.5 (10005)
Ped Client launched in startup mode.
PED client local IP : 172.20.9.77/192.168.255.223
Starting background process
Background process started
Ped Client Process created, exiting this process.

Command Result : 0 (Success)
```


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 [**-serial** <serialnum>] [**-force**]

Parameter	Shortcut	Description
-force	-f	Force the action without prompting.
-serial	**-s**	Token Serial Number

Example

```
lunacm:>ped disconnect

If you are sure that you wish to disconnect, then enter 'proceed', otherwise type 'quit'.
> proceed
Proceeding...
Remote PED connection closed.

Command Result : 0 (Success)
```


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 a default IP address and/or port that are used by the **ped connect** command when establishing a connection to a Remote PED Server. See "ped connect" on page 111 for more information.

Syntax

ped set {[**-ip** <ped_server_ip>] | [**-port** <ped_server_port_number>]}

Parameter	Shortcut	Description
-ip	**-i** <ped server ip>	Specifies the default IP Address used by the **ped connect** command.
-port	**-p** <server port num>	Specifies the default port used by the **ped connect** command. **Range:** 0-65535 **Default:** 1503

Example

```
lunacm:>hsm ped set -ip 106.55.19.59 -port 3456

Command Result : 0 (Success)

lunacm:>hsm ped show

Configured Remote PED Server IP address: 106.55.19.59
Configured Remote PED Server Port: 3456

Ped Client Version 2.0.0 (20000)
Ped Client launched in status mode.
Callback Server is running..

Callback Server Information:
Hostname:                       local_host
IP:                             106.55.9.165
Software Version:               2.0.0 (20000)

Operating Information:
Admin Port:                        1501
External Admin Interface:          No

Callback Server Up Time:                    269788 (secs)
Callback Server Current Idle Time:          269788 (secs)
Callback Server Total Idle Time:            269788 (secs) (100%)
Idle Timeout Value:                1800 (secs)

Number of PED ID Mappings:           0

Number of HMSs:                       1
HSM List:
Device Type:                       PCI HSM
HSM Serial Number:                 789654
HSM Firmware Version:              6.30.0
HSM Cmd Protocol Version:          18
HSM Callback IO Version:           1
HSM Callback Protocol Version:     1
HSM Up Time:                       269787 (secs)
```



```
HSM Total Idle Time:                269787 (secs) (100%)
HSM Current Idle Time:              269787 (secs)

Show command passed.

Command Result : No Error
```

ped vector

Create or delete a Remote PED Vector (RPV). Use this command to the following:

- create a Remote PED Vector (RPV) and imprint it onto the HSM and an orange PED Key (RPK).
- delete an RPV from the HSM.

Syntax

ped vector

delete
init

Parameter	Shortcut	Description
delete	**d**	Delete a Remote PED Vector (RPV) from the HSM. This does not affect RPV on orange PED Key(s). No PED action required.
init	**i**	Create a Remote PED Vector (RPV) and imprint it on an orange PED Key, or accept a pre-existing RPV from an orange PED Key. PED action required.

Example

```
lunacm:> ped vector init

You are about to initialize the Remote PED Vector
Are you sure (y|Y for yes, n|N for no)? Y

Please attend to the PED.

Command Result : No Error
```

remotebackup start

Start the remote backup server on the current slot. Your Luna Remote Backup HSM must be connected to that computer and the Luna 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 <port> **-timeout** <seconds>] [**-commandtimeout** <seconds>] [**-debug**]

Parameter	Shortcut	Description
-commandtimeout	**-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	**-po**	Port number the server will listen on. If no port number is provided, the default port number is used. **Default:** 2222
-timeout	**-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
```


slot

Access the slot-level commands.

Slots originated as a cryptographic software concept, later overlaid onto HSM function, and originally corresponded to individual removable cryptographic "token" HSMs. In general, a physical "slot" correlates to a PKCS#11 crypto slot. However, to allow for cases where more than one HSM, or where physical Luna HSMs containing multiple virtual HSMs can be connected, we declare placeholder slots that might or might not be occupied by a physical device, but which are seen by the library as ready for a device to be connected.

This allows (for example) a USB-connected HSM to be connected to a Luna appliance or to a Luna 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.

Syntax

slot

configset
configshow
list
partitionlist
set

Parameter	Shortcut	Description
configset	**cset**	Set a configuration item for a slot. See "slot configset" on page 120.
configshow	**cshow**	Show the configuration for a slot . See "slot configshow" on page 121.
list	**l**	List the available slots. See "slot list" on page 122.
partitionlist	**plist**	List the partitions for a slot. See "slot partitionlist" on page 123.
set	**s**	Set the current slot. See "slot set" on page 124.

slot configset

Set the configuration information for the specified slot number.

Syntax

slot configset -slot <slot_number> **-partitionname** <partitition_name>

Parameter	Shortcut	Description
-partitionname	**-p**	The partition name of the slot.
-slot	**-s**	Specifies the number of the slot for which you wish to set configuration settings.

Example

```
lunacm:> slot configset -slot 1 -partition thatslot
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>

Parameter	Shortcut	Description
-slot	**-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. You might have more than one Luna module, or perhaps another SafeNet token product on your system.

Syntax

slot list

Example

```
lunacm:> slot list

Slot Id ->                3
HSM Label ->              myluna
HSM Serial Number ->      65130
HSM Model ->              K3 Base
HSM Firmware Version ->   4.5.1

Current Slot ID:  3

Command Result : No Error
```


slot partitionlist

List the partitions for the specified slot.

Syntax

slot partitionlist -slot <slot number>

Parameter	Shortcut	Description
-slot	**-s**	The slot for which you want to list the partitions.

Example

```
lunacm:> slot partitionlist -slot 1

Number of Partitions: 1
Partition #: 1
Partition Name: mypar1

Command Result : No Error

lunacm:> slot plist -slot 2

Number of Partitions: 1
Partition #: 1
Partition Name: Cryptoki User

Command Result : No Error
```

slot set

Set the current slot number. The current slot is the slot to which you want the **lunacm** commands to apply.

> **Note:** This command is useful only if you have more than one Luna module in your computer. In that case, 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 modules (in their slots) you wish to address with **lunacm** commands.

Syntax

slot set -slot <slot_number>

Parameter	Shortcut	Description
-slot	**-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
```


srk

Access the srk-level commands. These commands manage the secure recovery key (SRK) behavior and the setting and recovery of Secure Transport Mode. See MTK and SRK discussion here.

Syntax

srk

disable
enable
generate
recover
show
transport

Parameter	Shortcut	Description
disable	**d**	Disable Secure Transport Mode functionality. See "srk disable" on page 126.
enable	**e**	Enable Secure Transport Mode functionality. See "srk enable" on page 127.
generate	**g**	Generate a new SRK. See "srk generate" on page 128.
recover	**r**	Recover from temper or exit transport mode. See "srk recover" on page 129.
show	**s**	Show the Secure Recovery state. See "srk show" on page 130.
transport	**t**	Set the HSM into transport mode. See "srk transport" on page 131.

srk disable

Disable external tamper keys. This command disables the use of external split(s) of the SRV (secure recovery vector) on purple PED Keys (SRK). The external split is brought from the purple key, back into the HSM. When SRK is disabled:

- Secure Transport Mode cannot be set.
- Any tamper event that is detected by the HSM stops the HSM only until you restart. The MTK is destroyed by a tamper, but is immediately recreated at the restart if both splits are internally available (i.e., when SRK is disabled).

The SO must be logged in to the HSM to issue this command.

Syntax

srk disable

Example

```
lunacm:> srk disable

Please attend to the PED.
Secure Transport functionality was successfully disabled.

Command Result : No Error
```

srk enable

Enable external tamper keys. This command enables the use of external split(s) of the SRV (secure recovery vector) on purple PED Keys (SRK). The external split is brought from the HSM to a purple key, and erased from the HSM, leaving only one split on the HSM. When SRK is enabled:

- Secure Transport Mode can be set.
- Any tamper event that is detected by the HSM stops the HSM until you restart and perform "srk recover". The "srk recover" operation makes the externally provided split (from the purple key) available to combine with the internal split, allowing the MTK to be recreated. The MTK is destroyed by a tamper (or by setting STM), and cannot be recreated until both splits are available (if SRK is enabled).

The SO must be logged in to the HSM to issue this command.

Syntax

srk enable

Example

```
lunacm:> srk enable

Please attend to the PED.
Secure Transport functionality was successfully enabled.

Command Result : No Error
```


srk generate

Resplit the Secure Recovery Key. This command generates new splits of the Secure Recovery Key. The internal split is stored in a secure memory area on the HSM. The external split is imprinted upon a purple PED Key (or multiple purple keys if you invoke MofN).

The PED must be connected, and you must present "new" purple PED Keys when prompted. "New" in this case, means a purple PED Key that is literally new, or a PED Key that has been used for another purpose - as long as it does not contain the current valid external SRK split, before the new generating operation. For safety reasons, the HSM and PED detect and refuse to overwrite the current purple PED Key(s).

Syntax

srk generate

Example

```
lunacm:> srk generate

Please attend to the PED.
New SRK generated.

Command Result : 0 (Success)
```


srk recover

Exit transport or tamper mode. This command reconstitutes the SRV on the HSM, using the SRK split(s) on the purple SRK PED Key(s), which in turn recreates the HSM's Master Key, allowing the HSM and its contents to be accessed and used again, following Transport Mode or a tamper event. The PED must be connected, and you must present the correct purple PED Keys when prompted.

Syntax

srk recover

Example

```
lunacm:> srk recover

Please attend to the PED.
Successfully recovered from Transport Mode/Tamper.

Command Result : No Error
```

srk show

Display the current SRK state.

Syntax

srk show

Example

```
lunacm:> srk show

Secure Transport Functionality is supported and disabled

Secure Recovery State flags:
================================
SRK Regeneration required:        0
Hardware (tamper) Zeroized:        0
Transport Mode:             0
Locked:                     1
Command Result : No Error

lunacm:> srk enable

Please attend to the PED.
Secure Transport functionality was successfully enabled.

Command Result : No Error

lunacm:> srk show
Secure Transport Functionality is supported and ensabled
Secure Recovery State flags:
================================
SRK Regeneration required:        0
Hardware (tamper) Zeroized:        0
Transport Mode:             0
Locked:                     1

Command Result : No Error
```


srk transport

Enter transport mode. This command places the HSM in transport mode, destroying the Master Key and causing all HSM content to be unusable. The use of external split(s) of the SRK (secure recovery key) on purple PED Keys must already be enabled.

The SO need not be logged in to the HSM to issue this command.

Syntax

srk transport

Example

```
lunacm:> srk transport

You are about to configure the HSM in transport mode.
If you proceed, Secure Recovery keys will be created
and the HSM will be tampered.
Are you sure you wish to continue?

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

Configuring the HSM for transport...
Please attend to the PED.
HSM was successfully configured for transport.

Command Result : No Error

lunacm:> hsm login

The HSM in the current slot (slot 1) cannot process the command
"login" in its current state.
--> SRK State is invalid.

Command Result: No Error
```

