

SafeNet Network HSM 6.3

LunaCM Command Reference Guide

Document Information

| | |
|-----------------------------|----------------|
| Product Version | 6.3 |
| Document Part Number | 007-011136-015 |
| Release Date | 14 July 2017 |

Revision History

| Revision | Date | Reason |
|-----------------|--------------|------------------|
| A | 14 July 2017 | Initial release. |

Trademarks, Copyrights, and Third-Party Software

Copyright 2001-2017 Gemalto. All rights reserved. Gemalto and the Gemalto logo are trademarks and service marks of Gemalto and/or its subsidiaries and are registered in certain countries. All other trademarks and service marks, whether registered or not in specific countries, are the property of their respective owners.

Acknowledgements

This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit.
(<http://www.openssl.org>)

This product includes cryptographic software written by Eric Young (eay@cryptsoft.com). This product includes software written by Tim Hudson (tjh@cryptsoft.com).

This product includes software developed by the University of California, Berkeley and its contributors.

This product uses Brian Gladman's AES implementation.

Refer to the End User License Agreement for more information.

Disclaimer

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

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

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

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

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

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

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

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

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

Acknowledgements

This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit. (<http://www.openssl.org>)

This product includes cryptographic software written by Eric Young (eay@cryptsoft.com). This product includes software written by Tim Hudson (tjh@cryptsoft.com).

This product includes software developed by the University of California, Berkeley and its contributors.

This product uses Brian Gladman's AES implementation.

Refer to the End User License Agreement for more information.

Regulatory Compliance

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

USA, FCC

This device complies with Part 15 of the FCC rules. Operation is subject to the following two conditions:

- (1) This device may not cause harmful interference, and
- (2) This device must accept any interference received, including interference that may cause undesired operation.

This equipment has been tested and found to comply with the limits for a "Class B" digital device, pursuant to part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation.

If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna

- Increase the separation between the equipment and receiver
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected
- Consult the dealer or an experienced radio/TV technician for help
- Changes or modifications not expressly approved by SafeNet could void the user's authority to operate the equipment.

Canada

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

Europe

This product is in conformity with the protection requirements of EC Council Directive 2004/108/EC. Conformity is declared to the following applicable standards for electro-magnetic compatibility immunity and susceptibility; CISPR22 and IEC801. This product satisfies the CLASS B limits of EN 55022.

CONTENTS

| | | |
|---|---|-----------|
| PREFACE | About the LunaCM Command Reference Guide | 9 |
| Customer Release Notes | | 9 |
| Gemalto Rebranding | | 9 |
| Audience | | 10 |
| Document Conventions | | 10 |
| Notes | | 10 |
| Cautions | | 10 |
| Warnings | | 11 |
| Command Syntax and Typeface Conventions | | 11 |
| Support Contacts | | 12 |
| 1 | Using LunaCM | 13 |
| Accessing LunaCM | | 13 |
| LunaCM Features | | 14 |
| Case Insensitivity | | 14 |
| Quotation Marks | | 15 |
| Operation | | 15 |
| 2 | LunaCM commands | 16 |
| appid | | 20 |
| appid close | | 21 |
| appid info | | 22 |
| appid open | | 23 |
| appid set | | 24 |
| audit | | 25 |
| audit changepw | | 27 |
| audit config | | 28 |
| audit export | | 30 |
| audit import | | 31 |
| audit init | | 32 |
| audit login | | 33 |
| audit logmsg | | 34 |
| audit logout | | 35 |
| audit status | | 36 |
| audit time | | 37 |
| audit verify | | 38 |
| clientconfig | | 39 |
| clientconfig deleteServer | | 40 |
| clientconfig deploy | | 41 |
| clientconfig listservers | | 42 |
| clientconfig restart | | 43 |

| | |
|----------------------------------|-----|
| clientconfig verify | 44 |
| file display | 45 |
| hagroup | 46 |
| hagroup addmember | 48 |
| hagroup addstandby | 49 |
| hagroup creategroup | 50 |
| hagroup deletegroup | 51 |
| hagroup halog | 52 |
| hagroup haonly | 53 |
| hagroup listgroups | 54 |
| hagroup recover | 56 |
| hagroup recoverymode | 57 |
| hagroup removemember | 58 |
| hagroup removestandby | 59 |
| hagroup retry | 60 |
| hagroup interval | 61 |
| hagroup synchronize | 62 |
| hsm | 63 |
| hsm changehsmpolicy | 66 |
| hsm changepw | 67 |
| hsm changesopolicy | 68 |
| hsm clear | 69 |
| hsm clone | 70 |
| hsm contents | 71 |
| hsm factoryreset | 72 |
| hsm init | 73 |
| hsm login | 76 |
| hsm logout | 78 |
| hsm migratepedkey | 79 |
| hsm monitor | 80 |
| hsm recoveryinit | 82 |
| hsm recoverylogin | 83 |
| hsm reset | 84 |
| hsm restart | 85 |
| hsm restoreuser | 86 |
| hsm restoresim2 | 87 |
| hsm rollbackfw | 88 |
| hsm setlagacydomain | 90 |
| hsm showinfo | 91 |
| hsm showmechanism | 93 |
| hsm showpolicies | 95 |
| hsm updatecap | 100 |
| hsm updatefw | 101 |
| partition | 102 |
| partition activate | 108 |
| partition archive | 110 |
| partition archive backup | 112 |
| partition archive contents | 115 |
| partition archive delete | 117 |

| | |
|--------------------------------------|-----|
| partition archive list | 119 |
| partition archive restore | 120 |
| partition changelabel | 123 |
| partition changepolicy | 125 |
| partition changepw | 126 |
| partition clear | 128 |
| partition clone | 129 |
| partition contents | 130 |
| partition create | 131 |
| partition createchallenge | 138 |
| partition createuser | 139 |
| partition deactivate | 140 |
| partition delete | 141 |
| partition init | 142 |
| partition login | 144 |
| partition logout | 145 |
| partition recoveryinit | 146 |
| partition recoverylogin | 147 |
| partition resetpw | 148 |
| partition resize | 148 |
| partition restoresim2 | 152 |
| partition restoresim3 | 153 |
| partition setlegacydomain | 154 |
| partition showinfo | 155 |
| partition showmechanism | 158 |
| partition policyTemplateChange | 160 |
| partition policyTemplatecreate | 162 |
| partition policyTemplateDelete | 164 |
| partition policyTemplateList | 166 |
| partition policytempleload | 167 |
| partition policyTemplateSave | 168 |
| partition policyTemplateShow | 169 |
| partition showpolicies | 171 |
| partition smkclone | 173 |
| ped | 174 |
| ped connect | 175 |
| ped disconnect | 177 |
| ped get | 178 |
| ped set | 179 |
| ped show | 181 |
| ped vector | 182 |
| remotebackup start | 183 |
| role | 184 |
| role changepw | 185 |
| role createChallenge | 188 |
| role deactivate | 189 |
| role init | 190 |
| role list | 192 |
| role login | 194 |

| | |
|---------------------------------------|-----|
| role logout | 197 |
| role recoveryinit | 198 |
| role recoverylogin | 199 |
| role resetpw | 200 |
| role setdomain | 201 |
| role show | 203 |
| slot | 204 |
| slot configset | 205 |
| slot configshow | 207 |
| slot list | 208 |
| slot partitionlist | 210 |
| slot set | 211 |
| srk | 212 |
| srk disable | 213 |
| srk enable | 214 |
| srk generate | 215 |
| srk recover | 216 |
| srk show | 217 |
| srk transport | 218 |
| stc | 219 |
| stc disable | 221 |
| stc enable | 222 |
| stc identitycreate | 223 |
| stc identitydelete | 224 |
| stc identityexport | 225 |
| stc identityshow | 226 |
| stc partitionderegister | 227 |
| stc partitionregister | 228 |
| stc status | 229 |
| stc tokeninit | 230 |
| stc tokenlist | 231 |
| stcconfig | 232 |
| stcconfig activationtimeoutset | 234 |
| stcconfig activationtimeoutshow | 235 |
| stcconfig cipherdisable | 236 |
| stcconfig cipherenable | 238 |
| stcconfig ciphershow | 240 |
| stcconfig clientderegister | 241 |
| stcconfig clientlist | 242 |
| stcconfig clientregister | 243 |
| stcconfig hmacdisable | 244 |
| stcconfig hmacenable | 246 |
| stcconfig hmacshow | 248 |
| stcconfig partitionidexport | 249 |
| stcconfig partitionidshow | 250 |
| stcconfig rekeythresholdset | 251 |
| stcconfig rekeythresholdshow | 252 |
| stcconfig replaywindowset | 253 |
| stcconfig replaywindowshow | 254 |

PREFACE

About the LunaCM Command Reference Guide

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

- ["Using LunaCM" on page 13](#)
- ["LunaCM commands" on page 16](#)

This preface also includes the following information about this document:

- ["Customer Release Notes" below](#)
- ["Gemalto Rebranding" below](#)
- ["Audience" on the next page](#)
- ["Document Conventions" on the next page](#)
- ["Support Contacts" on page 12](#)

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/cm_luna_hsm_6-3.pdf

Gemalto Rebranding

In early 2015, Gemalto completed its acquisition of SafeNet, Inc. As part of the process of rationalizing the product portfolios between the two organizations, the Luna name has been removed from the SafeNet HSM product line, with the SafeNet name being retained. As a result, the product names for SafeNet HSMs have changed as follows:

| Old product name | New product name |
|------------------|---------------------|
| Luna SA HSM | SafeNet Network HSM |
| Luna PCI-E HSM | SafeNet PCIe HSM |
| Luna G5 HSM | SafeNet USB HSM |
| Luna PED | SafeNet PED |

| Old product name | New product name |
|------------------|--------------------|
| Luna Client | SafeNet HSM Client |
| Luna Dock | SafeNet Dock |
| Luna Backup HSM | SafeNet Backup HSM |
| Luna CSP | SafeNet CSP |
| Luna JSP | SafeNet JSP |
| Luna KSP | SafeNet KSP |



Note: These branding changes apply to the documentation only. The SafeNet HSM software and utilities continue to use the old names.

Audience

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

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

Support Contacts

| Contact method | Contact | |
|--|--|------------------|
| Phone (Subject to change. An up-to-date list is maintained on the Technical Support Customer Portal) | Global | +1 410-931-7520 |
| | Australia | 1800.020.183 |
| | India | 000.800.100.4290 |
| | Netherlands | 0800.022.2996 |
| | New Zealand | 0800.440.359 |
| | Portugal | 800.863.499 |
| | Singapore | 800.1302.029 |
| | Spain | 900.938.717 |
| | Sweden | 020.791.028 |
| | Switzerland | 0800.564.849 |
| | United Kingdom | 0800.056.3158 |
| | United States | (800) 545-6608 |
| Web | https://safenet.gemalto.com | |
| Technical Support Customer Portal | https://supportportal.gemalto.com Existing customers with a Technical Support Customer Portal account can log in to manage incidents, get the latest software upgrades, and access the Knowledge Base. To create a new account, click the Register link at the top of the page. You will need your Customer Identifier number. | |

Using LunaCM

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

- ["Accessing LunaCM" below](#)
- ["LunaCM Features" on the next page](#)

Accessing LunaCM

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

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

- internally installed SafeNet PCIe HSM 6.x HSMs (K6 HSM card)
- locally USB-connected SafeNet USB HSMs
- remotely located SafeNet Network HSM application partitions, made available by a NTLS or STC network link between the distant HSM appliance and partition(s) and the local client computer.

To access LunaCM

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

| | |
|----------------------|---|
| Windows | <code>C:\> cd c:\Program Files\SafeNet\LunaClient</code> <code>C:\Program Files\SafeNet\LunaClient\> lunacm</code> |
| Linux/AIX | <code>> cd /usr/safenet/lunaclient/bin</code> <code>> ./lunacm</code> |
| Solaris/HP-UX | <code>> cd /opt/safenet/lunaclient/bin</code> <code>> ./lunacm</code> |

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

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



Note: For SafeNet PCIe HSM and SafeNet USB HSM, LunaCM is used to administer both the HSM as HSM SO, and the application partition, as HSM SO for HSMs with firmware older than 6.22.0, or as Partition SO for HSMs with firmware 6.22.0 and newer.



Note: For SafeNet Network HSM, LunaCM is used to manage application partitions (assuming an NTLS or STC link between your SafeNet HSM Client computer and the SafeNet Network HSM appliance). LunaCM is not used to perform HSM-wide administration by the HSM SO on SafeNet Network HSM - for that you must log into a LunaSH (lunash) session via SSH.

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

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

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 SafeNet HSMs. For Trusted Path Authenticated HSM, do not type the password - you are directed to the SafeNet PED, which prompts for the required PED Key.

Quotation Marks

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

Operation

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

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

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

LunaCM commands

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

- a brief description of the command function
- the command syntax and parameter descriptions
- usage examples

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

- SafeNet Network HSM application partitions (if any), network-connected to the host computer via NTLS or STC channels,
- SafeNet PCIe HSMs (if any) installed within the host computer,
- SafeNet USB HSMs (if any) connected via USB to the host computer.

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

Where did my command go?

The question mark (or any incorrect command) shows the lunacm commands available to be used in the current slot. The availability of lunacm commands changes according to four possible scenarios:

- the current slot is the HSM administrative partition for an HSM with firmware version 6.22.0 or newer
- the current slot is an application partition that has its own SO (a PPSO partition), on an HSM with firmware version 6.22.0 or newer
- the current slot is a separate-but-not-independent application partition that is administered by the HSM SO, and does not have its own separate SO (a legacy-style partition) on an HSM with firmware version 6.22.0 or newer
- the current slot is the HSM administrative partition and application partition for an HSM with firmware older than version 6.22.0 (a true legacy partition).

No single partition type has access to all the possible commands within lunacm.

Note: Persistence of login state

For HSMs with firmware 6.22.0 or newer, login state of a slot is preserved until explicitly ended (such as with "logout" or "deactivate" or closing the application). Therefore, login state persists when you switch slots in lunacm. That is, if you were logged into the partition in slot 1, then set current slot to slot 2, then came back to slot 1, the login state for the partition in slot 1 would still be in force, with no need to reinstate it.

For HSMs with older firmware, changing to a different slot terminates the login state in the original slot, as was always the case.

Lunacm command list on HSM admin partition, f/w 6.22.0

(These are the commands that you see if the current-slot partition is the initialized HSM's administrative partition, while the HSM is at firmware version 6.22.0 or newer. Some of these commands act on the current-slot partition; some have a -slot option to direct their action to another partition/slot.)

Select a link to display the command syntax or to help you to navigate to the sub-command you need:

appid
audit
file
clientconfig
hagroup
hsm
partition
ped
remoteBackup
role
slot
srk
stc
stcconfig

| Parameter | Shortcut | Description |
|---------------------|-------------|--|
| appid | a | > Manage Application Ids. See " appid " on page 20 . |
| audit | au | Audit commands. See " audit " on page 25 |
| clientconfig | ccfg | Client configuration. See " clientconfig " on page 39 . |
| file | f | File commands. See " file display " on page 45 . |
| hagroup | ha | High Availability Group commands. See " hagroup " on page 46 . |
| hsm | hs | HSM commands. See " hsm " on page 63 . |
| partition | par | Partition commands. See " partition " on page 102 . |
| ped | p | Remote PED commands. See " ped " on page 174 . |

| Parameter | Shortcut | Description |
|---------------------|-------------|--|
| remoteBackup | rb | Manage Remote Backup server. See "remotebackup start" on page 183 . |
| role | ro | Role management commands. See "role" on page 184 . |
| slot | s | Slot management commands. See "slot" on page 204 . |
| srk | r | Secure Recovery commands. See "srk" on page 212 . |
| stc | stc | Secure Trusted Channel commands. See "stc" on page 219 . |
| stcconfig | stcc | Secure Trusted Channel configuration commands. See "stcconfig" on page 232 . |

Lunacm command list on application partition, f/w 6.22.0

(These are the commands that you see if the current-slot partition is the initialized HSM's administrative partition, while the HSM is at firmware version 6.22.0 or newer. Some of these commands act on the current-slot partition; some have a -slot option to direct their action to another partition/slot.)

Select a link to display the command syntax or to help you to navigate to the sub-command you need:

[appid](#)
[file](#)
[clientconfig](#)
[hagroup](#)
[partition](#)
[ped](#)
[remoteBackup](#)
[role](#)
[slot](#)
[stc](#)
[stcconfig](#)

| Parameter | Shortcut | Description |
|---------------------|-------------|---|
| appid | a | > Manage Application Ids. See "appid" on page 1 . |
| file | f | File commands. See "file display" on page 1 . |
| clientconfig | ccfg | Client configuration. See "clientconfig" . |
| hagroup | ha | High Availability Group commands. See "hagroup" on page 1 . |
| partition | par | Partition commands. See "partition" on page 1 . |
| ped | p | Remote PED commands. See "ped" on page 1 . |

| Parameter | Shortcut | Description |
|---------------------|-------------|--|
| remoteBackup | rb | Manage Remote Backup server. See "remotebackup start" on page 1 . |
| role | ro | Role management commands. See "role" . |
| slot | s | Slot management commands. See "slot" on page 1 . |
| stc | stc | Secure Trusted Channel commands. See "stc" on page 219 . |
| stcconfig | stcc | Secure Trusted Channel configuration commands. See "stcconfig" on page 232 . |

appid

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

Syntax

appid

close
info
open
set

| Option | Shortcut | Description |
|--------------|----------|--|
| close | c | Close a previously set access ID. See "appid close" on page 1 . |
| info | i | Display information for the access IDs. See "appid info" on page 1 . |
| open | o | Open a previously set access ID. See "appid open" on page 1 . |
| set | s | Set an access ID. See "appid set" on page 1 . |

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
help           he      print this help
?              ?       print this help
```

Syntax: appid <sub command>

```
Command Result : No Error
```

appid close

Close an application access ID on the HSM to prevent your applications from using it to access the HSM. Application IDs are assigned as a way of sharing login state among multiple processes. AppIDs require two 4-byte/32-bit unsigned integers, one designated "major" and the other designated "minor". For a full description of application IDs, see ["Application IDs" on page 1](#) in the *SDK Reference Guide*.



Note: If you are concerned that an unauthorized process might be able to take over a login state, then you can use large, difficult-to-guess numbers for the major and minor appids. If this is not a concern, or for use in a development lab, you can use any arbitrary, conveniently small integers.

Syntax

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

| Parameter | Shortcut | Description |
|-----------------------|------------|------------------|
| -major <value> | -ma | The major appid. |
| -minor <value> | -mi | The minor appid. |

Example

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

```
Command Result : No Error
```

appid info

Display the currently set application IDs. This list includes all set application IDs, regardless of whether they are open or closed. For a full description of application IDs, see "[Application IDs](#)" on page 1 in the *SDK Reference Guide*.

Syntax

appid info

Example

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

    Application ID Major: 307
    Application ID Minor: 207

Command Result : No Error
```

appid open

Open an application access ID on the HSM to allow your applications to use it to access the HSM. Application IDs are assigned as a way of sharing login state among multiple processes. AppIDs require two 4-byte/32-bit unsigned integers, one designated "major" and the other designated "minor". For a full description of application IDs, see ["Application IDs" on page 1](#) in the *SDK Reference Guide*.



Note: If you are concerned that an unauthorized process might be able to take over a login state, then you can use large, difficult-to-guess numbers for the major and minor appids. If this is not a concern, or for use in a development lab, you can use any arbitrary, conveniently small integers.

Syntax

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

| Parameter | Shortcut | Description |
|-----------------------|------------|------------------|
| -major <value> | -ma | The major appid. |
| -minor <value> | -mi | The minor appid. |

Example

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

```
Command Result : No Error
```

appid set

Set an application access ID on the HSM. Application IDs are assigned as a way of sharing login state among multiple processes. AppIDs require two 4-byte/32-bit unsigned integers, one designated "major" and the other designated "minor". After setting an appid, you must open it using **appid open** to allow your applications to use it to access the HSM. Once you set an appid you can open and close it, as required, to allow or deny application access to the HSM using the appid. For a full description of application IDs, see "[Application IDs](#)" on page 1 in the *SDK Reference Guide*.



Note: If you are concerned that an unauthorized process might be able to take over a login state, then you can use large, difficult-to-guess numbers for the major and minor appids. If this is not a concern, or for use in a development lab, you can use any arbitrary, conveniently small integers.

Syntax

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

| Parameter | Shortcut | Description |
|-----------------------------|------------|------------------|
| -major <value> | -ma | The major appid. |
| -minor <value> | -mi | The minor appid. |

Example

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

```
Command Result : No Error
```


audit

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

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

Note: The list on this page is all the "audit" commands that are available to you when the current slot is an HSM with firmware older than version 6.22.0.

Where the HSM in the current slot has firmware version 6.22.0 or newer :



- application partition slots do not show the audit commands at all (as those commands are applicable only to an HSM administrative slot)

- HSM administrative slots with newer firmware show only some of the "audit" commands; the authentication-related functions are taken over by "role" commands instead.

Syntax for firmware older than version 6.22.0

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. <i>[Older firmware only]</i> See "audit changepw" on page 27 . |
| config | co | Configure the audit parameters. See "audit config" on page 28 . |
| export | e | Read the wrapped log secret from the HSM. See "audit export" on page 30 . |
| import | m | Import the wrapped log secret to the HSM. See "audit import" on page 31 . |
| init | i | Initialize the HSM Audit user. <i>[Older firmware only]</i> See "audit init" on page 32 . |

| Parameter | Shortcut | Description |
|---------------|-------------|---|
| login | logi | Login to the HSM as the Audit user. <i>[Older firmware only]</i> See "audit login" on page 33 . |
| logmsg | logm | Write a message to the HSM's log. See "audit logmsg" on page 34 . |
| logout | logo | Logout from the HSM as the Audit user. <i>[Older firmware only]</i> See "audit logout" on page 35 . |
| status | s | Show the status of the logging subsystem. See "audit status" on page 36 . |
| time | t | Synchronize the HSM time to the host, or get the HSM time. See "audit time" on page 37 . |
| verify | v | Verify a block of log messages. See "audit verify" on page 38 . |

Syntax for firmware version 6.22.0 or newer

audit

config
export
import
logmsg
status
time
verify

| Parameter | Shortcut | Description |
|---------------|-------------|--|
| config | co | Configure the audit parameters. See "audit config" on page 28 . |
| export | e | Read the wrapped log secret from the HSM. See "audit export" on page 30 . |
| import | m | Import the wrapped log secret to the HSM. See "audit import" on page 31 . |
| logmsg | logm | Write a message to the HSM's log. See "audit logmsg" on page 34 . |
| status | s | Show the status of the logging subsystem. See "audit status" on page 36 . |
| time | t | Synchronize the HSM time to the host, or get the HSM time. See "audit time" on page 37 . |
| verify | v | Verify a block of log messages. See "audit verify" on page 38 . |

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 SafeNet HSM with PED Authentication. In the case of multiple HSMs in the host computer, the command works on the current slot.



Note: This command applies to slots with HSMs having older firmware only. If the HSM in the current slot has firmware 6.22.0 or newer, then this command is replaced by ["role changepw" on page 185](#).

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 |
|-----------|----------|--|
| evmask | e | <p>The value you want to configure for the specified parameter.</p> <p>Valid values for the event parameter</p> <p>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:</p> <ul style="list-style-type: none"> • [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[!]: log everything (user will be warned) • [n]one: turn logging off <p>Note: When specifying an event class to log, you must specify whether successful or failed events are to be logged. For example, to log all key management events you would use the command "audit config e t,s,f".</p> |
| get | g | get (show) the current configuration |
| interval | i | <p>Valid values for the rotation interval parameter</p> <p>Enter one of the following options for the log rotation interval:</p> <ul style="list-style-type: none"> • hourly [@min] • daily [@hour:min] • weekly [@day:hour:min] • monthly [@date:hour:min] • never |
| path | p | path on the HOST to which logs will be written |
| size | s | <p>size limit of a log, to trigger rotation</p> <p>Valid values for the size parameter:</p> |

| Parameter | Shortcut | Description |
|-----------|----------|--|
| | | <p>An integer string signifying the size of the log in bytes. The optional modifiers k or m may be given after the string to specify KB or MB (for example, s 8388608, s 8192k, and s 8m all specify rotation when log size reaches 8MB).</p> <p>Valid Range: 4096k - 2097151k</p> <p>Default: 2097151k</p> |

Example

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

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

```
lunacm:> audit config e l,f,s
```

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

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

```
Command Result : No Error
```

```
lunacm:> audit config get
```

```
Current Logging Configuration
```

```
-----
event mask      : Log everything
rotation interval : daily@0:00
rotation size (KB): 2087151
path to log     : /var/audit/
```

```
Command Result : No Error
```



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

audit export

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

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, you are asked to “proceed” unless the `-force` switch is provided at the command line.



Note: This command is used for HSMs with firmware older than version 6.22.0. Expect an entry 'LUNA_CREATE_AUDIT_CONTAINER' in the audit log, when auditing is initialized. For HSMs with firmware 6.22.0 or newer, use "[role init](#)" on [page 190](#), and specify the `-name Auditor` parameter.

Syntax

audit init [`-auth`] [`-force`]

| Parameter | Shortcut | Description |
|---------------------|-----------------|--|
| <code>-auth</code> | <code>-a</code> | This option starts a login after the initialization completes. |
| <code>-force</code> | <code>-f</code> | If this option is included in the list, the audit role initialization action is forced without prompting 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:
> 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.



Note: This command applies to slots with HSMs having older firmware only. If the HSM in the current slot has firmware 6.22.0 or newer, then this command is replaced by "role login" on page 194 .

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 SafeNet PCIe HSM modules installed, or a Backup HSM or a SafeNet USB HSM locally connected to your host. |
| -password | -p <password> | <p>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.</p> <p>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.</p> |

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.



Note: This command applies to slots with HSMs having older firmware only. If the HSM in the current slot has firmware 6.22.0 or newer, then this command is replaced by ["role logout" on page 197](#) .

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 SafeNet USB HSM or SafeNet 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.

Note: If the log file is archived (tar or tgz) it must be untarred/unzipped before **audit verify** can work on records in that log. You cannot verify a ".tgz" file directly.



The audit verify command is not able to verify a log that was in-progress when it was archived. Only logs from the ready_for_archive folder, logs that have been completed and closed, can be verified. This usually means that if you cannot verify the most recent log entry in an archive, then that same entry is probably the first log entry in the next archive, where it was properly closed and can be verified.

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
```

clientconfig

Access the clientconfig-level commands to configure your client.

Syntax

clientconfig

deleteserver
deploy
listservers
restart
verify

| Parameter | Shortcut | Description |
|---------------------|-------------|--|
| deleteserver | d | Delete SafeNet Network HSM appliance from the list (" clientconfig deleteServer " on the next page) |
| deploy | dp | Create aNetwork Trust Link. (" clientconfig deploy " on page 41) |
| listservers | ls | List the SafeNet Network HSM appliances that are registered to the client. (" clientconfig listservers " on page 42) |
| restart | rest | Restart LunaCM. (" clientconfig restart " on page 43) |
| verify | ls | Verify the SafeNet Network HSM slots / partitions that are visible from the client. (" clientconfig verify " on page 44) |

clientconfig deleteServer

Delete an existing SafeNet Network HSM server from the trusted list.

Syntax

```
clientconfig deleteServer -server <hostname>
```

Example

```
lunacm:> ccfg deleteServer -server mysa30
```

```
Server deleted mysa30
```

```
Command Result : No Error
```

```
lunacm:>
```


clientconfig deploy

Delete an existing SafeNet Network HSM server from the trusted list.

Syntax

clientconfig deploy **-server** <hostname-or-ip> **-client** <hostname-or-ip> **-partition** <partition-name> [-password <string>] [-user <string>] [-regen] [-force] [-verbose]

| Option | Shortcut | Parameter | Description |
|-------------------|-------------|------------------|--|
| -server | -n | <hostname-or-ip> | SafeNet Network HSM server hostname or IP address (mandatory). |
| -client | -c | restart | Client hostname or IP address (mandatory). |
| -partition | -par | <partition-name> | Partition name to assign to the client (mandatory). |
| -password | -pw | <string> | Appliance admin role user's password. |
| -user | -ur | <string> | Appliance admin role user's name, (default is admin). |
| -regen | -rg | . | Regenerate new and replace existing client's certificate. |
| -force | -f | . | Force the action, no prompts. |
| -verbose | -v | . | Show verbose logs. |

Example

```
lunacm:> ccfg deploy -server mysa30
```

```
Server deleted mysa30
```

```
Command Result : No Error
lunacm:>
```

clientconfig listservers

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

Syntax

clientconfig listservers

Example

```
lunacm:> clientconfig listservers
```

| Server ID | Server | Channel | HTL Required |
|-----------|-------------|---------|--------------|
| 0 | 124.54.98.2 | STC | no |
| 1 | 124.54.98.6 | NTLS | yes |

```
Command Result : No Error  
lunacm:>
```

clientconfig restart

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

Syntax

clientconfig restart

Example

```
lunacm:> ccfg rest
```

```
You are about to restart this application.  
All current login sessions and remote PED connections will be terminated.
```

```
Are you sure you wish to continue?
```

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

```
...  
<slot_list>  
...
```

```
Command Result : No Error  
lunacm:>
```

clientconfig verify

Verify SafeNet Network HSM slots / partitions that are visible.

Syntax

clientconfig verify

Example

```
lunacm:> ccfg verify
```

```
Command Result : No Error  
lunacm:>
```

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 SafeNet HSMs for redundancy and load balancing.

Syntax

hagroup

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

| Parameter | Shortcut | Description |
|----------------------|-----------|--|
| addmember | am | Add a member to an HA group. See "hagroup addmember" on page 48 . |
| addstandby | as | Add a standby member to an HA group. See "hagroup addstandby" on page 49 . |
| creategroup | c | Create an HA group. See "hagroup creategroup" on page 50 . |
| deletegroup | d | Delete an HA group . See "hagroup deletegroup" on page 51 . |
| halog | hl | Configure the HA log file. See "hagroup halog" on page 52 . |
| haonly | ho | Enable "HA Only" mode. See "hagroup haonly" on page 53 . |
| interval | i | Set the HA recover retry interval. See "hagroup interval" on page 61 |
| listgroups | l | List the currently-configured HA groups. See "hagroup listgroups" on page 54 . |
| recover | re | Recover a failed HA member. See "hagroup recover" on page 56 . |
| recoveryMode | m | Set HA recovery mode to "active" or "passive". See "hagroup recoverymode" on page 57 . |
| removemember | rm | Remove a member from an HA group. See "hagroup removemember" on page 58 . |
| removestandby | rs | Remove a standby member from an HA group. See "hagroup |

| Parameter | Shortcut | Description |
|--------------------|-----------|--|
| | | removestandby " on page 59. |
| retry | rt | Set the HA recover retry count. See " hagroup retry " on page 60 |
| synchronize | s | Synchronize an HA group. See " hagroup synchronize " on page 62 |

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 deletigroup

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

Syntax

```
hagroup deletigroup -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.



Note: This command acts on your applications, either allowing (default) or disallowing (hagroup haonly -enable) the application to see individual HSM partition slots or just the HA group virtual slot, respectively. The command has no effect on administrative tools like lunacm, where a "slot list" returns all slots, both actual and virtual.

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 If No HA Group

```
lunacm:>hagroup listgroups

      HA auto recovery:  disabled
      HA recovery mode:  activeBasic
      Maximum auto recovery retry:  0
      Auto recovery poll interval:  60 seconds
      HA logging:  disabled
      Only Show HA Slots:  no
```

Command Result : No Error

Example for HA Group

LunaCM v6.2.2-4 - Copyright (c) 2006-2016 SafeNet, Inc.

Available HSMs:

```
Slot Id -> 0
Label -> MyPartition
Serial Number -> 364882803566
Model -> LunaSA
Firmware Version -> 6.23.0
Configuration -> Luna User Partition, No SO (PW) Signing With Cloning Mode
Slot Description -> Net Token Slot
```

```
Slot Id -> 1
Label -> MyPartition
Serial Number -> 352691792984
Model -> LunaSA
Firmware Version -> 6.23.0
Configuration -> Luna User Partition, No SO (PW) Signing With Cloning Mode
Slot Description -> Net Token Slot
```

```
Slot Id -> 5
HSM Label -> myHAGroup
HSM Serial Number -> 1364882803566
HSM Model -> LunaVirtual
HSM Firmware Version -> 6.23.0
HSM Configuration -> Luna Virtual HSM (PW) Signiguration With Cloning Mode
HSM Status -> N/A - HA Group
```

Current Slot Id: 0

```
lunacm:>hagroup listgroups
```

If you would like to see synchronization data for group myHAGroup, please enter the password for the group members. Sync info not available in HA Only mode.

Enter the password: *****

```
HA auto recovery: enabled
HA recovery mode: activeBasic
Maximum auto recovery retry: infinite
Auto recovery poll interval: 65 seconds
HA logging: enabled
HA log_file: /luna_ha_temp/haErrorLog.txt
Maximum HA log file length: 300000 bytes
Only Show HA Slots: no
```

```
HA Group Label: myHAGroup
HA Group Number: 1364882803566
HA Group Slot ID: 5
Synchronization: enabled
Group Members: 364882803566, 352691792984
Needs sync: no
Standby Members: <none>
```

```
Slot #  Member S/N  Member Label  Status
=====  =====  =====  =====
0      364882803566  MyPartition  alive
1      352691792984  MyPartition  alive
```

Command Result : No Error

hagroup recover

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

Syntax

```
hagroup recover -group <label>
```

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

Example

```
lunacm:> hagroup recover -group myHAGroup
```

```
Command Result : No Error
```


hagroup recoverymode

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

Syntax

hagroup recoverymode -mode {activebasic | activeenhanced}

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

Example

```
lunacm:> hagroup recoveryMode -mode activeEnhanced
```

```
HA Auto Recovery Mode has been set to activeEnhanced mode.
```

```
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> **-slot** <slot number> [**-group**] <grouplabel>

| 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. |

Example 1

```
lunacm:> hagroup removemember -serialnumber 12345679 -group myHAGroup
```

Command Result : No Error

Example 2

```
lunacm:> hagroup removemember -slot 6 -group myHAGroup
```

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.

For HA recovery attempts:

- The default retry interval is 60 seconds.
- The default number of retries is effectively infinite.
- The HA configuration section in the Chrystoki.conf/crystoki.ini file is created and populated when either the interval or the number of retries is specified in the lunacm hagroup retry commands.

Syntax

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

| Command | Shortcut | Description |
|---------------|-----------|---|
| -count | -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 disable automatic recovery 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.

For HA recovery attempts:

- The default retry interval is 60 seconds.
- The default number of retries is effectively infinite.
- The HA configuration section in the Chrystoki.conf/crystoki.ini file is created and populated when either the interval or the number of retries is specified in the lunacm hagroup retry commands.

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. Default: 60 seconds Range: 60 to 1200 seconds |

Example

```
lunacm:> hagroup interval -i 120
```

```
Command Result : No Error
```

hagroup synchronize

Synchronize an HA group or enable/disable key synchronization for key export applications.

Syntax

```
hagroup synchronize -p <password> -group <label_or_serial-number_of_group> [-enable | -disable]
```

| Parameter | Shortcut | Description |
|------------------|-----------|---|
| -disable | -d | Disable synchronization for this HA group. This option allows you to disable synchronization on HA groups that use HSMs configured for key export (KE) to wrap asymmetric private RSA keys. In this model, you create your symmetric wrapping keys, which are synchronized to each member of the HA group. After synchronizing the symmetric wrapping keys, you disable synchronization and begin creating your asymmetric RSA keys. If one of the HA members fails, the remaining members are still able to generate and wrap asymmetric private RSA keys using the synchronized symmetric wrapping key. |
| -enable | -e | Enable synchronization for this HA group. Synchronization is enabled by default. You require this setting only if you wish to re-enable synchronization on an HA group where synchronization was previously disabled. For example, to create and synchronize a new symmetric wrapping key. |
| -group | -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$ secur3N0w
```

```
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 SafeNet PCIe HSM or SafeNet USB HSM. When lunacm is directed at a slot corresponding to a remote SafeNet Network HSM, 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 SafeNet Network HSM appliance, you must use the Luna Shell (lunash).

Syntax


hsm

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


| Parameter | Shortcut | Description |
|-----------------|----------|--|
| changehsmpolicy | changehp | Change the HSM Policy value. See " hsm changehsmpolicy " on page 66. |
| changepw | changepw | Change the HSM SO password. See " hsm changepw " on page 67. |
| changesopolicy | changesp | Change the SO Policy value. See " hsm changesopolicy " on page 68. |
| clear | clr | Delete all of the SO's token objects. See " hsm clear " on page 69. |

| Parameter | Shortcut | Description |
|------------------------|--------------|---|
| clone | clo | Clone SO objects. See "hsm clone" on page 70 . |
| contents | con | Show the contents of the SO partition. See "hsm contents" on page 71 . |
| factoryreset | f | Factory reset the HSM. See "hsm factoryreset" on page 72 . |
| init | i | Initialize the HSM. See "hsm init" on page 73 . |
| login | logi | Login to the HSM as SO. See "hsm login" on page 76 . |
| logout | logo | Logout from the HSM as SO. See "hsm logout" on page 78 . |
| migratepedkey | mig | Migrate a PED Key from a legacy HSM. See "hsm migratepedkey" on page 79 . |
| monitor | mon | Get HSM utilization information. See "hsm monitor" on page 80 . |
| recoveryinit | ri | High Availability Initialize HSM (not related to load balancing). See "hsm recoveryinit" on page 82 . |
| recoverylogin | rl | High Availability Login (not related to load balancing) . See "hsm recoverylogin" on page 83 . |
| reset | rese | Restart the HSM. See "hsm reset" on page 84 . |
| restart | rs | Restart the HSM. See "hsm restart" on page 85 . |
| restoresim2 | rsim2 | Restore SO objects (using Scalable Key Storage2). See "hsm restoresim2" on page 87 . |
| restoreuser | ru | Restore a user. See "hsm restoreuser" on page 86 . |
| rollbackfw | rb | Rollback the HSM firmware. See "hsm rollbackfw" on page 88 . |
| setlegacydomain | sld | Set the legacy domain. See "hsm setlagacydomain" on page 90 . |
| showinfo | si | Get HSM information. See "hsm showinfo" on page 91 . |
| showmechanism | showm | Show all mechanisms. See "hsm showmechanism" on page 93 . |
| showpolicies | sp | Get HSM policy information. See "hsm showpolicies" on page 95 . |
| updatecap | uc | Update the HSM capabilities. See "hsm updatecap" on page 100 . |
| updatefw | uf | Update the HSM firmware. See "hsm updatefw" on page 101 . |

Note: If the current slot is an HSM administrative slot (SO) for an HSM with firmware older than version 6.22.0, then the list of available "hsm" commands appears as:

 **init**
recoveryinit
recoverylogin
login
logout
showinfo
showpolicies
changeHSMPolicy
changeSOPolicy
changePw
contents
clear
updateFW
rollbackFW
updateCap
reset
factoryReset
restoreSIM2
restoreUser
clone
setLegacyDomain
showmechanism
monitor

Note: If the current slot is an HSM administrative slot (SO) for an HSM with firmware version 6.22.0 or newer, then the list of available "hsm" commands appears as:

 **showinfo**
factoryReset
zeroize
restart
init
showpolicies
changeHSMPolicy
updateCap
updateFW
rollbackfw
migratePedKey
showmechanism
monitor

Some options that were previously "hsm" commands have become "role" commands.

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 SafeNet PCIe HSM or SafeNet USB HSM. When lunacm is directed at a slot corresponding to a remote SafeNet Network HSM, 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 SafeNet Network HSM 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 SafeNet PCIe HSM or SafeNet USB HSM. When lunacm is directed at a slot corresponding to a remote SafeNet Network HSM, 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 SafeNet Network HSM 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$$w0rd -oldpw OldPa$$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 SafeNet PCIe HSM or SafeNet USB HSM. When lunacm is directed at a slot corresponding to a remote SafeNet Network HSM, 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 SafeNet Network HSM appliance, you must use the Luna Shell (lunash).

You can use command **hsm showpolicies** before and after command **hsm changesopolicy** to verify that the change has occurred.

If you attempt to change a destructive policy, you are warned first, and asked to confirm before proceeding, so that you can never inadvertently destroy the contents of your HSM.

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 SafeNet PCIe HSM or SafeNet USB HSM. When lunacm is directed at a slot corresponding to a remote SafeNet Network HSM, 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 SafeNet Network HSM 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 SafeNet PCIe HSM or SafeNet USB HSM. When lunacm is directed at a slot corresponding to a remote SafeNet Network HSM, 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 SafeNet Network HSM 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 SafeNet PCIe HSM or SafeNet USB HSM. When lunacm is directed at a slot corresponding to a remote SafeNet Network HSM, 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 SafeNet Network HSM 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 SafeNet PCIe HSM or SafeNet USB HSM. When lunacm is directed at a slot corresponding to a remote SafeNet Network HSM, 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 SafeNet Network HSM appliance, you must use the Luna Shell (lunash).

Syntax

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

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

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 init on SafeNet Backup HSM

```
lunacm:>hsm init -label mybackuphsm -password s0mepw -domain s0med0maln -force -auth -init-
withpwd
```

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

```
Command Result : No Error
```

```
lunacm:>hsm si
```

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

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

```
License Count -> 4  
    1. 621000028-000 SafeNet Remote Backup HSM base configuration  
    1. 621000048-001 621-000048-001SCU,G5,BU,Partitions100  
    2. 621000006-001 Enabled for 15.5 megabytes of object storage  
    2. 621000008-001 Enable remote PED capability
```

```
Command Result : No Error
```

hsm 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 SafeNet PCIe HSM or SafeNet USB HSM. When lunacm is directed at a slot corresponding to a remote SafeNet Network HSM, 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 SafeNet Network HSM appliance, you must use the Luna Shell (lunash).

Syntax

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

| Parameter | Shortcut | Description |
|-----------|----------|--|
| -password | -pa | <p>Applies to Password-authenticated HSMs; ignored for PED-authenticated HSMs.</p> <p>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.</p> |
| -ped | -pe | <p>Applies to PED-authenticated HSMs, only. This option is a temporary way to override PED ID settings or default.</p> <p>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.</p> <p>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'.</p> <p>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>".</p> |

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 SafeNet PCIe HSM or SafeNet USB HSM. When lunacm is directed at a slot corresponding to a remote SafeNet Network HSM, 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 SafeNet Network HSM 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 SafeNet PED Key (looks like a colorful toy key) to a Version 2.x SafeNet PED USB iKey. This operation requires both a version 1.14 SafeNet PED (no earlier version will work - contact SafeNet Customer Support) and a Version 2.x SafeNet 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 SafeNet PCIe HSM or SafeNet USB HSM. When lunacm is directed at a slot corresponding to a remote SafeNet Network HSM, 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 SafeNet Network HSM 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 monitor

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



Note: This command requires HSM firmware version 6.20.0 or newer. If you run the command against a slot with older firmware, expect an error CKR_FUNCTION_NOT_SUPPORTED.

Syntax

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

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

Example

Without arguments

```
lunacm:>hsm monitor
```

```
-----|-----|-----|-----|-----|-----|
          |          HSM Command Counts          |          HSM Utilization (%)          |
HSM Uptime (Secs) |-----|-----|-----|-----|-----|-----|
          | Since HSM Reset | Last   5 Secs | Since HSM Reset | Last   5 Secs |
-----|-----|-----|-----|-----|-----|
          |          1,115,399 |          57,468,854 |          30 |          1.27 |          0.21 |
-----|-----|-----|-----|-----|-----|
```

```
Average HSM Utilization In This Period : 0.21%
HSM Last Reset (+/-5 Secs Error Margin) : Fri May 31 14:59:47 2013
```

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


With arguments

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

| HSM Uptime (Secs) | HSM Command Counts | | | HSM Utilization (%) | | |
|-------------------|--------------------|------|--------|---------------------|------|--------|
| | Since HSM Reset | Last | 6 Secs | Since HSM Reset | Last | 6 Secs |
| 1,116,668 | 57,470,863 | | 1 | 1.27 | | 0.00 |
| 1,116,674 | 57,470,864 | | 1 | 1.27 | | 0.00 |
| 1,116,680 | 57,470,894 | | 30 | 1.27 | | 0.18 |
| 1,116,686 | 57,470,895 | | 1 | 1.27 | | 0.00 |
| 1,116,692 | 57,470,896 | | 1 | 1.27 | | 0.00 |
| 1,116,698 | 57,470,926 | | 30 | 1.27 | | 0.18 |

Average HSM Utilization In This Period : 0.06%

HSM Last Reset (+/-5 Secs Error Margin) : Fri May 31 14:59:46 2013

Command Result : 0 (Success)

hsm recoveryinit

Performs 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 SafeNet PCIe HSM or SafeNet USB HSM. When lunacm is directed at a slot corresponding to a remote SafeNet Network HSM, 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 SafeNet Network HSM appliance, you must use the Luna Shell (lunash).

Syntax

hsm recoverylogin

Example

```
lunacm:> hsm recoverylogin
```

```
Command Result : Success
```

hsm reset

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

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

If you are an end-user customer, using an application developed by a supplier other than SafeNet, contact that company for a resolution of the problem. They know how their application is programmed to accomplish tasks that use the SafeNet HSM, and they can determine possible workarounds or fixes. If the third-party supplier determines that there is an actual implementation fault with the HSM, 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 SafeNet PCIe HSM or SafeNet USB HSM. When lunacm is directed at a slot corresponding to a remote SafeNet Network HSM, 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 SafeNet Network HSM appliance, you must use the Luna Shell (lunash).



Note: The **hsm reset** command is available when the currently selected slot is an HSM administrative slot on a local HSM with firmware older than version 6.22.0. HSMs with firmware 6.22.0 or newer have the command **hsm restart**, instead, which is more descriptive of what the command does.

Syntax

hsm reset

Example

```
lunacm:> hsm reset
```

```
Command Result : No Error
```

hsm restart

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

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

If you are an end-user customer, using an application developed by a supplier other than SafeNet, contact that company for a resolution of the problem. They know how their application is programmed to accomplish tasks that use the SafeNet 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 SafeNet PCIe HSM or SafeNet USB HSM. When lunacm is directed at a slot corresponding to a remote SafeNet Network HSM, 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 SafeNet Network HSM appliance, you must use the Luna Shell (lunash).



Note: The **hsm reset** command is available when the currently selected slot is an HSM administrative slot on a local HSM with firmware older than version 6.22.0. HSMs with firmware 6.22.0 or newer have the command **hsm restart**, instead, which is more descriptive of what the command does.

Command **hsm reset** did not have a "proceed" option, and went directly to execution. Command **hsm restart** asks you to verify that you wish to proceed, unless you use the **-force** option.

Syntax

hsm restart [-force]

| Parameter | Shortcut | Description |
|---------------|-----------|--|
| -force | -f | Force the action (useful when scripting) |

Example

```
lunacm:> hsm restart
```

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

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

```
Command Result : No Error
```

hsm 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 SafeNet PCIe HSM or SafeNet USB HSM. When lunacm is directed at a slot corresponding to a remote SafeNet Network HSM, 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 SafeNet Network HSM 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 Scalable Key Storage2-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 SafeNet PCIe HSM or SafeNet USB HSM. When lunacm is directed at a slot corresponding to a remote SafeNet Network HSM, 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 SafeNet Network HSM 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 Scalable Key Storage 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: 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).



Note: LunaCM performs an automatic restart following a firmware rollback.



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 SafeNet PCIe HSM or SafeNet USB HSM. When lunacm is directed at a slot corresponding to a remote SafeNet Network HSM, 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 SafeNet Network HSM 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 SafeNet HSM to a release 6.x SafeNet 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 SafeNet PCI HSM or SafeNet Network HSM whose contents are to be migrated to the SafeNet 6.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 SafeNet 6.x HSM SO space.

You cannot migrate objects from a password-authenticated token/HSM to a PED authenticated SafeNet 6.x HSM, and you cannot migrate objects from a PED authenticated token/HSM to a password-authenticated SafeNet 6.x HSM.

Your target SafeNet 6.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 SafeNet 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 SafeNet PCIe HSM or SafeNet USB HSM. When lunacm is directed at a slot corresponding to a remote SafeNet Network HSM, 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 SafeNet Network HSM 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 SafeNet PCIe HSM or SafeNet USB HSM. When lunacm is directed at a slot corresponding to a remote SafeNet Network HSM, 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 SafeNet Network HSM appliance, you must use the Luna Shell (lunash).

Syntax

hsm showinfo

Example

```
lunacm:> hsm showinfo lunacm:> hsm showinfo
```

```
Partition Label -> mypcie6
Partition Manufacturer -> Safenet, Inc.
Partition Model -> K6 Base
Partition Serial Number -> 150022
Partition Status -> OK
Token Flags ->
    CKF_RESTORE_KEY_NOT_NEEDED
    CKF_PROTECTED_AUTHENTICATION_PATH
    CKF_TOKEN_INITIALIZED
RPV Initialized -> Yes
Slot Id -> 1
Tunnel Slot Id -> 2
Session State -> CKS_RW_PUBLIC_SESSION
Role Status -> none logged in
Token Flags ->
    TOKEN_KCV_CREATED
Partition OUID: 0000000000000000064a0200
```

```
Partition Storage:
    Total Storage Space: 262144
    Used Storage Space: 0
    Free Storage Space: 262144
    Object Count: 0
    Overhead: 9280
```

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

```
Firmware Version -> 6.22.0
Rollback Firmware Version -> 6.21.0
HSM Storage:
    Total Storage Space: 2097152
    Used Storage Space: 174288
    Free Storage Space: 1922864
    Allowed Partitions: 1
```

Number of Partitions: 1

License Count -> 9

1. 621000026-000 K6 base configuration
1. 620127-000 Elliptic curve cryptography
1. 620114-001 Key backup via cloning protocol
1. 620109-000 PIN entry device (PED) enabled
1. 621010358-001 Enable a split of the master tamper key to be stored externally
1. 621010089-001 Enable remote PED capability
1. 621000021-001 Performance level 15
1. 621000079-001 Enable Small Form Factor Backup
1. 621000099-001 Enable per-partition Security Officer

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 SafeNet PCIe HSM or SafeNet USB HSM. When lunacm is directed at a slot corresponding to a remote SafeNet Network HSM, 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 SafeNet Network HSM appliance, you must use the Luna Shell (lunash).

Syntax

hsm showmechanism[-m <number of a mechanism>]

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

Example of List

```
lunacm:> hsm showmechanism
```

Mechanisms Supported:

```
0x00000000 - CKM_RSA_PKCS_KEY_PAIR_GEN
0x00000001 - CKM_RSA_PKCS
0x00000003 - CKM_RSA_X_509
0x00000006 - CKM_SHA1_RSA_PKCS
0x00000009 - CKM_RSA_PKCS_OAEP
0x0000000a - CKM_RSA_X9_31_KEY_PAIR_GEN
0x0000000c - CKM_SHA1_RSA_X9_31
0x0000000d - CKM_RSA_PKCS_PSS
0x0000000e - CKM_SHA1_RSA_PKCS_PSS
0x00000010 - CKM_DSA_KEY_PAIR_GEN
0x00000011 - CKM_DSA
0x00000012 - CKM_DSA_SHA1
.
.
.
0x80000140 - CKM_DSA_SHA224
0x80000141 - CKM_DSA_SHA256
0x80000a02 - CKM_NIST_PRF_KDF
0x80000a03 - CKM_PRF_KDF
```

Command Result : No Error

Example of Information about One Mechanism

```
lunacm:> hsm showmechanism -m 8000001b

(0x8000001b - -2147483621) CKM_XOR_BASE_AND_KEY
    Min Key Size 8
    Max Key Size 4096
    Flags 0x80001
Command Result : No Error

lunacm:>
```

hsm showpolicies

Displays the HSM-level capability and policy settings for the HSM [and for the SO - deprecated; see notes below].



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 SafeNet 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 SafeNet PCIe HSM or SafeNet USB HSM. When lunacm is directed at a slot corresponding to a remote SafeNet Network HSM, 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 SafeNet Network HSM appliance, you must use the Luna Shell (lunash).



Note: The output of this command differs considerably, depending on the firmware version of the HSM in the current slot. See the examples and discussion below.

Syntax

hsm showpolicies

Examples

Example with HSM firmware older than 6.22.0

```
lunacm:>hsm sp
```

```
HSM Capabilities
 0: Enable PIN-based authentication : 1
 1: Enable PED-based authentication : 0
 2: Performance level : 15
 4: Enable domestic mechanisms & key sizes : 1
 6: Enable masking : 1
 7: Enable cloning : 1
 8: Enable special cloning certificate : 0
 9: Enable full (non-backup) functionality : 1
12: Enable non-FIPS algorithms : 1
15: Enable SO reset of partition PIN : 1
16: Enable network replication : 1
17: Enable Korean Algorithms : 0
18: FIPS evaluated : 0
19: Manufacturing Token : 0
20: Enable Remote Authentication : 1
21: Enable forcing user PIN change : 1
22: Enable offboard storage : 1
23: Enable partition groups : 0
25: Enable remote PED usage : 0
26: Enable External Storage of MTK Split : 0
```

```

27: HSM non-volatile storage space : 2097152
28: Enable HA mode CGX : 0
29: Enable Acceleration : 1
30: Enable unmasking : 0
31: Enable FW5 compatibility mode : 0
34: Enable ECIES support : 0
35: Enable Single Domain : 0
36: Enable Unified PED Key : 0
37: Enable MofN : 0
38: Enable small form factor backup/restore : 0

```

HSM Policies

```

0: PIN-based authentication : 1
1: PED-based authentication : 0
6: Allow masking : 1
7: Allow cloning : 1
12: Allow non-FIPS algorithms : 1
15: SO can reset partition PIN : 1
16: Allow network replication : 1
20: Allow Remote Authentication : 1
21: Force user PIN change after set/reset : 0
22: Allow offboard storage : 1
23: Allow partition groups : 0
25: Allow remote PED usage : 0
26: Store MTK Split Externally : 0
29: Allow Acceleration : 1
30: Allow unmasking : 0
31: Allow FW5 compatibility mode : 0
34: Allow ECIES support : 0
35: Force Single Domain : 0
36: Allow Unified PED Key : 0
37: Allow MofN : 0
38: Allow small form factor backup/restore : 0

```

SO Capabilities

```

0: Enable private key cloning : 1
1: Enable private key wrapping : 0
2: Enable private key unwrapping : 1
3: Enable private key masking : 0
4: Enable secret key cloning : 1
5: Enable secret key wrapping : 1
6: Enable secret key unwrapping : 1
7: Enable secret key masking : 0
10: Enable multipurpose keys : 1
11: Enable changing key attributes : 1
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
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
31: Enable private key unmasking : 1
32: Enable secret key unmasking : 1
33: Enable RSA PKCS mechanism : 0
34: Enable CBC-PAD (un)wrap keys of any size : 0
35: Enable private key SFF backup/restore : 0
36: Enable secret key SFF backup/restore : 0

```

SO Policies

```

0: Allow private key cloning : 1
1: Allow private key wrapping : 0
2: Allow private key unwrapping : 1
3: Allow private key masking : 0
4: Allow secret key cloning : 1
5: Allow secret key wrapping : 1
6: Allow secret key unwrapping : 1
7: Allow secret key masking : 0
10: Allow multipurpose keys : 1
11: Allow changing key attributes : 1
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
20: Max failed user logins allowed : 3
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 : 1
31: Allow private key unmasking : 1
32: Allow secret key unmasking : 1
33: Allow RSA PKCS mechanism : 0
34: Allow CBC-PAD (un)wrap keys of any size : 0
35: Allow private key SFF backup/restore : 0
36: Allow secret key SFF backup/restore : 0

```

Command Result : No Error

Example with HSM firmware 6.22.0 or newer

```

llunacm:>hsm sp
HSM Capabilities
0: Enable PIN-based authentication : 1
1: Enable PED-based authentication : 0
2: Performance level : 15
4: Enable domestic mechanisms & key sizes : 1
6: Enable masking : 1
7: Enable cloning : 1
8: Enable special cloning certificate : 0
9: Enable full (non-backup) functionality : 1
12: Enable non-FIPS algorithms : 1

```

```
15: Enable SO reset of partition PIN : 1
16: Enable network replication : 1
17: Enable Korean Algorithms : 0
18: FIPS evaluated : 0
19: Manufacturing Token : 0
20: Enable Remote Authentication : 1
21: Enable forcing user PIN change : 1
22: Enable offboard storage : 1
23: Enable partition groups : 0
25: Enable remote PED usage : 0
26: Enable External Storage of MTK Split : 0
27: HSM non-volatile storage space : 2097152
29: Enable Acceleration : 1
30: Enable unmasking : 0
31: Enable FW5 compatibility mode : 0
33: Maximum number of partitions : 20
34: Enable ECIES support : 0
35: Enable Single Domain : 1
36: Enable Unified PED Key : 1
37: Enable MofN : 1
38: Enable small form factor backup/restore : 0
39: Enable Secure Trusted Channel : 1
40: Enable decommission on tamper : 0
41: Enable Per-Partition SO : 1
42: Enable partition re-initialize : 1
```

HSM Policies

```
0: PIN-based authentication : 1
1: PED-based authentication : 0
6: Allow masking : 1
7: Allow cloning : 1
12: Allow non-FIPS algorithms : 1
15: SO can reset partition PIN : 1
16: Allow network replication : 1
20: Allow Remote Authentication : 1
21: Force user PIN change after set/reset : 0
22: Allow offboard storage : 1
23: Allow partition groups : 0
25: Allow remote PED usage : 0
26: Store MTK Split Externally : 0
29: Allow Acceleration : 1
30: Allow unmasking : 0
31: Allow FW5 compatibility mode : 0
33: Current maximum number of partitions : 20
34: Allow ECIES support : 0
35: Force Single Domain : 0
36: Allow Unified PED Key : 0
37: Allow MofN : 1
38: Allow small form factor backup/restore : 0
39: Allow Secure Trusted Channel : 0
40: Allow decommission on tamper : 0
42: Allow partition re-initialize : 0
```

Command Result : No Error

Notice that, as of HSM firmware 6.22.0, "SO Capabilities" and "SO Policies" are no longer part of the **hsm showpolicies** output. They have been moved to the output of command ["partition showpolicies" on page 171](#), when the current slot is the HSM admin partition. If the current slot is an application partition, then command **partition showpolicies** shows capabilities and policies under the control of a partition SO (for PPSO partitions) or the HSM SO (for legacy partitions).

So, for example, if you were looking for "Max failed user logins allowed", you would now look at **partition showpolicies**.

hsm updatecap

Perform an update of the HSM capabilities on the SafeNet 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 SafeNet 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 SafeNet PCIe HSM.

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

For SafeNet Network HSM, the HSM commands are available via 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 uc -cuf 621-000100-001_RC4_G5PPSO.CUF -a G5PPSO-RC6.txt
```

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

```
Are you sure you wish to continue?
```

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

```
Command Result : No Error
```



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

hsm updatefw

Update the firmware on the SafeNet HSM.



Note: LunaCM performs an automatic restart following a firmware update.



Note: The `lunacm hsm` commands appear only when the current slot selected in `lunacm` is for a locally-installed HSM, such as a SafeNet PCIe HSM or SafeNet USB HSM. When `lunacm` is directed at a slot corresponding to a remote SafeNet Network HSM, 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 SafeNet Network HSM 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 |
|------------------------|-----------------|---|
| <code>-fuf</code> | <code>-u</code> | Specifies the firmware update file. |
| <code>-authcode</code> | <code>-a</code> | Specifies the file containing the authorization code for the firmware update. |
| <code>-force</code> | <code>-f</code> | 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 partition-level commands.

Note: The partition command with no options shows the partition commands available to be used in the current slot.

The availability of partition commands changes according to four possible scenarios:

- the current slot is the HSM administrative partition for an HSM with firmware version 6.22.0 or newer



- the current slot is an application partition that has its own SO (a PPSO partition), on an HSM with firmware version 6.22.0 or newer

- the current slot is a separate-but-not-independent application partition that is administered by the HSM SO, and does not have its own separate SO (meaning, this is a legacy-style partition) on an HSM with firmware version 6.22.0 or newer

- the current slot is the HSM administrative partition and application partition for an HSM with firmware older than version 6.22.0 (meaning, this is a true legacy partition).

No single partition type has access to all the possible partition commands within lunacm.

Syntax of partition command on HSM admin partition, f/w 6.22.0

(These are the commands that you see if the current-slot partition is the initialized HSM's administrative partition, while the HSM is at firmware version 6.22.0 or newer. Some of these commands act on the current-slot partition; some have a -slot option to direct their action to another partition/slot.)

partition

archive
changeLabel
changePolicy
clear
clone
contents
create
createchallenge
delete
policyTemplateChange
policyTemplateCreate
policyTemplateDelete
policyTemplateList
policyTemplateLoad
policyTemplateSave
policyTemplateShow
resetpw
resize
restoresim3file

setlegacydomain
showinfo
showmechanism
showpolicies

| Parameter | Shortcut | Description |
|-----------------------------|------------------|---|
| archive | ar | > Partition archive management commands. See " partition archive " on page 110. |
| changeLabel | changeL | Change the Partition Label of a PPSO partition. See " partition changelabel " on page 123 |
| changePolicy | changeppo | Change the Partition Policy value. See " partition changepolicy " on page 125 |
| clear | clr | Delete all of the user's token objects. See " partition clear " on page 128. |
| clone | clo | Clone user objects. See " partition clone " on page 129. |
| contents | con | Show the contents of the application partition. See " partition contents " on page 130. |
| create | crp | Create the application partition. See " partition create " on page 131. |
| createchallenge | crc | Create the user challenge. See " partition createchallenge " on page 138. |
| delete | del | Delete an application partition. See " partition delete " on page 141. |
| policyTemplateChange | tch | Modify policy settings. See " partition policyTemplateChange " on page 160. |
| policyTemplateCreate | tcr | Create partition policy template . See " partition policyTemplatecreate " on page 162. |
| policyTemplateDelete | td | Delete partition policy template . See " partition policyTemplateDelete " on page 164. |
| policyTemplateList | tli | List partition policy templates . See " partition policyTemplateList " on page 166. |
| policyTemplateLoad | tchlo | Load partition policy template . See " partition policytempleload " on page 167. |
| policyTemplateSave | tsa | Save partition policy template . See " partition policyTemplateSave " on page 168. |
| policyTemplateShow | tsh | Show partition policy template . See " partition policyTemplateShow " on page 169. |
| resetpw | rp | Reset the partition password. See " partition resetpw " on page 148. |
| resize | res | Re-size an application partition. See " partition resize " on page 148. |

| Parameter | Shortcut | Description |
|------------------------|---------------|--|
| restoresim3 | rsim3f | Restore user objects (using Scalable Key Storage3). See " partition restoresim3 " on page 153. |
| setlegacydomain | sld | Set the legacy domain. " partition setlegacydomain " on page 154. |
| showinfo | si | Display partition information. See " partition showinfo " on page 155. |
| showmechanism | showm | Show all available mechanisms. See " partition showmechanism " on page 158. |
| showpolicies | sp | Get partition policy information. See " partition showpolicies " on page 171. |

Syntax of partition command on PPSO application partition (f/w 6.22.0 or newer)

(Same as for legacy-style partition, later on this page, except that this version of the partition command set does include an **init** command for the PPSO application partition. These are the commands that you see if the current-slot application partition was created using the "-slot" option while the HSM was at firmware version 6.22.0 or newer.)

partition

- archive
- changepolicy
- clear
- clone
- contents
- init
- restoresim3
- setlegacydomain
- showinfo
- showmechanism
- showpolicies

| Parameter | Shortcut | Description |
|---------------------|-----------------|--|
| archive | ar | > Partition archive management commands. See " partition archive " on page 110. |
| changepolicy | changepo | Change the Partition Policy value. See " partition changepolicy " on page 125 |
| clear | clr | Delete all of the user's token objects. See " partition clear " on page 128. |
| clone | clo | Clone user objects. See " partition clone " on page 129. |
| contents | con | Show the contents of the user partition. See " partition contents " on page 130. |
| init | in | Initialize an application partition. See " partition init " on page 142. |

| Parameter | Shortcut | Description |
|------------------------|--------------|--|
| restoresim3 | rsim3 | Restore user objects (using Scalable Key Storage3). See " partition restoresim3 " on page 153. |
| setlegacydomain | sld | Set the legacy domain. " partition setlegacydomain " on page 154. |
| showinfo | si | Display partition information. See " partition showinfo " on page 155. |
| showmechanism | showm | Show all available mechanisms. See " partition showmechanism " on page 158. |
| showpolicies | sp | Get partition policy information. See " partition showpolicies " on page 171. |

Syntax of partition command on legacy application partition (f/w 6.22.0 or newer)

(Same as for PPSO partition, above, except there is no partition init command for the legacy application partition. These are the commands that you see if the current-slot application partition was created using the "-label" option while the HSM was at firmware version 6.22.0 or newer.)

partition

- archive
- changepolicy
- clear
- clone
- contents
- createchallenge
- restoresim3
- setlegacydomain
- showinfo
- showmechanism
- showpolicies

| Parameter | Shortcut | Description |
|------------------------|------------------|--|
| archive | ar | > Partition archive management commands. See " partition archive " on page 110. |
| changepolicy | changeppo | Change the Partition Policy value. See " partition changepolicy " on page 125 |
| clear | clr | Delete all of the user's token objects. See " partition clear " on page 128. |
| clone | clo | Clone user objects. See " partition clone " on page 129. |
| contents | con | Show the contents of the user partition. See " partition contents " on page 130. |
| createchallenge | crc | Create the user challenge. See " partition createchallenge " on page 138. |

| Parameter | Shortcut | Description |
|------------------------|--------------|--|
| restoresim3 | rsim3 | Restore user objects (using Scalable Key Storage3). See " partition restoresim3 " on page 153. |
| setlegacydomain | sld | Set the legacy domain. " partition setlegacydomain " on page 154. |
| showinfo | si | Display partition information. See " partition showinfo " on page 155. |
| showmechanism | showm | Show all available mechanisms. See " partition showmechanism " on page 158. |
| showpolicies | sp | Get partition policy information. See " partition showpolicies " on page 171. |

Syntax of partition command on HSM admin and application partition (f/w pre-6.22.0)

(These are the commands that you see if the current-slot partition is the initialized HSM's administrative partition, while the HSM is at firmware version *older* than 6.22.0.)

partition

- archive
- changepolicy
- changepw
- clear
- clone
- contents
- create
- login
- logout
- recoveryinit
- recoverylogin
- resetpw
- restoreSIM2
- restoreSIM3
- setlegacydomain
- showinfo
- showmechanism
- showpolicies

| Parameter | Shortcut | Description |
|---------------------|------------------|---|
| archive | ar | > Partition archive management commands. See " partition archive " on page 110. |
| changepolicy | changeppo | Change the Partition Policy value. See " partition changepolicy " on page 125 |

| Parameter | Shortcut | Description |
|------------------------|-----------------|--|
| changepw | changepw | Change the partition password. See "partition changepw" on page 126 . |
| clear | clr | Delete all of the user's token objects. See "partition clear" on page 128 . |
| clone | clo | Clones user objects. See "partition clone" on page 129 . |
| contents | con | Show the contents of the user partition. See "partition contents" on page 130 . |
| create | f | Create the user partition. See "partition create" on page 131 . |
| login | logi | Login to the HSM as user. See "partition login" on page 144 . |
| logout | logo | Logout from the HSM as user. See "partition logout" on page 145 . |
| recoveryinit | ri | Setup/configure User for "Recovery Login" (formerly "HA Init", not related to load balancing). See "partition recoveryinit" on page 146 . |
| recoverylogin | rl | Login as the User using "Recovery Login" (formerly "HA Login", not related to load balancing). See "partition recoverylogin" on page 147 . |
| resetpw | resetpw | Reset the partition password. See "partition resetpw" on page 148 . |
| restoresim2 | rsim2 | Restore user objects (using Scalable Key Storage2). See "partition restoresim2" on page 152 . |
| restoresim3 | rsim3 | Restore user objects (using Scalable Key Storage3). See "partition restoresim3" on page 153 . |
| setlegacydomain | sld | Set the legacy domain. See "partition setlegacydomain" on page 154 . |
| showinfo | si | Display partition information. See "partition showinfo" on page 155 . |
| showmechanism | showm | Show all available mechanisms. See "partition showmechanism" on page 158 . |
| showpolicies | sp | Get partition policy information. See "partition showpolicies" on page 171 . |

partition activate

Cache Partition PED Key data [SafeNet PCIe HSM with PED (Trusted Path) Authentication only]. Use this command to cache 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 SafeNet PED operation (requiring the appropriate black PED Key). Partition activation makes unattended operation possible.

Partition Policy settings needed

Partition policies must be set before you can activate.

Note: Activate only

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: Activate and Autoactivate

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 or 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, no matter how brief.



Note: This partition activate command is used for "legacy" or "legacy-style" partitions, application partitions that are administratively owned by the HSM Security Officer (SO), either because the HSM firmware is older than version 6.22.0 or because the application partition has been declared without a Partition Security Officer (even though the firmware version might support PSO).

If the application partition has its own SO, then the policies must be set, as discussed above, but simply logging in as Crypto Officer or Crypto User activates the partition for client access.

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 |

| Parameter | Shortcut | Description |
|-------------|-------------|--|
| | | <p>scripting). Normally, however, you should leave out the password when issuing the command.</p> <p>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.</p> <p>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.</p> |
| -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 "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 SafeNet PCIe HSM.
- a SFF backup token (SafeNet iKey e7300) USB device connected to a SafeNet PED. The SafeNet 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.



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

Specifying the backup device

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

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

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

To specify a SFF backup (eToken 7300) inserted into a SafeNet 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 SafeNet Remote Backup HSM

When using a password-authenticated SafeNet 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 are prompted on the remote workstation console.

Device initialization

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

Appending objects to an existing backup partition

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

Remote backups

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

Syntax

partition archive

backup
contents
delete
list
restore

| 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 the next page. |
| contents | c | List the contents of a backup partition in a backup device in a specified slot. See " partition archive contents " on page 115. |
| delete | d | Delete the specified backup partition in a backup device in a specified slot. See " partition archive delete " on page 117. |
| list | l | List the backup partitions on a backup device in a specified slot. See " partition archive list " on page 119. |
| 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 120. |

partition archive backup

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



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

Syntax

partition archive backup **-slot** <slot> **-password** <password> **-partition** <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: <ul style="list-style-type: none"> <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 SafeNet PED connected to the local HSM or connected by USB to a |

| Parameter | Shortcut | Description |
|--------------------|-------------|------------------------------------|
| | | host computer running PedServer. |
| -sopassword | -sop | SO password for the backup device. |

Example

```
lunacm:> par ar b -s 7 -par P2SA2nonppsoBK
```

```
Logging in as the SO on slot 7.
```

```
Please attend to the PED.
```

```
Creating partition P2SA2nonppsoBK on slot 7.
```

```
Please attend to the PED.
```

```
Logging into the container P2SA2nonppsoBK on slot 7 as the user.
```

```
Please attend to the PED.
```

```
Creating Domain for the partition P2SA2nonppsoBK on slot 7.
```

```
Please attend to the PED.
```

```
Verifying that all objects can be backed up...
```

```
3 objects will be backed up.
```

```
Backing up objects...
```

```
Cloned object 73 to partition P2SA2nonppsoBK (new handle 16).
```

```
Cloned object 100 to partition P2SA2nonppsoBK (new handle 17).
```

```
Cloned object 99 to partition P2SA2nonppsoBK (new handle 18).
```

```
Backup Complete.
```

```
3 objects have been backed up to partition P2SA2nonppsoBK  
on slot 7.
```

```
Command Result : No Error
```

```
lunacm:>
```

Example Backup an Object to an SFF eToken

```
lunacm:>partition archive backup -s eToken -l SFFbackup -o 30
```

```
WARNING: continuing the backup operation will wipe out all keys on the backup token!  
Are you sure you wish to continue?
```

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

```
Operation in progress, please wait.
```

```
(1/1) Backing up object with handle 30... Success!
```

```
Backup Complete.
```

```
1 objects have been backed up to token with label localSFFuserPCI  
on the backup device
```

```
Command Result : No Error
```

Example: Backup All Objects to an SFF eToken

```
lunacm:>partition archive backup -s eToken -l SFFbackup
```

```
WARNING: continuing the backup operation will wipe out all keys on the backup token!  
Are you sure you wish to continue?
```

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

```
Operation in progress, please wait.
```

```
(1/5): Backing up object with handle 30... Success!  
(2/5): Backing up object with handle 26... Success!  
(3/5): Backing up object with handle 57... Success!  
(4/5): Backing up object with handle 58... Success!  
(5/5): Backing up object with handle 29... Success!
```

```
Backup Complete.
```

```
5 objects have been backed up to token with label SFFbackup  
on the backup device
```

```
Command Result : No Error
```

partition archive contents

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



Note: If you want to use this command to view the contents of an SFF token, you must be logged into an HSM partition that has the SFF capability enabled. You can be logged into any SFF-enabled partition – it is not necessary to log into the partition the backup was made against. However, SFF token and target partition must share the same cloning domain.



Note: For full, detailed enumeration of SFF token content, the objects must be decrypted and enumerated within the secure boundary of the HSM. To run **partition archive contents**, free space must be available within the target partition, equivalent to the size of the largest object on the SFF token.

Syntax

partition archive contents **-slot** <slot> **-partition** <partition_name> **-password** <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: <ul style="list-style-type: none"> • <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 SafeNet PED connected to the local HSM or connected by USB to a host computer running PedServer. |

Example: No objects

```
lunacm:>par ar c -s eToken
```

```
Listing all objects...
```

```
Found 0 backup objects:
```

```
Command Result : No Error
```

Example: Objects found

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

```
Listing all objects...
```

```
Found 5 backup objects:
```

```
Partition:      SFFbackup
Object Type:    Partition
Object UID:     6a0300004800000620420700
```

```
Label:          Generated DES3 Key
Index:          1
Object Type:    Symmetric Key
Object UID:     7a0300004800000620420700
Fingerprint:    9f63f36d7cddf5e870c8fb533d6568cc95b619141961690a76da1ac83934a18c
```

```
Label:          Created data object
Index:          2
Object Type:    Data
Object UID:     7b0300004800000620420700
Fingerprint:    ef3c747fe4bacd1d8fd6acf8a2fffd3d75c147979e92e3613b62a249f852167
```

```
Label:          Generated RSA Public Key
Index:          3
Object Type:    Public Key
Object UID:     7c0300004800000620420700
Fingerprint:    f592724ccadac362a1b220061fd6da5f6d4dbadd45c2fd87bff2b2889aed6bee
```

```
Label:          Generated RSA Private Key
Index:          4
Object Type:    Private Key
Object UID:     7d0300004800000620420700
Fingerprint:    a8ec49a3bc319e22f6772b19c2970c161078757b0d9ec78f2427232946c8e97f
```

```
Label:          Created certificate object
Index:          5
Object Type:    Certificate
Object UID:     7e0300004800000620420700
Fingerprint:    48516c4a0baf2bf2cca190ed816224f00484b73bff659441f84ef79e71a647a
```

```
Command Result : No Error
```

partition archive delete

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

Syntax

partition archive delete **-slot** <slot> **-partition** <partition name> **-password** <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 -slot 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 -slot remote is used) |
| -slot | -s | Target slot containing the backup device. It can be specified by any of the following: <ul style="list-style-type: none"> • <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, -slot 5) • etoken to specify a SFF backup (eToken 7300) inserted into a SafeNet PED connected to the local HSM or connected by USB to a host computer running PedServer. |

Example



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

```
lunacm:> slot set -s 1
Current Slot Id: 1 (Luna User Slot 6.22.0 (PW) Signing With Cloning Mode)
```

Command Result : No Error

```
lunacm:> par ar delete -slot 6 -partition JRLegacyPPSOK6 -password userpin
```

```
Logging in as the SO on slot 6.
```

```
Partition JRLegacyPPSOK6 was successfully deleted on slot 6.
```

```
Command Result : No Error
```

```
lunacm:>
```

Example: Delete all Objects from an SFF eToken

```
lunacm:>partition archive delete -slot eToken
```

```
WARNING: continuing the backup operation will wipe out all keys on the backup token!  
Are you sure you wish to continue?
```

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

```
Operation in progress, please wait.
```

```
Command Result : No Error
```

Example: Attempt to Delete Objects from an Empty SFF eToken

```
lunacm:>partition archive delete -slot eToken
```

```
WARNING: continuing the backup operation will wipe out all keys on the backup token!  
Are you sure you wish to continue?
```

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

```
Operation in progress, please wait.
```

```
Command Result : 0x20 (CKR_DATA_INVALID)
```

partition archive list

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



Note: If you want to use this command to list the partition on an SFF token, you must be logged into a partition that has the SFF capability enabled. You can be logged into any SFF-enabled partition – it is not necessary to log into the partition the backup was made against.

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: <ul style="list-style-type: none"> <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 SafeNet PED connected to the local HSM or connected by USB to a host computer running PedServer. |

Example

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

```
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> **-password** <password> **-partition** <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 -slot remote is used - this is used for a non-RBS, TCP/IP-only connection, no NTLS) |
| -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 -slot remote is used - this is used for a non-RBS, TCP/IP-only connection, no NTLS) |
| -slot | -s | Target slot containing the backup device. It can be specified by any of the following: <ul style="list-style-type: none"> <slot number>, if the backup slot is visible in the current system as an NTLS/RBS slot. 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 Backup HSM, you can specify that slot number explicitly (for example, -slot 5) etoken to specify a SFF backup (eToken 7300) inserted into a SafeNet PED connected to the local HSM or connected by USB to a host computer running PedServer. |

Example

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

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

```
    Verifying that all objects can be restored...
```

```
    1 object will be restored.
```



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

```
Restore Complete.
```

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

```
Command Result : No Error
```

Example: Restore One or All Objects from an SFF eToken

```
lunacm:>partition archive restore -slot eToken -o 1
```

```
Restoring objects...
```

```
(1/1) Restoring object 00-7a0300004800000620420700-9f63f36d7cddf5e870c8fb533d6568cc95b619141961
```

```
Command Result : No Error
```

Example: Restore All objects from an SFF eToken

```
lunacm:>partition archive restore -slot eToken
```

```
Restoring objects...
```

```
(1/5) Restoring object 00-7a0300004800000620420700-9f63f36d7cddf5e870c8fb533d6568cc95b619141961
(2/5) Restoring object 00-7b0300004800000620420700-ef3c747fe4bacd1d8fd6acf8a2fffd3d75c147979e9
(3/5) Restoring object 00-7c0300004800000620420700-f592724ccadac362a1b220061fd6da5f6d4dbadd45c2
(4/5) Restoring object 00-7d0300004800000620420700-a8ec49a3bc319e22f6772b19c2970c161078757b0d9e
(5/5) Restoring object 00-7e0300004800000620420700-48516c4a0baf2bf2cca190ed816224f00484b73bff6
```

```
Command Result : No Error
```

Example: Restore Objects from an SFF eToken, where some already exist on target

```
lunacm:>partition archive restore -slot eToken
```

```
Restoring objects...
```

```
(1/5) Restoring object 00-7a0300004800000620420700-9f63f36d7cddf5e870c8fb533d6568cc95b619141961
(2/5) Restoring object 00-7b0300004800000620420700-ef3c747fe4bacd1d8fd6acf8a2fffd3d75c147979e9
(3/5) Restoring object 00-7c0300004800000620420700-f592724ccadac362a1b220061fd6da5f6d4dbadd45c2
(4/5) Restoring object 00-7d0300004800000620420700-a8ec49a3bc319e22f6772b19c2970c161078757b0d9e
(5/5) Restoring object 00-7e0300004800000620420700-48516c4a0baf2bf2cca190ed816224f00484b73bff6
```

```
WARNING: Errors occurred during the restore process.
```

```
Command Result : 0x1 (CKR_CANCEL)
```



Note: Objects that also exist on the target HSM fail to be restored from the SFF eToken.

partition changelabel

This command can be run by the PSO, and changes the partition label on a Per-Partition SO partition (PPSO).

This command is the complement of "[partition rename](#)" on page 1 command in Luna Shell on SafeNet Network HSMs. The **partition rename** command can change the names and labels of legacy partitions on the appliance HSM, but the label for a PPSO partition is not created until that partition is initialized by the Partition SO on a connected client, in lunacm. This command gives the PSO the option to rename the partition without re-initializing.

Syntax

partition changelabel [-slot <number>] -label <string> [-force]

| Parameter | Shortcut | Description |
|---------------|-----------|--|
| -slot | -s | Slot of partition on which to change the label. Optional. If a slot is not specified, the command attempts to change the label of the partition in the current slot. |
| -label | -l | Specifies the new label for the indicated partition (PSO partitions only). Mandatory. |
| -force | -f | Force the action. Useful for scripting. |

Example

```
lunacm:>role login -n Partition SO

Please attend to the PED.

Command Result : No Error

lunacm:>par changeLabel -slot 3 -label newlbl -force

Command Result : No Error

lunacm:>par showinfo

Partition Label -> newlbl
Partition Manufacturer -> SafeNet Inc.
Partition Model -> Luna K6
Partition Serial Number -> 2328328
Partition Status -> OK
HSM Certificates -> *** Test Certs ***
HSM Part Number -> Not Available
Token Flags ->
CKF_LOGIN_REQUIRED
CKF_RESTORE_KEY_NOT_NEEDED
CKF_PROTECTED_AUTHENTICATION_PATH
CKF_TOKEN_INITIALIZED
RPV Initialized -> No
Slot Id -> 3
Session State -> CKS_RW_SO_FUNCTIONS
Role Status -> Partition SO logged in
Token Flags ->
```

TOKEN_KCV_CREATED
Partition OID: 110000001f00000001000000

Partition Storage:

Total Storage Space: 95537
Used Storage Space: 248
Free Storage Space: 95289
Object Count: 2
Overhead: 9320

*** The partition is in FIPS 140-2 approved operation mode. ***

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 change the password that authenticates the Crypto Officer or Crypto User and/or the client to the application partition. You, as User (or Crypto Officer), 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/Crypto Officer password in order to reset it.

Password authentication

For Password authenticated SafeNet 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 SafeNet HSM, the data on the black PED Key is the administrative authentication (used by the Partition Owner/User or Crypto Officer 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. The partition structure remains in place.

Syntax

partition clear [-force]

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

Example

```
lunacm:> partition clear

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

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

    2 objects were deleted.

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: <ul style="list-style-type: none"> • a single object handle • zero, to indicate that all objects are to be extracted • a list of handles, separated by commas. For example: <code>-objects 3,4,6</code> |
| -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 an application partition on a locally installed or USB-connected HSM.

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

Syntax for command in HSM with firmware 6.22.0 or newer

partition create [-password <string>] [-label <string>] [-slot <number>] [-size <number>] [-domain <string>] [-defaultdomain]][policyTemplate] <template name>] [-force]

| Parameter | Shortcut | Description |
|------------------------|-------------|--|
| -defaultdomain | -def | use default domain instead of a private, secure domain (deprecated; not recommended) |
| -domain | -d | domain for cloning (Password-auth) |
| -force | -f | force the action (useful when scripting commands) |
| -label | -l | label of the partition (declares a legacy partition - not used if "-slot" is specified) |
| -password | -p | user role password (Password-auth) |
| -policyTemplate | -tn | policy template file to apply to the partition; useful for repetitive provisioning and deployment (see "partition policytemplate" on page 1 and "Partition Creation with Policy Template Using LunaCM" on page 1) |
| -size | -si | storage size of partition (used only for HSMs supporting multiple application partitions, to specify a size other than the calculated default size - depends on HSM memory, existing application partitions, and their specifications) |
| -slot | -sl | slot where the new partition is to be created <ul style="list-style-type: none"> if "-slot" is specified, the new partition will have its own Security Officer (PSO); the PSO must initialize the partition (including assigning a label), adjust policies, initialize user roles, specify a slot number that is not already in use, usually below the number of the HSM administrative slot from which you are running the command not used if "-label" is specified |

Must delete old partition first

For HSMs with firmware 6.22.0 or newer, the partition creation does not overwrite an existing partition. If the HSM supports just a single application partition, and one already exists, the **partition create** command stops and throws the error "Error in execution : CKR_LICENSE_CAPACITY_EXCEEDED." To create a new application partition, delete the existing one first, with **partition delete**, then re-issue **partition create**.

Partition SO requires capability

The **partition create** command help shows the "-slot" option, and the "-label" option, which are mutually exclusive.

The "-label" option creates a legacy-style application partition that is "owned"/ administered by the HSM SO.

The "-slot" option attempts to create a partition with its own Security Officer (a separate entity from the HSM SO), but if your HSM does not contain the PSO Capability Update, then the attempt fails, and you can create only a legacy-style application partition.

In general, PSO partitions are advantageous for Network HSMs that support multiple application partitions, and confer no advantage for a PCIe HSM or USB HSM that support only a single application partition, locally administered.

Rules for names and passwords

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

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

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

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

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

Valid characters that can be used in a **password** or in a cloning **domain**, when entered via LunaSH [¹], are:

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

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

Invalid or problematic characters, not to be used in passwords or cloning domains are

```
"&';<>`\|()
```

Valid characters that can be used in a **password** or in a cloning **domain**, when entered via *lunacm*, are:

```
!"#$%&'\()*+,-./0123456789:;<=>?@ABCDEFGHIJKLMNPOQRSTUVWXYZ[\]^_`abcdefghijklmnopqrstuvwxyz{|}~
```

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

Minimum password length is 7 characters; maximum is 255 characters in *lunash* or *lunacm*.

Minimum domain string length is 1 character; maximum domain length is 128 characters via *lunash*. No arbitrary maximum domain string length is enforced for domain strings entered via *lunacm*, and we have successfully input domain strings longer than 1000 characters in testing.

[¹] LunaSH on the SafeNet Network HSM has a few input-character restrictions that are not present in LunaCM, run from a client host. It is unlikely that you would ever be able to access, via LunaSH, a partition that received a password or domain via LunaCM, but the conservative approach would be to avoid the few "invalid or problematic characters" generally.

Syntax for command in HSM with firmware older than 6.22.0

partition create [-password <string>] [-domain <string>] [-defaultdomain] [-force]

| Parameter | Shortcut | Description |
|-----------|----------|------------------------------------|
| -password | -p | user role password (Password-auth) |

| Parameter | Shortcut | Description |
|-----------------------|-------------|--|
| -domain | -d | domain for cloning (Password-auth) |
| -defaultdomain | -def | use default domain instead of a private, secure domain (deprecated; not recommended) |
| -force | -f | force the action (useful when scripting commands) |



Note: For HSMs with firmware older than version 6.22.0, supporting just a single application partition, **partition create** overwrites (with a warning) any pre-existing application partition.

Example creating a legacy partition (PED-auth f/w 6.22.0 or newer)

```
lunacm:> slot list
```

```

Slot Id ->          1
Tunnel Slot Id ->  2
Label ->           mypcie6
Serial Number ->   150022
Model ->           K6 Base
Firmware Version -> 6.22.0
Configuration ->   Luna HSM Admin Partition (PED) Signing With Cloning Mode
Slot Description -> Admin Token Slot
HSM Configuration -> Luna HSM Admin Partition (PED)
HSM Status ->      OK

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

```

```
Current Slot Id: 1
```

```
Command Result : No Error
```

```
lunacm:> partition create -label mypcielegacypar
```

```
Please attend to the PED.
```

```
Command Result : No Error
```

```
lunacm:> slot list
```

```

Slot Id ->          0
Tunnel Slot Id ->  2
Label ->           mypcielegacypar
Serial Number ->   349297122735
Model ->           K6 Base
Firmware Version -> 6.22.0
Configuration ->   Luna User Partition, No SO (PED) Signing With Cloning Mode

```

```

Slot Description ->      User Token Slot

Slot Id ->              1
Tunnel Slot Id ->      2
Label ->               mypcie6
Serial Number ->       150022
Model ->               K6 Base
Firmware Version ->    6.22.0
Configuration ->       Luna HSM Admin Partition (PED) Signing With Cloning Mode
Slot Description ->    Admin Token Slot
HSM Configuration ->   Luna HSM Admin Partition (PED)
HSM Status ->         OK

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

```

Current Slot Id: 1

Command Result : No Error

lunacm:>

Example creating a PPSO partition (PED-auth f/w 6.22.0 or newer)

lunacm:> slot list

```

Slot Id ->              1
Tunnel Slot Id ->      2
Label ->               mypcie6
Serial Number ->       150022
Model ->               K6 Base
Firmware Version ->    6.22.0
Configuration ->       Luna HSM Admin Partition (PED) Signing With Cloning Mode
Slot Description ->    Admin Token Slot
HSM Configuration ->   Luna HSM Admin Partition (PED)
HSM Status ->         OK

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

```

Current Slot Id: 1

Command Result : No Error

lunacm:>

lunacm:> partition create -slot 0

Command Result : No Error

lunacm:> slot list

```
Slot Id -> 0
Tunnel Slot Id -> 2
Label ->
Serial Number -> 349297122736
Model -> K6 Base
Firmware Version -> 6.22.0
Configuration -> Luna User Partition With SO (PED) Signing With Cloning Mode
Slot Description -> User Token Slot
```

```
Slot Id -> 1
Tunnel Slot Id -> 2
Label -> mypcie6
Serial Number -> 150022
Model -> K6 Base
Firmware Version -> 6.22.0
Configuration -> Luna HSM Admin Partition (PED) Signing With Cloning Mode
Slot Description -> Admin Token Slot
HSM Configuration -> Luna HSM Admin Partition (PED)
HSM Status -> OK
```

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

Current Slot Id: 1

Command Result : No Error

lunacm:>

Example creating a legacy partition (PW-auth f/w 6.10.9)

lunacm:> slot list

```
Slot Id -> 1
Tunnel Slot Id -> 2
Label -> mypcie6
Serial Number -> 150022
Model -> K6 Base
Firmware Version -> 6.22.0
Configuration -> Luna HSM Admin Partition (PED) Signing With Cloning Mode
Slot Description -> Admin Token Slot
HSM Configuration -> Luna HSM Admin Partition (PED)
HSM Status -> OK
```

```
Slot Id -> 3
HSM Label -> myG5pw
```

```
HSM Serial Number -> 7001312
HSM Model -> G5Base
HSM Firmware Version -> 6.10.4
HSM Configuration -> SafeNet USB HSM (PW) Signing With Cloning Mode
HSM Status -> OK
```

```
Current Slot Id: 1
```

```
Command Result : No Error
```

```
lunacm:>
```

```
lunacm:> partition showinfo
```

```
The User has not been created.
```

```
Command Result : No Error
```

```
lunacm:> hsm login
```

```
Option -password was not supplied. It is required.
```

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

```
Command Result : No Error
```

```
lunacm:> partition create
```

```
Option -password was not supplied. It is required.
```

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

```
Re-enter the password: *****
```

```
Option -domain was not specified. It is required.
```

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

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

```
Command Result : No Error
```

```
lunacm:> partition showinfo
```

```
HSM Serial Number -> 7001312
HSM Status -> OK
Token Flags ->
    CKF_RNG
    CKF_LOGIN_REQUIRED
    CKF_USER_PIN_INITIALIZED
    CKF_RESTORE_KEY_NOT_NEEDED
    CKF_TOKEN_INITIALIZED
RPV Initialized -> Not Available / Not Supported
Slot Id -> 3
Session State -> CKS_RW_PUBLIC_SESSION

User Status-> Not Logged In
```



```
Crypto Officer Failed Logins-> 0
Crypto User Failed Logins-> 0
User Flags ->
    CONTAINER_KCV_CREATED
User OUID: 1200000745010000e0d46a00
```

```
User Storage:
    Total Storage Space: 2094996
    Used Storage Space: 0
    Free Storage Space: 2094996
    Object Count: 0
```

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

```
License Count -> 4
    1. 621000001-000 G5 base configuration
    1. 620139-000 Elliptic curve cryptography
    1. 620131-000 Key backup via cloning protocol
    1. 621010083-001 Performance level 15
```

Command Result : No Error

lunacm:>

Note: In the examples above, for the newer firmware, **slot list**, before and after, showed that the application partition had been created.



For the older firmware, the creation of an application partition did not alter the slot list, so instead we show the output of **partition showinfo**, before the application partition is created, and then again afterward.

partition createchallenge

Create the legacy application partition's Crypto Officer challenge for a PED-authenticated SafeNet USB HSM or SafeNet PCIe HSM.

In the HSM's administrative partition, log in first, as the HSM SO.

Run the **partition createchallenge** command after you run the **partition createuser** command.

If HSM firmware is version 6.22.0 or newer, then a legacy application partition is separate from the HSM administrative partition. Run the **partition createchallenge** command from the HSM's administrative partition, specifying the slot number corresponding to the target application partition.

If HSM firmware is older than version 6.22.0, then a legacy application partition is *not* separate from the HSM administrative partition. Run the **partition createchallenge** command from the HSM's administrative partition, and do not specify a slot.

Record the 16-character text string displayed by the PED, using a text editor to avoid transcription errors that sometimes occur with handwriting.

The equivalent of this command for a PPSO partition is the **role createchallenge** command, which is run within the application partition, and which is run by the partition SO.

Syntax

partition createChallenge -slot <number> [-defchallenge]

| Parameter | Shortcut | Description |
|----------------------|------------|--|
| -slot | -sl | Slot where creating user challenge (for legacy partition) |
| -defchallenge | -d | Use Default Challenge Password . [Optional] This is intended as a convenience when provisioning or integrating. The challenge must be changed before you can perform cryptographic operations. |

Example

```
lunacm:> partition createChallenge -slot 0
```

```
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 SafeNet PCIe HSM with PED (trusted path) authentication only.

Syntax

partition deactivate

Example

```
lunacm:> partition deactivate
```

```
Command Result : No Error
```

partition delete

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

Syntax

partition resize-slot <number> [-size<number>]

| Parameter | Shortcut | Description |
|---------------|------------|---|
| -slot | -sl | Slot number of partition to be deleted. |
| -force | -f | force the action (useful for scripting) |

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

```
lunacm:> slot list

Slot Id -> 0
Tunnel Slot Id -> 2
Label -> pcieppsopar
Serial Number -> 349297122733
Model -> K6 Base
Firmware Version -> 6.22.0
Configuration -> Luna User Partition With SO (PED) Signing With Cloning Mode
Slot Description -> User Token Slot

Slot Id -> 1
Tunnel Slot Id -> 2
Label -> mypcie6
Serial Number -> 150022
Model -> K6 Base
Firmware Version -> 6.22.0
Configuration -> Luna HSM Admin Partition (PED) Signing With Cloning Mode
Slot Description -> Admin Token Slot
HSM Configuration -> Luna HSM Admin Partition (PED)
HSM Status -> OK

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

Current Slot Id: 1
```

Command Result : No Error

```
lunacm:> partition delete -slot 0
```

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

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

Command Result : No Error

```
lunacm:> slot list
```

```
Slot Id -> 1
Tunnel Slot Id -> 2
Label -> mypcie6
Serial Number -> 150022
Model -> K6 Base
Firmware Version -> 6.22.0
Configuration -> Luna HSM Admin Partition (PED) Signing With Cloning Mode
Slot Description -> Admin Token Slot
HSM Configuration -> Luna HSM Admin Partition (PED)
HSM Status -> OK
```

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

```
Current Slot Id: 1
```

Command Result : No Error

```
lunacm:>
```

partition init

Initialize an application partition. This command is used within the partition being initialized.

Syntax

```
partition init-label <string> [-password<string>] [-domain<string>] [-defaultdomain] [-auth] [-force]
```

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

Example

```
lunacm:> partition init -label pcieppsopar
```

```
You are about to initialize the partition.
All partition objects will be destroyed.
All partition roles 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
```

```
Please attend to the PED.
```

```
Command Result : No Error
```

```
lunacm:>
```

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: <ul style="list-style-type: none"> • 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.

Used with older firmware. The HSM SO must be logged in.

For firmware 6.22.0 and newer, use **role resetPW**, instead.

Syntax

partition resetPw [-password <password>]

| Parameter | Shortcut | Description |
|------------------|-----------|--|
| -password | -p | New partition password. If you do not provide it at the command line, you are prompted for it. |

Example

```
lunacm:> partition resetPw
```

```
Option -password was not supplied. It is required.
```

```
Enter the new password: *****
```

```
Re-enter the new password: *****
```

```
Command Result : No Error
```

```
lunacm:>
```

partition resize

Re-size an application partition.

You must be HSM SO, in the HSM administrative partition/slot in order to re-size an application partition. If the slot that currently has focus is an application partition, this command is not visible.

Syntax

partition **resize-slot** <number> [-**size**<number>]

| Parameter | Shortcut | Description |
|---------------|------------|---|
| -slot | -sl | Slot number of partition to be re-sized. |
| -size | -si | New storage size of target partition (bytes). |
| -force | -f | force the action (useful for scripting) |

Example of partition resize, showing before and after

The **partition showinfo** command is run from the partition/slot about which you wish to see the current information, such as, in this case, the current storage space allocated to that partition.

The **partition resize** command is run from the HSM's administrative partition.

For this example, the HSM SO has previously logged in.

```
lunacm:> slot list
```

```
Slot Id -> 0
Tunnel Slot Id -> 2
Label -> pcieppsopar
Serial Number -> 349297122733
Model -> K6 Base
Firmware Version -> 6.22.0
Configuration -> Luna User Partition With SO (PED) Signing With Cloning Mode
Slot Description -> User Token Slot
```

```
Slot Id -> 1
Tunnel Slot Id -> 2
Label -> mypcie6
Serial Number -> 150022
Model -> K6 Base
Firmware Version -> 6.22.0
Configuration -> Luna HSM Admin Partition (PED) Signing With Cloning Mode
Slot Description -> Admin Token Slot
HSM Configuration -> Luna HSM Admin Partition (PED)
HSM Status -> OK
```

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

```
Current Slot Id: 1
```

```
Command Result : No Error
```

```
lunacm:>
```

```
lunacm:> slot set slot 0
```

```
Current Slot Id: 0 (Luna User Slot 6.22.0 (PED) Signing With Cloning Mode)
```

```
Command Result : No Error
```

```
lunacm:> partition showinfo
```

```
Partition Label -> pcieppsopar
Partition Manufacturer -> Safenet, Inc.
Partition Model -> K6 Base
Partition Serial Number -> 349297122733
Partition Status -> OK
Token Flags ->
    CKF_LOGIN_REQUIRED
```

```

    CKF_RESTORE_KEY_NOT_NEEDED
    CKF_PROTECTED_AUTHENTICATION_PATH
    CKF_TOKEN_INITIALIZED
Slot Id -> 0
Tunnel Slot Id -> 2
Session State -> CKS_RW_PUBLIC_SESSION
Role Status -> none logged in
Token Flags ->
    TOKEN_KCV_CREATED
Partition OUID: 7202000072000001064a0200

```

```

Partition Storage:
  Total Storage Space: 1200000
  Used Storage Space: 0
  Free Storage Space: 1200000
  Object Count: 0
  Overhead: 9288

```

Command Result : No Error

```

lunacm:> slot set slot 1
    Current Slot Id: 1 (Luna Admin Slot 6.22.0 (PED) Signing With Cloning Mode)

```

Command Result : No Error

```

lunacm:> partition resize -slot 0 -size 1000000

```

```

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

```

```

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

```

Command Result : No Error

```

lunacm:> slot set slot 0
    Current Slot Id: 0 (Luna User Slot 6.22.0 (PED) Signing With Cloning Mode)

```

Command Result : No Error

```

lunacm:> partition showinfo

```

```

Partition Label -> pcieppsopar
Partition Manufacturer -> Safenet, Inc.
Partition Model -> K6 Base
Partition Serial Number -> 349297122733
Partition Status -> OK
Token Flags ->
    CKF_LOGIN_REQUIRED
    CKF_RESTORE_KEY_NOT_NEEDED
    CKF_PROTECTED_AUTHENTICATION_PATH
    CKF_TOKEN_INITIALIZED
Slot Id -> 0
Tunnel Slot Id -> 2
Session State -> CKS_RW_PUBLIC_SESSION
Role Status -> none logged in
Token Flags ->
    TOKEN_KCV_CREATED

```

Partition OID: 7202000072000001064a0200

Partition Storage:

| | |
|----------------------|---------|
| Total Storage Space: | 1000000 |
| Used Storage Space: | 0 |
| Free Storage Space: | 1000000 |
| Object Count: | 0 |
| Overhead: | 9288 |

Command Result : No Error

lunacm:>

partition restoresim2

Restore/insert HSM information from a Scalable Key Storage2 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 $SomePa55word
```

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 Scalable Key Storage3 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 $SomePa55word
```

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 SafeNet PCI HSM whose contents are to be migrated to the SafeNet 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 SafeNet PCI 5.x HSM partition.

Your target HSM partition has, and retains, whatever modern partition cloning domain was imprinted (on a red PED Key) when the partition was created. This command takes the domain value from your legacy HSM's red PED Key and associates that with the modern-format domain of the partition, to allow the partition to be the cloning (restore...) recipient of objects from the legacy (token) HSM.

You cannot migrate objects from a password-authenticated token/HSM to a PED-authenticated HSM partition, and you cannot migrate objects from a PED authenticated token/HSM to a Password authenticated HSM partition. Again, this is a security provision.

See "[Legacy Domains and Migration](#)" on page 1 in the *Administration Guide* 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.



Note: You can use this command repeatedly to associate different legacy domains to the current partition's cloning domain. This allows you to consolidate content from multiple legacy HSMs onto a single partition of a modern HSM.

Syntax

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

| 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 for the current slot.

The output from this command varies, depending on the type of partition in the current slot, and on the HSM firmware version.

Syntax

partition showinfo

Examples

Partition Info for an HSM admin partition (f/w 6.22.0 or newer)

```
lunacm:> partition showinfo
```

```

Partition Label -> mypcie6
Partition Manufacturer -> Safenet, Inc.
Partition Model -> K6 Base
Partition Serial Number -> 150022
Partition Status -> OK
Token Flags ->
    CKF_RESTORE_KEY_NOT_NEEDED
    CKF_PROTECTED_AUTHENTICATION_PATH
    CKF_TOKEN_INITIALIZED
Slot Id -> 1
Tunnel Slot Id -> 2
Session State -> CKS_RW_PUBLIC_SESSION
Role Status -> none logged in
Token Flags ->
    TOKEN_KCV_CREATED
Partition OUID: 0000000000000000064a0200

Partition Storage:
    Total Storage Space: 262144
    Used Storage Space: 0
    Free Storage Space: 262144
    Object Count: 0
    Overhead: 9280
Firmware Version -> 6.22.0
Rollback Firmware Version -> 6.21.0
RPV Initialized -> Yes
HSM Storage:
    Total Storage Space: 2097152
    Used Storage Space: 2097152
    Free Storage Space: 0
    Allowed Partitions: 1
    Number of Partitions: 1

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

License Count -> 9
    1. 621000026-000 K6 base configuration
    1. 620127-000 Elliptic curve cryptography
    1. 620114-001 Key backup via cloning protocol

```

1. 620109-000 PIN entry device (PED) enabled
1. 621010358-001 Enable a split of the master tamper key to be stored externally
1. 621010089-001 Enable remote PED capability
1. 621000021-001 Performance level 15
1. 621000079-001 Enable Small Form Factor Backup
1. 621000099-001 Enable per-partition Security Officer

Command Result : No Error

Partition Info for a PPSO application partition (f/w 6.22.0 or newer)

lunacm:> partition showinfo

```

Partition Label -> mypciepsopar
Partition Manufacturer -> Safenet, Inc.
Partition Model -> K6 Base
Partition Serial Number -> 349297122736
Partition Status -> OK
Token Flags ->
    CKF_LOGIN_REQUIRED
    CKF_RESTORE_KEY_NOT_NEEDED
    CKF_PROTECTED_AUTHENTICATION_PATH
    CKF_TOKEN_INITIALIZED
Slot Id -> 0
Tunnel Slot Id -> 2
Session State -> CKS_RW_PUBLIC_SESSION
Role Status -> none logged in
Token Flags ->
    TOKEN_KCV_CREATED
Partition OID: 6d02000074000001064a0200

Partition Storage:
    Total Storage Space: 2087864
    Used Storage Space: 0
    Free Storage Space: 2087864
    Object Count: 0
    Overhead: 9288

```

Command Result : No Error

Partition Info for a Legacy application partition (f/w older than 6.22.0)

lunacm:> partition showinfo

```

HSM Serial Number -> 7001312
HSM Status -> OK
Token Flags ->
    CKF_RNG
    CKF_LOGIN_REQUIRED
    CKF_USER_PIN_INITIALIZED
    CKF_RESTORE_KEY_NOT_NEEDED
    CKF_TOKEN_INITIALIZED
RPV Initialized -> Not Available / Not Supported
Slot Id -> 3
Session State -> CKS_RW_PUBLIC_SESSION

```

User Status-> Not Logged In

Crypto Officer Failed Logins-> 0

Crypto User Failed Logins-> 0

User Flags ->

CONTAINER_KCV_CREATED

User OID: 1200000745010000e0d46a00

User Storage:

Total Storage Space: 2094996

Used Storage Space: 3116

Free Storage Space: 2091880

Object Count: 2

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

License Count -> 4

1. 621000001-000 G5 base configuration

1. 620139-000 Elliptic curve cryptography

1. 620131-000 Key backup via cloning protocol

1. 621010083-001 Performance level 15

Command Result : No Error

partition showmechanism

Lists the supported mechanisms, or shows some detail about a named mechanism.

Syntax

partition showmechanism [-m <number_of_mechanism>]

| Option | Short | Description |
|----------------|-------|--|
| [no arguments] | . | Lists all available mechanisms. |
| -m | -m | Shows expanded information for the indicated mechanism (optional). |

Example

List all mechanisms available to the partition

```
lunacm:> partition showmechanism
```

```
Mechanisms Supported:
```

```

0x00000000 - CKM_RSA_PKCS_KEY_PAIR_GEN
0x00000001 - CKM_RSA_PKCS
0x00000003 - CKM_RSA_X_509
0x00000006 - CKM_SHA1_RSA_PKCS
0x00000009 - CKM_RSA_PKCS_OAEP
0x0000000a - CKM_RSA_X9_31_KEY_PAIR_GEN
0x80000142 - CKM_RSA_FIPS_186_3_AUX_PRIME_KEY_PAIR_GEN
0x80000143 - CKM_RSA_FIPS_186_3_PRIME_KEY_PAIR_GEN
0x0000000b - CKM_RSA_X9_31
0x0000000c - CKM_SHA1_RSA_X9_31
0x80000135 - CKM_SHA224_RSA_X9_31
0x80000136 - CKM_SHA256_RSA_X9_31
0x80000137 - CKM_SHA384_RSA_X9_31
0x80000138 - CKM_SHA512_RSA_X9_31
0x8000013e - CKM_RSA_X9_31_NON_FIPS
0x80000139 - CKM_SHA1_RSA_X9_31_NON_FIPS
0x8000013a - CKM_SHA224_RSA_X9_31_NON_FIPS
0x8000013b - CKM_SHA256_RSA_X9_31_NON_FIPS
0x8000013c - CKM_SHA384_RSA_X9_31_NON_FIPS
0x8000013d - CKM_SHA512_RSA_X9_31_NON_FIPS
0x0000000d - CKM_RSA_PKCS_PSS
0x0000000e - CKM_SHA1_RSA_PKCS_PSS
:
:
0x00000365 - CKM_EXTRACT_KEY_FROM_KEY
0x00000391 - CKM_MD2_KEY_DERIVATION
0x00000390 - CKM_MD5_KEY_DERIVATION
0x00000392 - CKM_SHA1_KEY_DERIVATION
0x00000350 - CKM_GENERIC_SECRET_KEY_GEN
0x00000371 - CKM_SSL3_MASTER_KEY_DERIVE
0x00000372 - CKM_SSL3_KEY_AND_MAC_DERIVE
0x00000380 - CKM_SSL3_MD5_MAC
0x00000381 - CKM_SSL3_SHA1_MAC

```

```
0x00000221 - CKM_SHA_1_HMAC
0x00000222 - CKM_SHA_1_HMAC_GENERAL
0x00000211 - CKM_MD5_HMAC
0x00000212 - CKM_MD5_HMAC_GENERAL
0x00000370 - CKM_SSL3_PRE_MASTER_KEY_GEN
0x80000140 - CKM_DSA_SHA224
0x80000141 - CKM_DSA_SHA256
0x80000a02 - CKM_NIST_PRF_KDF
0x80000a03 - CKM_PRF_KDF
```

Command Result : No Error

Show information about a particular mechanism

```
lunacm:> partition showmechanism -m 80000142
```

```
(0x80000142 - -2147483326) CKM_RSA_FIPS_186_3_AUX_PRIME_KEY_PAIR_GEN
  Min Key Size 1024
  Max Key Size 3072
  Flags 0x10001
```

Command Result : No Error

partition policyTemplateChange

Modify a policy's initial value and destructive settings within the partition policy template currently being edited. This change is done independently of any partition when the edit is performed. The change becomes accessible when the template is saved. The change becomes active if the template is applied to an application partition.

Syntax

```
partition policyTemplateChange -policy <polycynumber> [-value <value> ] [-on{destructive | non-destructive}] [-off
{destructive | non-destructive}]
```

| Option | Shortcut | Parameter | Description |
|----------------|-------------|-----------------|---|
| -off | -off | . | Specifies whether the action of switching the policy <i>off</i> shall be destructive. |
| -on | -on | . | Specifies whether the action of switching the policy <i>on</i> shall be destructive. |
| -policy | -p | <policy number> | Specifies the policy code identifying the policy to alter. Policy descriptions and codes are obtained with the partition showpolicies command. |
| -value | -v | <policy value> | Specifies the value that should be assigned to the specified policy. When specifying values for an on/off type policy, use '1' for on and '0' for off, or just type the text "on" or "off". Either is acceptable. |

Example

```
lunacm:> partition policyTemplateChange -policy 23 -value on
```

| Code | Description | Destructive | | |
|------|-----------------------|-------------|-----------|-----------|
| | | Value | Off-To-On | On-To-Off |
| 23 | Allow auto-activation | On | No | No |

```
Command Result : No Error
```

```
lunacm:> partition policyTemplateChange -policy 25 -value 246
```

| Code | Description | Destructive | | |
|------|--|-------------|-----------|-----------|
| | | Value | Off-To-On | On-To-Off |
| 25 | Minimum pin length (inverted: 255 - min) | 246 | N/A | N/A |

```
Command Result : No Error
```

```
lunacm:> partition policyTemplateChange -policy 20 -value 9
```

| Code | Description | Destructive | | |
|------|--------------------------------|-------------|-----------|-----------|
| | | Value | Off-To-On | On-To-Off |
| 20 | Max failed user logins allowed | 9 | N/A | N/A |

Command Result : No Error

```
lunacm:> partition policyTemplateChange -policy 7 -on non-destructive
```

| Code | Description | Destructive | | |
|------|--------------------------|-------------|-----------|-----------|
| | | Value | Off-To-On | On-To-Off |
| 7 | Allow secret key masking | Off | No | No |

Command Result : No Error

partition policyTemplatecreate

Create an application partition policy template in memory (for editing). To preserve the template, it must be saved separately by the **partition policyTemplatesave** command.

Partition policy template naming

A policy template must have a unique name, which can be a character string.

Acceptable characters are:

-.0123456789ABCDEFGHIJKLMNOPQRSTUVWXYZ_abcdefghijklmnopqrstuvwxy

Minimum length is a single character.

Maximum length is 20 characters.

Syntax

partition create -policyTemplateCreate[-force]

| Option | Shortcut | Parameter | Description |
|---------------|-----------|-----------|--|
| -force | -f | . | Force the partition creation with no prompting - you are still prompted by SafeNet PED, if yours is a PED authenticated HSM. |

Example

```
lunacm:> partition policytemplatecreate
```

| Code | Description | Destructive | | |
|------|--|-------------|-----------|-----------|
| | | Value | Off-To-On | On-To-Off |
| 0 | Allow private key cloning | On | Yes | No |
| 1 | Allow private key wrapping | Off | Yes | No |
| 2 | Allow private key unwrapping | On | No | No |
| 3 | Allow private key masking | Off | Yes | No |
| 4 | Allow secret key cloning | On | Yes | No |
| 5 | Allow secret key wrapping | On | Yes | No |
| 6 | Allow secret key unwrapping | On | No | No |
| 7 | Allow secret key masking | Off | Yes | No |
| 10 | Allow multipurpose keys | On | Yes | No |
| 11 | Allow changing key attributes | On | Yes | No |
| 15 | Ignore failed challenge responses | On | Yes | No |
| 16 | Operate without RSA blinding | On | Yes | No |
| 17 | Allow signing with non-local keys | On | No | No |
| 18 | Allow raw RSA operations | On | Yes | No |
| 20 | Max failed user logins allowed | 10 | N/A | N/A |
| 21 | Allow high availability recovery | On | No | No |
| 22 | Allow activation | On | No | No |
| 23 | Allow auto-activation | On | No | No |
| 24 | Allow indirect login | Off | No | No |
| 25 | Minimum pin length (inverted: 255 - min) | 248 | N/A | N/A |
| 26 | Maximum pin length | 255 | N/A | N/A |

| | | | | |
|----|--|-----|-----|-----|
| 28 | Allow Key Management Functions | On | Yes | No |
| 29 | Perform RSA signing without confirmation | On | Yes | No |
| 30 | Allow Remote Authentication | On | No | No |
| 31 | Allow private key unmasking | On | No | No |
| 32 | Allow secret key unmasking | On | No | No |
| 33 | Allow RSA PKCS mechanism | On | Yes | No |
| 34 | Allow CBC-PAD (un)wrap keys of any size | On | Yes | No |
| 35 | Allow private key SFF backup/restore | Off | Yes | No |
| 36 | Allow secret key SFF backup/restore | Off | Yes | No |
| 37 | Force Secure Trusted Channel | Off | No | Yes |

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

Success: Created and loaded the new partition policy template.

Use 'partition policyTemplateChange' to edit the template and 'partition policyTemplateSave' to save the template once you have applied all necessary changes.

Command Result : No Error

partition policyTemplateDelete

Delete partition policy template.

Syntax

partition policyTemplateDelete [-all] [-name<template-name>] [-force]

| Option | Shortcut | Parameter | Description |
|---------------|-----------|-----------------|---|
| -all | -a | . | Delete all templates |
| -name | -n | <template name> | Specifies the name of the application partition policy template to delete. Application partition policy template names are obtained with the partition policyTemplate -list command. |
| -force | -f | . | Force the option. Useful for scripting. |

Example

```
lunacm:> slot set slot 1
```

```
Current Slot Id: 1 (Luna Admin Slot 6.24.0 (PED) Signing With Cloning Mode)
```

```
Command Result : No Error
```

```
lunacm:> partition policyTemplateList
```

```
Name Description
```

```
Sample02 Another template
sample01
```

```
No partition policy template is currently loaded.
```

```
Command Result : No Error
```

```
lunacm:> partition policyTemplateDelete -name sample01
```

```
Are you sure you wish to delete partition policy template: sample01
```

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

```
Success: Deleted partition policy template: sample01
```

```
Command Result : No Error
```

```
lunacm:> slot set slot 1
```

```
Current Slot Id: 1 (Luna Admin Slot 6.24.0 (PED) Signing With Cloning Mode)
```

```
Command Result : No Error
```

```
lunacm:> partition policyTemplateList
```

| Name | Description |
|------|-------------|
|------|-------------|

| | |
|----------|------------------|
| Sample02 | Another template |
|----------|------------------|

No partition policy template is currently loaded.

Command Result : No Error

partition policyTemplateList

List the partition policies templates created by the HSM administrator and which template is currently being modified.

Syntax

partition policyTemplateList

Example

```
lunacm:> slot set slot 1
```

```
Current Slot Id: 1 (Luna Admin Slot 6.24.0 (PED) Signing With Cloning Mode)
```

```
Command Result : No Error
```

```
lunacm:> partition policyTemplateList
```

| Name | Description |
|----------|------------------------------------|
| Sample02 | Another template |
| sample01 | My first partition policy template |

```
No partition policy template is currently loaded.
```

```
Command Result : No Error
```

Each row represents a template. The first column is the template name. Each template name is unique and is specified by the user when creating the template. The second column is a description (provided by the creator of the template) for each template. You are also reminded if a partition policy template is currently loaded for modification.

partition policytempleload

Load a partition policy template for modification

Syntax

partition policyTemplateLoad -name<template-name> [**-force**]

| Option | Shortcut | Parameter | Description |
|---------------|-----------|-----------------|--|
| -name | -n | <template name> | Specifies the name of the application partition policy template to load, for editing/altering policies. Application partition policy template names are obtained with the partition policyTemplateList command. |
| -force | -f | . | Force the option. Useful for scripting. |

Example

```
lunacm:> partition policyTemplateLoad -name Sample02
```

```
Success: Loaded Sample02 partition policy template for editing.
```

```
Command Result : No Error
```

partition policyTemplateSave

Save the partition policy template modifications. This command saves a newly created partition policy template from editing memory, or saves a previously created partition policy template that was loaded for editing and re-saving.

Syntax

partition policyTemplateSave [-name<template-name>] [-description<string>] [-force]

| Option | Shortcut | Parameter | Description |
|---------------------|-----------|-----------------|---|
| -name | -n | <template name> | Specifies the name of the HSM Partition on which to alter policies. HSM Partition names are obtained with the partition -list command. |
| -description | -d | <string> | An identifying comment for your own reference, when managing application partition policy templates. |
| -force | -f | . | Force the option. Useful for scripting. |

Example

```
lunacm:> partition policyTemplateSave
```

```
    Saving the modified settings will overwrite the existing template "Sample02".
```

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

```
Success: Sample02 saved.
```

```
Command Result : No Error
```


partition policyTemplateShow

Display the destructiveness and value of each policy from the specified partition policy template name.

Syntax

partition policyTemplateShow [-name <template_name>]

| Option | Shortcut | Parameter | Description |
|--------------|-----------|-----------------|--|
| -name | -n | <template_name> | Specifies the name of the template for which to display information. If no template is named, the command shows the template that is currently loaded for editing, or tells you that no template is being modified. |

Example

```
lunacm:> partition policyTemplateShow -name Sample02
```

| Code | Description | Destructive | | |
|------|--|-------------|-----------|-----------|
| | | Value | Off-To-On | On-To-Off |
| 0 | Allow private key cloning | On | Yes | No |
| 1 | Allow private key wrapping | Off | Yes | No |
| 2 | Allow private key unwrapping | On | No | No |
| 3 | Allow private key masking | Off | Yes | No |
| 4 | Allow secret key cloning | On | Yes | No |
| 5 | Allow secret key wrapping | On | Yes | No |
| 6 | Allow secret key unwrapping | On | No | No |
| 7 | Allow secret key masking | Off | Yes | No |
| 10 | Allow multipurpose keys | On | Yes | No |
| 11 | Allow changing key attributes | On | Yes | No |
| 15 | Ignore failed challenge responses | On | Yes | No |
| 16 | Operate without RSA blinding | On | Yes | No |
| 17 | Allow signing with non-local keys | On | No | No |
| 18 | Allow raw RSA operations | On | Yes | No |
| 20 | Max failed user logins allowed | 10 | N/A | N/A |
| 21 | Allow high availability recovery | On | No | No |
| 22 | Allow activation | On | No | No |
| 23 | Allow auto-activation | On | No | No |
| 24 | Allow indirect login | Off | No | No |
| 25 | Minimum pin length (inverted: 255 - min) | 248 | N/A | N/A |
| 26 | Maximum pin length | 255 | N/A | N/A |
| 28 | Allow Key Management Functions | On | Yes | No |
| 29 | Perform RSA signing without confirmation | On | Yes | No |
| 30 | Allow Remote Authentication | On | No | No |
| 31 | Allow private key unmasking | On | No | No |
| 32 | Allow secret key unmasking | On | No | No |
| 33 | Allow RSA PKCS mechanism | On | Yes | No |
| 34 | Allow CBC-PAD (un)wrap keys of any size | On | Yes | No |
| 35 | Allow private key SFF backup/restore | On | Yes | No |
| 36 | Allow secret key SFF backup/restore | On | Yes | No |

| | | | | |
|----|------------------------------|-----|----|-----|
| 37 | Force Secure Trusted Channel | Off | No | Yes |
|----|------------------------------|-----|----|-----|

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 Scalable Key Storage 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 $some-Pa55word
```

Command Result : No Error

ped

Access the Remote-PED configuration commands. These commands manage the use of Remote PED with your SafeNet 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](#)" on page 1 in the *Administration Guide* for more information.

Syntax

ped

connect
disconnect
get
set
show
vector

| Parameter | Shortcut | Description |
|-------------------|-----------|---|
| connect | c | Connect to the remote PED. See " ped connect " on the next page. |
| disconnect | d | Disconnect from the remote PED. See " ped disconnect " on page 177. |
| get | g | Show the PED ID and the listening slot ID. See " ped get " on page 178. |
| set | se | Set the PED ID. See " ped set " on page 179. |
| show | sh | Display the remote PED server configuration. See " ped show " on page 181. |
| vector | v | Initialize or delete the remote PED vector. See " ped vector " on page 182. |

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 179 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 specify 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 192.20.10.155
```

```
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 : 192.20.9.77/192.168.255.223
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 175 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 show

Display information for the current HSM PED connection.

Syntax

ped show

Example

```
lunacm:> ped show
```

```
Ped Client Version 1.0.5 (10005)  
Ped Client launched in status mode.  
Ped PedClient is not currently running.
```

```
Show command passed.
```

```
Command Result : No Error
```

ped vector

Create or delete a Remote PED Vector (RPV) on the HSM in the current slot. Use this command to do the following:

- create a Remote PED Vector (RPV) and imprint it onto the HSM and an orange PED Key (RPK), or optionally allow the HSM to accept an RPV that already exists on an orange PED Key (this allows your HSMs to share a common RPV, if desired).
- 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 SafeNet Remote Backup HSM must be connected to that computer and the SafeNet HSM client software must be installed, including the library and the Backup HSM driver. Use the **slot -set -slot <number>** command to set the backup HSM as the current slot for use by the remote backup server.



Note: This feature is not currently supported for use with IPv6 networks.

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
```

role

Perform administrative commands related to HSM and partition roles - list roles, log in and log out, initialize a role on a partition, create a challenge secret, change or reset password for a role, etc. This command set is available when the currently selected slot points to a partition on an HSM with firmware 6.22.0 or newer.

Syntax

role

changepw
createchallenge
deactivate
init
list
login
logout
recoveryinit
recoverylogin
resetpw
setdomain
show

| Parameter | Shortcut | Description |
|------------------------|--------------|---|
| changepw | cp | Change password (see "role changepw" on the next page) |
| createchallenge | cc | Challenge create (see "role createChallenge" on page 188) |
| deactivate | deact | Deactivate role (see "role deactivate" on page 189) |
| init | in | Initialize a role on the partition (see "role init" on page 190) |
| list | li | List roles on the partition (see "role list" on page 192) |
| login | logi | Role login (see "role login" on page 194) |
| logout | logo | Role logout (see "role logout" on page 197) |
| recoveryinit | ri | Setup/configure for "Recovery Login" (see "role recoveryinit" on page 198) |
| recoverylogin | rl | Login using "Recovery Login" (see "role recoverylogin" on page 199) |
| resetpw | r | Reset password (see "role resetpw" on page 200) |
| setdomain | d | Set the domain for a role (see "role setdomain" on page 201) |
| show | s | Show state of a role (see "role show" on page 203) |

role changepw

Change the password for a specified role.

Syntax

```
role changePW -name <string> [-oldpw <string>] [-newpw <string>] [-prompt] [-force]
```

| Parameter | Shortcut | Description |
|----------------|-------------|--|
| -name | -n | role to change password for |
| -oldpw | -old | <p>Current password (for application partition on PW authenticated HSM) or current challenge secret (for application partition on PED authenticated HSM).</p> <p>If you include option "-oldpw" the HSM assumes that you wish to change the challenge secret, which is the "secondary credential". This applies to Crypto Officer and Crypto User, which each have primary and secondary credentials, but not to Partition SO, which has only primary credential.</p> <p>If you omit option "-oldpw" the HSM assumes that you wish to change the "primary credential" or PED Key secret.</p> <p>Required if you wish to change the secondary credential.</p> |
| -newpw | -new | <p>New password (for application partition on PW authenticated HSM) or new challenge secret (for application partition on PED authenticated HSM).</p> <p>Required if you have already provided an "-oldpw".</p> |
| -prompt | -p | prompt for challenges (challenges will be hidden by *) |
| -force | -f | Force the action. Use this option to bypass the warning about primary/secondary credentials on a PED-authenticated HSM, as shown in the example. |

Examples

Change credential on the HSM's Admin partition

```
lunacm:> role changePW -name Administrator -prompt
```

```
    A role must be logged in to change password.
```

```
Error in execution: command cancelled.
```

```
Command Result : 0xb (User Cancelled Operation)
```

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

```
    Please attend to the PED.
```

Command Result : No Error

```
lunacm:> role changePW -name SO -prompt
```

```
Warning: this role has no secondary credentials.  
-prompt parameter will be ignored.
```

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

```
Please attend to the PED.
```

Command Result : No Error

Change Crypto Officer's secondary credential (challenge secret)

With prompting (no -force)

```
lunacm:> role changepw -oldpw PASSWORD -newpw userpin -name Crypto Officer
```

```
This role has secondary credentials.  
You are about to change the secondary credentials.  
Are you sure you wish to continue?
```

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

Command Result : No Error

Using the -force option

```
lunacm:> role changepw -oldpw PASSWORD -newpw userpin2 -name Crypto Officer -force
```

Command Result : No Error

Change the Crypto Officer's primary credential (PED Key secret)

```
lunacm:> role changepw -name Crypto Officer
```

```
This role has secondary credentials.  
You are about to change the primary credentials.  
Are you sure you wish to continue?
```

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

Command Result : No Error

Attempt to change a role's credential when a different role is logged in

```
lunacm:> role changepw -name Crypto Officer -oldpw 6Ks5bTs3PxPMWqPP -newpw 5parE puppy
```

A role must be logged in to change password.

Error in execution: command cancelled.

Command Result : 0xb (User Cancelled Operation)

```
lunacm:> role login -name Crypto Officer
```

```
enter password: *****
```

```
Please attend to the PED.
```

Error in execution: CKR_USER_ALREADY_LOGGED_IN.

Command Result : 0x100 (CKR_USER_ALREADY_LOGGED_IN)

```
lunacm:> role logout
```

Command Result : No Error

```
lunacm:> role login -name Crypto Officer
```

```
enter password: *****
```

Command Result : No Error

```
lunacm:> role changepw -name Crypto Officer -oldpw 6Ks5bTs3PxPMWqPP -newpw 5parEpuppy
```

```
This role has secondary credentials.  
You are about to change the secondary credentials.  
Are you sure you wish to continue?
```

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

Command Result : No Error

role createChallenge

Creates a challenge secret for a role - either Crypto Officer or Crypto User - for a PPSO partition. The challenge is a text-string secret used by an application to access the application partition with either Crypto Officer or Crypto User access level, respectively.



Note: Creating a challenge is optional, and applies only to PED-authenticated SafeNet HSMs. Role activation (caching of the black or gray PED Key credential following Crypto Officer or Crypto User login) is permitted only if a challenge secret has been created for the role, and the Allow Activation policy is set for the partition.

- The application partition must be the current slot.
- For firmware 6.22.0 (or newer), in a PPSO partition, this command is used by the Partition SO, who must be logged in, to create a challenge for the Crypto Officer.
Or, this command is used by the Crypto Officer, who must be logged in, to create a challenge for the Crypto User.

Both the role initiating the command and the target role must exist on the same application partition, and the initiating role must be logged in, at the current slot; therefore, no "-slot" parameter is needed.

- For a legacy partition, the Crypto Officer challenge is created by the HSM SO, while logged into the HSM administrative partition, and therefore the **partition createchallenge** command is used instead (see "[partition createchallenge](#)" on page 138).
- Before you can use the **role createChallenge** command, the target role must already exist. See "[role init](#)" on page 190.
- When the current slot is an HSM with firmware older than version 6.22.0, lunacm supports the commands you have always used, and does not make available the role commands, nor any newer parameters and options for other commands.

Syntax

command -name <string> [-defchallenge]

| Parameter | Shortcut | Description |
|----------------------|-----------|--|
| -name | -n | name of role for which the challenge is to be created |
| -defchallenge | -d | Use Default Challenge Password . [Optional] This is intended as a convenience when provisioning or integrating. The challenge must be changed before you can perform cryptographic operations. |

Example

```
lunacm:> role createChallenge -name Crypto Officer
```

```
    Please attend to the PED.
```

```
Command Result : No Error
```

```
lunacm:>
```

role deactivate

Deactivates a role on a partition.

If the "Allow activation" policy is set, then activation/re-activation happens with login.

Syntax

role deactivate -name <string>

| Parameter | Shortcut | Description |
|--------------|-----------|--------------------------------|
| -name | -n | name of role to be deactivated |

Example

example

role init

Initializes (creates) the named role on the current partition / slot, if applicable.

Use the command "[role list](#)" on page 192 to see which roles are possible on the current partition/slot.

Syntax

role init -name <string> [-password <string>]

| Parameter | Shortcut | Description |
|-----------|----------|--------------------------------|
| -name | -n | name of role to be initialized |
| -password | -p | password for role |

Example1

```
lunacm:> role init -name Crypto Officer
```

```
    Please attend to the PED.
```

```
Command Result : No Error
```

```
lunacm:>
```

Example2

```
lunacm:> role init -name Auditor
```

```
    Please attend to the PED.
```

```
Command Result : No Error
```

```
lunacm:>
```



Note: The Auditor role can exist only on the HSM's administrative partition, and shares that partition with the HSM Security Officer or SO (firmware 6.22.0 and newer). The Auditor role cannot be initialized by another role. Therefore, if the HSM SO is currently logged in, the SO must log out before you run **role init** to create the Auditor.



Note: When the Auditor role is created, it has no domain set. To allow Auditor to clone, you must log in as Auditor and run the command **role setDomain**. See "[role setdomain](#)" on page 201.



Note: This command is used for HSMs with firmware version 6.22.0 or newer. Expect an entry like 'LUNA_INIT_PIN returned RC_OK(0x00000000) roleID=8 container=3 'in the audit log, when the Auditor role is initialized. To initialize audit logging for HSMs with older firmware, use ["audit init" on page 32](#).

role list

List the roles available on the current partition/slot.

Syntax

role list

Example

LunaCM v6.0.0 - Copyright (c) 2006-2015 SafeNet, Inc.

Available HSMs:

```
Slot Id -> 0
Tunnel Slot Id -> 2
Label -> mypciepsopar
Serial Number -> 349297122736
Model -> K6 Base
Firmware Version -> 6.22.0
Configuration -> Luna User Partition With SO (PED) Signing With Cloning Mode
Slot Description -> User Token Slot
```

```
Slot Id -> 1
Tunnel Slot Id -> 2
Label -> mypcie6
Serial Number -> 150022
Model -> K6 Base
Firmware Version -> 6.22.0
Configuration -> Luna HSM Admin Partition (PED) Signing With Cloning Mode
Slot Description -> Admin Token Slot
HSM Configuration -> Luna HSM Admin Partition (PED)
HSM Status -> OK
```

```
Slot Id -> 3
HSM Label -> myG5
HSM Serial Number -> 7001312
HSM Model -> G5Base
HSM Firmware Version -> 6.10.4
HSM Configuration -> SafeNet USB HSM (PED) Signing With Cloning Mode
HSM Status -> OK
```

Current Slot Id: 0

```
lunacm:> role list
```

```
Roles
=====
Partition SO
Crypto Officer
Crypto User
```

Command Result : No Error


```
lunacm:> slot set slot 1
```

```
Current Slot Id: 1 (Luna Admin Slot 6.22.0 (PED) Signing With Cloning Mode)
```

```
Command Result : No Error
```

```
lunacm:> role list
```

```
Roles
=====
SO
Admin User
Auditor
```

```
Command Result : No Error
```

Change to a slot with older firmware, and the role commands are not available

```
lunacm:> slot set slot 3
```

```
Current Slot Id: 3 (SafeNet USB HSM 6.10.1 (PED) Signing With Cloning Mode)
```

```
Command Result : No Error
```

```
lunacm:> role list
```

```
Valid Commands:
```

```
The following commands are available:
```

| Command | Short | Description |
|--------------|-------|----------------------------------|
| exit | e | exits this utility |
| help | h | displays this information |
| hsm | hs | HSM commands |
| audit | au | Audit commands |
| partition | par | Partition commands |
| appid | a | Manage Application Ids |
| slot | s | Manage the active slot number |
| file | f | File commands |
| srk | r | Secure Recovery commands |
| remoteBackup | rb | Manage Remote Backup Server |
| hagroup | ha | High Availability Group Commands |
| clientconfig | ccfg | Client Configuration |
| stc | stc | STC commands |

```
Command Result : 0x1 (Unknown command)
```

```
lunacm:> slot set slot 1
```

role login

Logs the named user into the partition at the current slot.

For Password-authenticated HSM, the entire credential is the password. When using the 'role login' command, you can enter your password at the command line where it will be visible on screen, or omit it and wait to be prompted after pressing enter. Passwords entered at the prompt are masked by '*' characters. This is the administrative password (Crypto Officer or Crypto User), and it is also the same password that is presented by your application program when it performs cryptographic operations on the application partition.

For PED-authenticated HSM, the authentication is the black PED Key and the password/challenge for Crypto Officer, or the gray PED Key and the password/challenge for Crypto User. You can create a challenge secret with command ["role createChallenge" on page 188](#) . The challenge secret will be needed, in addition to the PED Key secret, for you application to perform cryptographic operations.

If Partition Policy 22: Allow activation is not set (value = 0), then you must present both the black PED Key and the challenge secret for each login, including authentication by your application program.

If Partition Policy 22: Allow activation is set (value = 1 see ["partition changepolicy" on page 125](#)), then the PED Key secret is cached, and you can present only the password/challenge string at each subsequent login. That is, if the partition is activated, you are not prompted to respond to the PED.

At that point, your application program can authenticate with just the password/challenge string, as if the HSM was PW-authenticated.

Activation (caching of the PED Key secret) persists until you explicitly deactivate (see ["role deactivate" on page 189](#)) or until the HSM is restarted or loses power.



CAUTION: If too many bad login attempts are made against a role, the appropriate security policy for that role is enacted. For example, three bad attempts to log into the HSM SO role causes all HSM contents to be zeroized. Too many attempts on the Crypto Officer role causes that role to be locked out until reset by the SO. The bad-login count is reset by a successful login.



Note: For the Auditor role, if the bad login attempt threshold is exceeded, the HSM locks out that role for 60 seconds. The output of **role show**, during that time, gives a status of "Locked out".

However, **role show** continues to show a state of "Locked out" even after the lockout time has expired; the displayed status does not reset until after a successful login.



Note: PKCS#11 permits one role to be logged into a slot, per session. If a role is logged in, and you attempt to log in as a different role, the HSM presents an error message like USER_ALREADY_LOGGED_IN, indicating that some other user role is logged into the current slot via the current session. If you need to log in, your options are:

- log out the other user and log in as the desired user, in the current session
- or
- launch another session (lunacm or other tool), select the slot, and log in from there.

Note: Slots retain login state when current-slot focus changes.



For HSMs with firmware earlier than version 6.22.0, when you used **slot set** to move the focus from an HSM partition or slot with logged in session(s), to another partition or slot, any sessions on the original slot were automatically closed (thus logged out).

For HSMs with firmware version 6.22.0 of newer, you can use **slot set** to repeatedly shift focus among slots, and whatever login state was in force when you were previously focused on a slot is still in effect when you return to that slot.

Syntax

role login -name <name of role> [**-password** <password>]

| Parameter | Shortcut | Description |
|------------------|-----------|--|
| -name | -n | Specifies the name of the role that is logging in. Note: If you specify multiple users (for example role login -n Crypto Officer -n Partition SO , the last one entered (in this example, Partition SO), is used. |
| -password | -p | Specifies the password for the role. Omit this parameter to be prompted for a password, which will be obscured by * characters when entered. |

Example

Logging in to the administrative slot as the HSM SO

```
lunacm:> role list
```

```
Roles
=====
SO
Admin User
Auditor
```

```
Command Result : No Error
```

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

```
Please attend to the PED.
```

```
Command Result : No Error
```

```
lunacm:>
```

Logging in to the application partition slot as the Partition SO

```
lunacm:> role list
```

```
Roles
=====
Partition SO
```

Crypto Officer
Crypto User

Command Result : No Error

```
lunacm:> role login -name Partition SO
```

Please attend to the PED.

Command Result : No Error

Bad log in attempt as the HSM SO

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

Please attend to the PED.

Caution: You have only 2 Administrator login attempts left. If you fail 2 more consecutive login attempts (i.e. with no successful logins in between) the HSM will be ZEROIZED!!!

Error in execution: CKR_PIN_INCORRECT.

Command Result : 0xa0 (CKR_PIN_INCORRECT)

role logout

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

For PED-authenticated HSMs, if the activation policy is set, then logout does not uncache the PED Key data, so the next login will require only the password/challenge for success - no PED prompt appears.

Syntax

role logout

| Parameter | Shortcut | Description |
|-----------|----------|-------------|
| none | none | none. |

Example

```
lunacm:> role logout
```

```
Command Result : No Error
```

```
lunacm:>
```

role recoveryinit

Create an HA keypair. This command applies to SafeNet PCIe HSM or SafeNet USB HSM. Does not apply to SafeNet Network HSM partitions that appear in Lunacm via NTLS or STC channel.

(See also CKDemo "The HIGH AVAILABILITY RECOVERY Menu Functions")

Syntax

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

| 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 action (useful for scripting). |

Example

example here, please

role recoverylogin

Perform an HA recovery login. This command applies to SafeNet PCIe HSM or SafeNet USB HSM. Does not apply to SafeNet Network HSM partitions that appear in Lunacm via NTLS or STC channel.

(See also CKDemo "The HIGH AVAILABILITY RECOVERY Menu Functions")

Syntax

role recoverylogin -user <string> -slot <number> -keyhandle <number>

| Parameter | Shortcut | Description |
|-------------------|------------|-------------------------------|
| -user | -pl | User name. |
| -slot | -s | Target slot. |
| -keyhandle | -kh | Handle of RSA Private to use. |

Example

example here, please

role resetpw

Resets the password for a specified role. The partition SO can reset the Crypto Officer password or black PED key only if HSM policy 15: "Enable SO reset of partition PIN" is enabled. By default, this policy is not enabled and changing it is destructive.

If the target role is not on the current partition, you must specify the target role's partition's slot.



Note: Resetting passwords for roles on partitions other than the current partition is possible only from the administrative partition.

Syntax

```
role resetPW -name <role> [-password <password>] [-slot <slotnumber>]
```

| Parameter | Shortcut | Description |
|------------------|-----------|---|
| -name | -n | Name of role to have password reset. |
| -password | -p | Password for the specified role. Use this option for password-authenticated HSMs only. PED-authenticated HSMs will return an error. |
| -slot | -s | Target slot. |

Example

```
lunacm:> role resetpw -name Crypto Officer
```

```
    Please attend to the PED.
```

```
Command Result : No Error
```


role setdomain

Sets the domain of a role. Used only by the HSM's Auditor user. The Auditor role must have been initialized previously, and must be logged in, in order to set the domain.

Syntax

role setdomain [-domain <string> | -defaultdomain] [-force]

| Parameter | Shortcut | Description |
|-----------------------|-------------|--|
| -domain | -d | Set the role Cloning Domain string for password-authenticated HSM only; ignored for PED-authenticated HSM) NOTE: -domain and -defaultdomain are mutually exclusive parameters - attempting to use both causes the command to fail with an error message. |
| -defaultdomain | -def | Set the defaultdomain on a password-authenticated HSM; ignored for PED-authenticated HSM. (Deprecated - not recommended unless needed to clone with older HSMs that had defaultdomain set.) NOTE: -domain and -defaultdomain are mutually exclusive parameters - attempting to use both causes the command to fail with an error message. |
| -force | -f | Force the action (useful for scripting) |

Example 1 - setDomain on PED-auth HSM

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

```
    Please attend to the PED.
```

```
Command Result : No Error
```

```
lunacm:> role setDomain
```

```
    You are about to set a new domain for the role.
    Are you sure you wish to continue?
```

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

```
    Please attend to the PED.
```

```
Command Result : No Error
```

```
lunacm:>
```

Example 2 - setDomain choosing Defaultdomain on PW-auth HSM (not recommended)

```
lunacm:> role setDomain -defaultdomain
```

```
Warning: You have selected to use the default domain.
```

This is not recommended for new implementations and is only available for backwards compatibility.
This capability is deprecated and will be discontinued in a future release.

You are about to set a new domain for the role.
Are you sure you wish to continue?

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

Please attend to the PED.

Command Result : No Error

lunacm:>

role show

Shows the state of the named role.



Note: For the Auditor role, if the bad login attempt threshold is exceeded, the HSM locks out that role for 60 seconds. The output of **role show**, during that time, gives a status of "Locked out".

However, **role show** continues to show a state of "Locked out" even after the lockout time has expired; the displayed status does not reset until after a successful login.

Syntax

role show -name <string>

| Parameter | Shortcut | Description |
|-----------|----------|----------------------|
| -name | -n | name of role to show |

Example

```
lunacm:> role show -name Crypto Officer
```

```
State of role 'Crypto Officer':
  Primary authentication type:      PED
  Secondary authentication type:    PIN
  Failed login attempts before lockout: 10
```

Command Result : No Error

```
lunacm:> role show -name Crypto User
```

```
State of role 'Crypto User':
  Not initialized.
```

Command Result : No Error

```
lunacm:>
```

slot

Access the slot commands.

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

This allows (for example) a USB-connected HSM to be connected to a SafeNet appliance or to a SafeNet HSM client computer during a cryptographic session without requiring a restart. Similarly, it allows HA operation, where client activity is directed toward the HA virtual slot, but the client must be able to see all physical slots, in addition to that HA virtual slot, in order to coordinate the function of the HA group.

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

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

Syntax

slot

```

configset
configshow
list
partitionlist
set

```

| Parameter | Shortcut | Description |
|----------------------|--------------|--|
| configset | cset | Set a configuration item for a slot. See "slot configset" on the next page . |
| configshow | cshow | Show the configuration for a slot . See "slot configshow" on page 207 . |
| list | l | List the available slots. See "slot list" on page 208 . |
| partitionlist | plist | List the partitions for a slot. See "slot partitionlist" on page 210 . |
| set | s | Set the current slot. See "slot set" on page 211 . |

slot configset

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

This command is used only with a SafeNet Backup HSM at firmware version earlier than 6.22.0, and allows an archive partition on the Backup HSM to be accessed in a manner similar to an application partition on a general-purpose HSM. This command was originally developed for purposes of object migration from older PCMCIA-type HSMs in a SafeNet DOCK reader. It is still available, and can be used on a SafeNet Backup HSM, if you have a use for it. For a Backup HSM partition that is exposed by the **slot configset** command, the following limitations apply:

- keys cannot be used for cryptographic objects
- keys cannot be modified.

The benefit of applying the **slot configset** command to a Backup HSM is that, on an identified archive partition:

- keys can be deleted, individually/selectively
- keys can be cloned to other HSM partitions.

Partitions are named as they are created on a Backup HSM to accept archived objects during backup operations. If more than one backup partition exists on a Backup HSM, they are not exposed when you perform the `lunacm slot list` command. Generally the only backup partition that is referenced by default when the slot listing shows a slot as containing a SafeNet Backup HSM is from older editions of SafeNet HSMs, and is called "Cryptoki User". To choose which, of potentially several, archive partitions within a Backup HSM is the active partition, and to make it accessible, you need to identify that archive partition by name.

The process is to list/view the partitions while the Backup HSM is the current slot in LunaCM, using **partition list**, in order to see their partition names. Then run **slot configset -slot** <slot#-of-the-backup-hsm> **-partitionname** <name-of-desired-partition-on-backup-hsm> Then, for example, use **partition clone** to clone selected objects to other HSM partition slots.



Note: This command can be used with SafeNet Backup HSMs at firmware versions older than 6.22.0. Backup HSMs with firmware 6.22.0 or newer already appear as multiple independent partitions in a slot list, without need for **slot configset**.



Note: The configuration set with this command exists for the current LunaCM session only. If you log out of your LunaCM session, your **slot configset** configuration is erased.

Syntax

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

| 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 backuppar3
```

Slot configuration was successfully updated.

Command Result : No Error

slot configshow

Show the configuration information for the specified slot number.

Syntax

slot configshow -slot <slot_number>

| 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. If your host computer contains, or is connected to, only a single SafeNet HSM with firmware older than version 6.22.0, then a slot list has just one entry. If your single HSM has firmware 6.22.0 or newer, then the HSM administrative partition and any application partition are distinct and appear individually in a lunacm slot list, so at least two slots. Similarly, if you have several local SafeNet HSMs installed or connected, or if you have SafeNet Network HSM application partitions Ethernet-connected via NTLS or STC links, then you can have multiple slots represented in a lunacm slot list.

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

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



Note: The lunacm command **hagroup haonly** acts on your client applications, either allowing (default or `hagroup haonly -disable`) or disallowing (`hagroup haonly -enable`) the application to see individual HSM partition slots or just the HA group virtual slot, respectively. The command has no effect on administrative tools like lunacm, where a "slot list" returns all slots, both actual and virtual, regardless of the status of **hagroup haonly**.

Syntax

slot list

Example

```
lunacm:> slot list
```

```
Slot Id -> 1
Tunnel Slot Id -> 2
Label -> mypci-e
Serial Number -> 150022
Model -> K6 Base
Firmware Version -> 6.22.0
Configuration -> Luna HSM Admin Partition Signing With Cloning Mode
Slot Description -> Admin Token Slot
HSM Configuration -> Luna HSM Admin Partition (PED)
HSM Status -> OK
```

```
Slot Id -> 3
Label -> SafeG5
Serial Number -> 7001812
Model -> G5Base
Firmware Version -> 6.22.0
Configuration -> Luna HSM Admin Partition Signing With Cloning Mode
Slot Description -> Admin Token Slot
HSM Configuration -> Luna HSM Admin Partition (PED)
HSM Status -> OK
```

```
Slot Id -> 4
```



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

Slot Id ->           4
Label ->            myRBSG5Bk
Serial Number ->    7000329
Model ->           G5Backup
Firmware Version -> 6.22.0
Configuration ->   Luna HSM Admin Partition (PW) Backup Mode
Slot Description -> Net Admin Token Slot
HSM Configuration -> Luna HSM Admin Partition (PW) Backup Device
HSM Status ->      OK
```

Current Slot ID: 3

Command Result : No Error



Note: Each HSM administrative partition in a slot list includes "HSM Status". The possible values are listed, along with expanded descriptions and possible responses, at ["HSM Status Values" on page 1](#) in the *Administration Guide*.

slot partitionlist

List the partitions for the specified slot. This is of interest when a cryptographic slot might contain more than one HSM partition. In general, one slot contains one partition, but a SafeNet Backup HSM, for example, might occupy one cryptographic slot while containing many partitions (see "[slot configset](#)" on page 205).

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.

Lunacm commands work on the current slot. If there is only one slot, then it is always the current slot. If there is more than one slot, then use the **slot set** command to direct the focus at the desired slot/partition, so that you can use lunacm commands against whatever HSM admin partition or application partition occupies the indicated slot.

If you have only a single HSM with firmware older than version 6.22.0 installed-in/connected-to your computer, then lunacm displays just the one slot, which is both the HSM administrative partition and the application partition. So **slot set** would not be useful in that case.

This command is useful where you have more than one SafeNet module installed-in or connected-to your computer, or when you have a single HSM with firmware 6.22.0 or newer, such that the HSM administrative slot is separate from the application partition slot. In those cases, you can use the **slot list** command to see which slot numbers have been assigned, and then use **slot set** to specify which of the available HSM partitions (in their slots) you wish to address with **lunacm** commands.

Note: Slots retain login state when current-slot focus changes.



For HSMs with firmware earlier than version 6.22.0, when you used **slot set** to move the focus from an HSM partition or slot with logged in session(s), to another partition or slot, any sessions on the original slot were automatically closed (thus logged out).

For HSMs with firmware version 6.22.0 or newer, you can use **slot set** to repeatedly shift focus among slots, and whatever login state was in force when you were previously focused on a slot is still in effect when you return to that slot.

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 Secure Recovery commands to configure and manage the HSM tamper and secure recovery key (SRK) behavior and the setting and recovery from Secure Transport Mode. See MTK and SRK discussion in "[Tamper, Secure Transport, and Purple PED Keys](#)" on page 1 in the *Product Overview*.



Note: If Lunacm **srk show** command does not show the expected state for SRK after you run the **srk enable** or **srk disable** command, the cache might not have been updated, following the most recent change. Exit and re-launch lunacm to see the current state of SRK.

Syntax

srk

disable
enable
generate
recover
show
transport

| Parameter | Shortcut | Description |
|------------------|----------|--|
| disable | d | Disable Secure Transport Mode functionality. See " srk disable " on the next page. |
| enable | e | Enable Secure Transport Mode functionality. See " srk enable " on page 214. |
| generate | g | Generate a new SRK. See " srk generate " on page 215. |
| recover | r | Recover from temper or exit transport mode. See " srk recover " on page 216. |
| show | s | Show the Secure Recovery state. See " srk show " on page 217. |
| transport | t | Set the HSM into transport mode. See " srk transport " on page 218. |

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.



Note: If Lunacm **srk show** command does not show the expected state for SRK after you run the **srk enable** or **srk disable** command, the cache might not have been updated, following the most recent change. Exit and re-launch lunacm to see the current state of SRK.

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.



Note: If Lunacm **srk show** command does not show the expected state for SRK after you run this command, the cache might not have been updated, following the most recent change. Exit and re-launch lunacm to see the current state of SRK.

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.



Note: If Lunacm **srk show** command does not show the expected state for SRK after you run the **srk enable** or **srk disable** command, the cache might not have been updated, following the most recent change. Exit and re-launch lunacm to see the current state of SRK.

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 enabled
```

```
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
```

stc

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

See also "[stconfig](#)" on [page 232](#) for the STC configuration commands, which you can use to specify the network and security settings for the STC link.

Syntax

stc

disable
enable
identitycreate
identitydelete
identityexport
identityshow
partitionderegister
partitionregister
status
tokeninit
tokenlist

| Parameter | Shortcut | Description |
|----------------------------|-------------|--|
| disable | d | Disable STC for the current slot. See " stc disable " on page 221 . |
| enable | e | Enable STC for the current slot. See " stc enable " on page 222 . |
| identitycreate | idc | Create a client identity on the STC client token. See " stc identitycreate " on page 223 . |
| identitydelete | idd | Delete a client identity from the STC identity token. See " stc identitydelete " on page 224 . |
| identityexport | ide | Export the STC client identify to a file. See " stc identityexport " on page 225 . |
| identityshow | idsh | Display the client name, public key hash, and registered partitions for the STC client token. See " stc identityshow " on page 226 . |
| partitionderegister | pard | Remove a partition identity from the STC client token. See " stc partitionderegister " on page 227 . |
| partitionregister | parr | Register a partition to the STC client token. See " stc partitionregister " on page 228 . |
| status | s | Display status and configuration information for an STC link. See " stc status " on page 229 . |
| tokeninit | ti | Initialize a client token. See " stc tokeninit " on page 230 . |

| Parameter | Shortcut | Description |
|------------------|-----------|---|
| tokenlist | tl | List the available STC client identity tokens. See " stc tokenlist " on page 231. |

stc disable

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



CAUTION: Disabling the STC link terminates all existing sessions.

Syntax

stc disable [-id <server_id>] [-force]

| Parameter | Shortcut | Description |
|-----------------|----------------|---|
| -id <server_id> | -i <server_id> | Specifies the identifier of the SafeNet Network HSM appliance to which you want to disable STC, as displayed using the command " clientconfig listservers " on page 42. |
| -force | -f | Force the action without prompting. |

Example

```
lunacm:> stc disable
```

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

```
0,1,2,3
```

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

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

stc enable

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

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



CAUTION: Enabling the STC link terminates all existing NTLS sessions.

Syntax

stc enable [-force]

| Parameter | Shortcut | Description |
|------------------------------|-----------------------------|--|
| -force | -f | Force the action without prompting. |
| -id <server_id> | -i <server_id> | Specifies the identifier of the SafeNet Network HSM appliance to which you want to disable STC, as displayed using the command "clientconfig listservers" on page 42 . |

Example

```
lunacm:> stc e
```

This command will enable STC.

The existing LunaCM session will be terminated. Are you sure you wish to continue?

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

stc identitycreate

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

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



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

Syntax

stc identitycreate -label <label> [-force]

| Parameter | Shortcut | Description |
|-----------------------|-------------------|-------------------------------------|
| -label <label> | -l <label> | Specifies the token label. |
| -force | -f | Force the action without prompting. |

Example

```
lunacm:> stc idc -l dsittler
```

Client identity dsittler successfully created.

The client identity is placed under /usr/safenet/lunaclient/data/client_identities/dsittler

stc identitydelete

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

This command does the following, in the order specified:

1. Deletes the client identity public key in the partition.
2. Deletes each registered partition identity.
3. Deletes the client identity.

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



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

Syntax

stc identitydelete [-force]

| Parameter | Shortcut | Description |
|-----------|----------|-------------------------------------|
| -force | -f | Force the action without prompting. |

Example

```
lunacm:> stc idd
```

```
Are you sure you want to delete the client identity <name>?
If the client identity is deleted, all the registered partitions will be lost and will cause
loss of service.
```

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

```
Successfully deleted client identity myclient.
```


stc identityexport

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

Syntax

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

| Parameter | Shortcut | Description |
|--------------|-----------|--|
| -file | -f | Specifies the full path of the file to which you want to export the client identity. If this parameter is not specified, the client identity is saved to the following location: <ul style="list-style-type: none"><luna_client_root_dir>/data/client_identities/<client-name> |

Example

```
lunacm:> stc ide
```

```
Successfully exported the client identity to  
/usr/safenet/lunaclient/data/client_identities/dsittler
```

stc identityshow

Display the following information for the STC client token:

- the client identity name
- the public key SHA1 hash for the client identity
- a list of the partitions registered with the client identity

Syntax

stc identityshow

Example

```
lunacm:> stc ids
```

```
Client Identity Name:      myclient
Public Key SHA1 Hash:     5f3395af2ae01ac25c1a27dc25
```

| Partition Name | Partition Serial Number | Partition Public Key SHA1 Hash |
|----------------|-------------------------|--|
| par_app3 | 124338921 | 23159590be9b57fd0c9d8a84beeed04d4279c01c |
| par_app47 | 152943202 | de9f2c7fd25e1b3afad3e85a0bd17d9b100db4b3 |
| par_app12 | 150253010 | 2fd4e1c67a2d28fced849ee1bb76e7391b93eb12 |

stc partitionderegister

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

After invoking this command, use the command "[clientconfig restart](#)" on page 43 to restart LunaCM and refresh the slot list.



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

Syntax

stc partitionderegister -serial <partition_serial_number> [-force]

| Parameter | Shortcut | Description |
|--|-------------------------------------|---|
| -serial <partition_serial_number> | -s <partition_serial_number> | Specifies the serial number of the partition to deregister. |
| -force | -f | Force the action without prompting. |

Example

```
lunacm:> stc pard -s 98730559
```

```
Are you sure you want to deregister the partition 98730559?
Type 'proceed' to continue, or 'quit' to quit now -> proceed
```

```
Partition 98730559 successfully deregistered from the client token.
```

stc partitionregister

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

After invoking this command, use the command ["clientconfig restart" on page 43](#) to restart LunaCM and refresh the slot list.

Syntax

stc partitionregister -file <partition_id_file_path> [-label <partition_id_label>]

| Parameter | Shortcut | Description |
|---------------------------------------|------------------------------------|---|
| -file <partition_id_file_path> | -f <partition_id_file_path> | Specifies the full path to the partition identity file. |
| -label <partition_id_label> | -l <partition_id_label> | Specifies a label for the partition identity. |

Example

```
lunacm:> lunacm:> stc partitionregister -file /usr/safenet/lunaclient/partition_identities/359693009026.pid -label mySA_mySTCpartition
```

Partition identity 359693009026 successfully registered.

stc status

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

Syntax

stc status [-all]

| Parameter | Shortcut | Description |
|-----------|----------|---------------------------------------|
| -all | -a | Display the STC status for all slots. |

Example



Note: The key life is displayed only if allowed by the partition security policy settings.

```
lunacm:> stc status
```

```
Enabled:           Yes
Status:           Connected
Channel ID:       2
Cipher Name:      AES-256 Bit with Cipher Block Chaining
HMAC Name:        HMAC with SHA 512 Bit
```

stc tokeninit

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

Use the command "[stc tokenlist](#)" on the next page to list the available tokens and to determine whether the token has been initialized.



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

Syntax

stc tokeninit -label <token_label> [-force]

| Parameter | Shortcut | Description |
|-----------------------------|-------------------------|-------------------------------------|
| -label <token_label> | -l <token_label> | Specifies the label of the token. |
| -force | -f | Force the action without prompting. |

Example

Uninitialized token

```
lunacm:> stc ti -l rkelly
```

Successfully initialized the identity token.

Previously initialized token

```
lunacm:> stc ti -l nullman
```

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

```
Client Identity Name:      fmahovolich
Public Key SHA1 Hash:     5f3395af2ae01ac25c1a27dc25
```

```
Partition Name  Partition Serial Number  Partition Public Key SHA1 Hash
mapleleafs     124338921                 23159590be9b57fd0c9d8a84beeed04d4279c01c
redwings       152943202                 de9f2c7fd25e1b3afad3e85a0bd17d9b100db4b3
```

```
Would you like to re-initialize the identity token?
Type 'proceed' to continue, or 'quit' to quit now -> proceed
```

Successfully initialized the identity token.

stc tokenlist

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

- which token to use when setting up a token using the command "[stc tokeninit](#)" on the previous page.
- whether the token has been initialized.



Note: Only one token per client is supported in this release.

Syntax

stc tokenlist

Example

```
lunacm:> stc tk1
```

| Token Slot ID | Token Name | Serial Number | Initialized |
|---------------|------------|---------------|-------------|
| 1 | token_1 | 23c9882a1 | Yes |

stconfig

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



Note: These commands are visible only if the current slot is a PPSO partition.

See also "[stc](#)" on [page 219](#) for STC setup commands, which you can use to set up and manage an STC network link.

Syntax

stconfig

activationtimeoutset
activationtimeoutshow
cipherdisable
cipherenable
ciphershow
clientderegister
clientlist
clientregister
hmacdisable
hmacenable
hmacshow
partitionidexport
partitionidshow
rekeythresholdset
rekeythresholdshow
replaywindowset
replaywindowshow

| Parameter | Shortcut | Description |
|------------------------------|-------------|---|
| activationtimeoutset | atse | Set the activation timeout for an STC link. See " stconfig activationtimeoutset " on page 234 . |
| activationtimeoutshow | atsh | Display the activation timeout for an STC link. See " stconfig activationtimeoutshow " on page 235 . |
| cipherdisable | cid | Disable the use of a symmetric encryption cipher algorithm for data encryption on an STC link. See " stconfig cipherdisable " on page 236 . |
| cipherenable | cie | Enable the use of a symmetric encryption cipher algorithm for data encryption on an STC link. See " stconfig cipherenable " on page 238 . |
| ciphershow | cish | List the symmetric encryption cipher algorithms you can use for data encryption on an STC link. See " stconfig ciphershow " on page 240 . |
| clientderegister | cld | Deregister a client's STC public key from a partition. See " stconfig |

| Parameter | Shortcut | Description |
|---------------------------|--------------|--|
| | | clientderegister " on page 241. |
| clientlist | cli | List the clients registered to a partition. See " stconfig clientlist " on page 242. |
| clientregister | clr | Register a client's STC public key to a partition. See " stconfig clientregister " on page 243. |
| hmacdisable | hmd | Disable the use of an HMAC message digest algorithm for message integrity verification on an STC link. See " stconfig hmacdisable " on page 244. |
| hmacenable | hme | Enable the use of an HMAC message digest algorithm for message integrity verification on an STC link. See " stconfig hmacenable " on page 246 |
| hmacshow | hsh | List the HMAC message digest algorithms you can use for message integrity verification on an STC link. See " stconfig hmacshow " on page 248. |
| partitionidexport | pidex | Export a partition's STC public key to a file. See " stconfig partitionidexport " on page 249. |
| partitionidshow | pish | Display a partition's STC public key and serial number. " stconfig partitionidshow " on page 250. |
| rekeythresholdset | rkse | Set the rekey threshold for the symmetric key used to encrypt data on an STC link. See " stconfig rekeythresholdset " on page 251. |
| rekeythresholdshow | rksh | Display the rekey threshold for the symmetric key used to encrypt data on an STC link. See " stconfig rekeythresholdshow " on page 252. |
| replaywindowset | rwse | Set the size of the packet replay window for an STC link. See " stconfig replaywindowset " on page 253. |
| replaywindowshow | rwsh | Display the size of the packet replay window for an STC link. See " stconfig replaywindowshow " on page 254. |

stccconfig activationtimeoutset

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

This command is available only if the current slot is a PPSO partition.

Syntax

stccconfig activationtimeoutset [-slot <slot_id>] -time <timeout>

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

Example

Current slot

```
lunacm:> stcc atse -time 30
```

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

Specified slot

```
lunacm:> stcc atse -slot 3 -time 30
```

Successfully changed the activation timeout for slot 3 to 30 seconds.

stccnfig activationtimeoutshow

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

This command is available only if the current slot is a PPSO partition.

Syntax

stccnfig activationtimeoutshow [-slot <slot_id>]

| Parameter | Shortcut | Description |
|-----------------|--------------|--|
| -slot <slot_id> | -s <slot_id> | Specifies the slot containing the partition for which you want to display the STC link activation timeout. This parameter is available only if you are logged into the HSM's Admin partition. |

Example

Current slot

```
lunacm:> stcc atsh
```

The activation timeout for the current slot is 30 seconds.

Specified slot

```
lunacm:> stcc atsh -s 3
```

The activation timeout for slot 3 is 60 seconds.

stcconfig cipherdisable

Disable the use of a symmetric encryption cipher algorithm for data encryption on an STC link. All data transmitted over the STC link will be encrypted using the cipher that is both enabled and that offers the highest level of security. For example, if AES 192 and AES 256 are enabled, and AES 128 is disabled, AES 256 will be used. You can use the command ["stcconfig ciphershow" on page 240](#) to show which ciphers are currently enabled and the command ["stc status" on page 229](#) to display the cipher that is currently being used.

This command is available only if the current slot is a PPSO partition.



Note: Performance is reduced for larger ciphers.

Syntax

stcconfig cipherdisable [-slot <slot_id>] -id <cipher_id>

| Parameter | Shortcut | Description |
|-----------------|-----------------|---|
| -slot <slot_id> | -s <slot_id> | Specifies the slot containing the partition for which you want to allow or disallow a cipher algorithm. This parameter is available only if you are logged into the HSM's Admin partition. |
| -id <cipher_id> | -id <cipher_id> | Specifies the numerical identifier of the cipher you want to allow or disallow, as listed by "stcconfig ciphershow" on page 240 |

Example

Current slot

```
lunacm:> stcc cish
```

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

```
STC Encryption: On
```

| Cipher ID | Cipher Name | Enabled |
|-----------|--|---------|
| 1 | AES 128 Bit with Cipher Block Chaining | Yes |
| 2 | AES 192 Bit with Cipher Block Chaining | Yes |
| 3 | AES 256 Bit with Cipher Block Chaining | Yes |

```
lunacm:> stcc cid -id 1
```

AES 128 Bit with Cipher Block Chaining is now disabled for the current slot.

Specified slot

```
lunacm:> stcc cish -s 3
```

This table lists the ciphers supported for STC links to the current slot. Enabled ciphers are accepted during STC link negotiation with a client.

If all ciphers are disabled, STC links to the partition are not encrypted.

STC Encryption: On

| Cipher ID | Cipher Name | Enabled |
|-----------|--|---------|
| 1 | AES 128 Bit with Cipher Block Chaining | Yes |
| 2 | AES 192 Bit with Cipher Block Chaining | Yes |
| 3 | AES 256 Bit with Cipher Block Chaining | Yes |

```
lunacm:> stcc cid -s 3 -d -id 2
```

AES 192 Bit with Cipher Block Chaining is now disabled for slot 3.

stcconfig cipherenable

Enable the use of a symmetric encryption cipher algorithm for data encryption on an STC link. All data transmitted over the STC link will be encrypted using the cipher that is both enabled and that offers the highest level of security. For example, if AES 192 and AES 256 are enabled, and AES 128 is disabled, AES 256 will be used. You can use the command "[stcconfig ciphershow](#)" on page 240 to show which ciphers are currently enabled and the command "[stc status](#)" on page 229 to display the cipher that is currently being used.

This command is available only if the current slot is a PPSO partition.



Note: Performance is reduced for larger ciphers.

Syntax

stcconfig cipherenable [-slot <slot_id>] -id <cipher_id>

| Parameter | Shortcut | Description |
|-----------------|-----------------|---|
| -slot <slot_id> | -s <slot_id> | Specifies the slot containing the partition for which you want to allow or disallow a cipher algorithm. This parameter is available only if you are logged into the HSM's Admin partition. |
| -id <cipher_id> | -id <cipher_id> | Specifies the numerical identifier of the cipher you want to allow or disallow, as listed by " stcconfig ciphershow " on page 240 |

Example

Current slot

```
lunacm:> stcc cish
```

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

STC Encryption: On

| Cipher ID | Cipher Name | Enabled |
|-----------|--|---------|
| 1 | AES 128 Bit with Cipher Block Chaining | No |
| 2 | AES 192 Bit with Cipher Block Chaining | Yes |
| 3 | AES 256 Bit with Cipher Block Chaining | Yes |

```
lunacm:> stcc cie -id 1
```

AES 128 Bit with Cipher Block Chaining is now enabled for the current slot.

Specified slot

```
lunacm:> stcc cish -s 3
```

This table lists the ciphers supported for STC links to the current slot. Enabled ciphers are accepted during STC link negotiation with a client.

If all ciphers are disabled, STC links to the partition are not encrypted.

STC Encryption: On

| Cipher ID | Cipher Name | Enabled |
|-----------|--|---------|
| 1 | AES 128 Bit with Cipher Block Chaining | No |
| 2 | AES 192 Bit with Cipher Block Chaining | Yes |
| 3 | AES 256 Bit with Cipher Block Chaining | Yes |

```
lunacm:> stcc cie -s 3 -id 1
```

AES 128 Bit with Cipher Block Chaining is now enabled for slot 3.

stccconfig ciphershow

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

This command is available only if the current slot is a PPSO partition.

Syntax

stccconfig ciphershow [-slot <slot_id>]

| Parameter | Shortcut | Description |
|-----------------|--------------|---|
| -slot <slot_id> | -s <slot_id> | Specifies the slot containing the partition whose available cipher algorithms to want to display. This parameter is available only if you are logged into the HSM's Admin partition. |

Example

Current slot

```
lunacm:> stcc cish
```

```
Cipher ID  Cipher Name
0           No Cipher
1           AES 128 Bit with Cipher Block Change
2           AES 192 Bit with Cipher Block Change
3           AES 256 Bit with Cipher Block Change
```

Specified slot

```
lunacm:> stcc cish -s
```

```
Cipher ID  Cipher Name
0           No Cipher
1           AES 128 Bit with Cipher Block Change
2           AES 192 Bit with Cipher Block Change
3           AES 256 Bit with Cipher Block Change
```


stccconfig clientderegister

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

This command is available only if the current slot is a PPSO partition.



CAUTION: Deregistering a client's public key disables the STC link to that client.



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

Syntax

```
stccconfig clientderegister -slot <slot_id> -label <client_label>
```

| Parameter | Shortcut | Description |
|------------------------------|--------------------------|---|
| -slot <slot_id> | -s <slot_id> | Specifies the slot containing the partition from which you want to deregister the client. This parameter is available only if you are logged into the HSM's Admin partition. |
| -label <client_label> | -l <client_label> | A string used to identify the client being deregistered. |

Example

Current slot

```
lunacm:> stcc cld -l dkeon
```

Successfully deregistered the client public key of dkeon in slot 3

Specified slot

```
lunacm:> stcc -s 2 cld -l dkeon
```

Successfully deregistered the client public key of dkeon in slot 2

stccconfig clientlist

List the clients registered to a partition.

This command is available only if the current slot is a PPSO partition.

Syntax

stccconfig clientlist [-slot <slot_id>]

| Parameter | Shortcut | Description |
|-----------------|--------------|---|
| -slot <slot_id> | -s <slot_id> | Specifies the slot containing the partition for which you want to list the registered clients This parameter is available only if you are logged into the HSM's Admin partition. |

Example

Current slot

```
lunacm:> stcc cll
```

```
Client Name   Client Identity Public Key SHA1 Hash
rellis        2fd4e1c67a2d28fced849ee1bb76e7391b93eb1
nullman       de9f2c7fd25e1b3afad3e85a0bd17d9b100db4b3
phenderson    da39a3ee5e6b4b0d3255bfe95601890afd80709
```

Specified slot

```
lunacm:> stcc cll -s 4
```

```
Client Name   Client Identity Public Key SHA1 Hash
rellis        2fd4e1c67a2d28fced849ee1bb76e7391b93eb1
nullman       de9f2c7fd25e1b3afad3e85a0bd17d9b100db4b3
phenderson    da39a3ee5e6b4b0d3255bfe95601890afd80709
```

stccconfig clientregister

Register a client's STC public key to a partition. You must be logged in to the partition as the SO to use this command. This command is available only if the current slot is a PPSO partition.



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

Syntax

stccconfig clientregister [-slot <slot_id>] -label <client_label> -file <client_public_key>

| Parameter | Shortcut | Description |
|-----------------|--------------|--|
| -slot <slot_id> | -s <slot_id> | Specifies the slot containing the partition to which you want to register the client. This parameter is available only if you are logged into the HSM's Admin partition. |
| -label | -l | A string used to identify the client being registered. |
| -file | -f | Specifies the full path to the client public key file. |

Example

Current slot

```
lunacm:> stcc clr -n bsalming -f /usr/safenet/lunaclient/identities/45021294.pem
```

Successfully registered the client public key of bsalming in slot 3

Specified slot

```
lunacm:> stcc clr -s 2 -n bsalming -f /usr/safenet/lunaclient/identities/45021294.pem
```

Successfully registered the client public key of bsalming in slot 2

stcconfig hmacdisable

Disable the use of an HMAC message digest algorithm for message integrity verification on an STC link. The HMAC algorithm that is both enabled and that offers the highest level of security is used. For example, if SHA 256 and SHA 512 are enabled, SHA 512 is used. You can use the command `stcconfig hmacshow` on page 248 to show which HMAC message digest algorithms are currently enabled/disabled and the command `stc status` on page 229 to display the HMAC message digest algorithm that is currently being used.

This command is available only if the current slot is a PPSO partition.

Syntax

`stcconfig hmacdisable -id <hmac_id> [-slot <slot_id>]`

| Parameter | Shortcut | Description |
|------------------------------------|----------------------------------|---|
| <code>-id <hmac_id></code> | <code>-id <hmac_id></code> | Specifies the numerical identifier of the HMAC message digest algorithm you want to use, as listed using <code>stcconfig hmacshow</code> on page 248 |
| <code>-slot <slot_id></code> | <code>-s <slot_id></code> | Specifies the slot containing the partition on which you want to allow or disallow an HMAC algorithm. This parameter is available only if you are logged into the HSM's Admin partition. |

Example

Current slot

```
lunacm:> stcconfig hmacshow -slot 1
```

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

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

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

```
lunacm:> stcconfig hmacdisable -id 0
```

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

```
lunacm:> stcc hmacshow
```

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

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

Specified slot

```
lunacm:> stcc hsh
```

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

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

```
lunacm:> stccconfig hmacdisable -slot 2 -id 0
```

HMAC with SHA 256 Bit is now disabled for slot 2.

stconfig hmacenable

Enable the use of an HMAC message digest algorithm for message integrity verification on an STC link. The HMAC algorithm that is both enabled and that offers the highest level of security is used. For example, if SHA 256 and SHA 512 are enabled, SHA 512 is used. You can use the command `stconfig hmacshow` on page 248 to show which HMAC message digest algorithms are currently enabled/disabled and the command `stc status` on page 229 to display the HMAC message digest algorithm that is currently being used.

This command is available only if the current slot is a PPSO partition.

Syntax

`stconfig hmacenable [-slot <slot_id>] -id <hmac_id>`

| Parameter | Shortcut | Description |
|------------------------------------|----------------------------------|---|
| <code>-slot <slot_id></code> | <code>-s <slot_id></code> | Specifies the slot containing the partition on which you want to allow or disallow an HMAC algorithm. This parameter is available only if you are logged into the HSM's Admin partition. |
| <code>-id <hmac_id></code> | <code>-id <hmac_id></code> | Specifies the numerical identifier of the HMAC message digest algorithm you want to use, as listed using <code>stconfig hmacshow</code> on page 248 |

Example

Current slot

```
lunacm:> stconfig hmacshow -slot 1
```

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

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

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

```
lunacm:> stconfig hmacenable -id 0
```

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

```
lunacm:> stcc hmacshow
```

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

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

Specified slot

```
lunacm:> stcc hsh
```

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

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

```
lunacm:> stccconfig hmacdisable -slot 2 -id 0
```

HMAC with SHA 256 Bit is now enabled for slot 2.

stcconfig hmacshow

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

This command is available only if the current slot is a PPSO partition.

Syntax

stcconfig hmac show [-slot <slot_id>]

| Parameter | Shortcut | Description |
|-----------------|--------------|--|
| -slot <slot_id> | -s <slot_id> | Specifies the slot containing the partition whose available HMAC algorithms you want to display. This parameter is available only if you are logged into the HSM's Admin partition. |

Example

Current slot

```
lunacm:> stcc hsh
```

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

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

Specified slot

```
lunacm:> stcc hsh -s 2
```

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

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

stccconfig partitionidexport

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

This command is available only if the current slot is a PPSO partition.



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

Syntax

stccconfig partitionidexport [-slot <slot_id>] [-file <file_path>]

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

Example

Current slot

```
lunacm:> stcc pidex
```

Successfully exported the partition identity public key of slot 3 to /usr/lunaclient/bin/identities/36928740.pem

Specified slot

```
lunacm:> stcc pidex -s 2
```

Successfully exported the partition identity public key of slot 2 to /usr/lunaclient/bin/identities/30987740.pem

stcconfig partitionidshow

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

This command is available only if the current slot is a PPSO partition.

Syntax

stcconfig partitionidshow [-slot <slot_id>]

| Parameter | Shortcut | Description |
|-----------------|--------------|--|
| -slot <slot_id> | -s <slot_id> | Specifies the slot for the partition for which you want to display the public key and serial number. This parameter is available only if you are logged into the HSM's Admin partition. |

Example

Current slot

```
lunacm:> stcc pidsh
```

```
Partition Serial Number:          150253010
Partition Identity Public Key SHA1 Hash: 2fd4e1c67a2d28fced849ee1bb76e7391b93eb12
```

Specified slot

```
lunacm:> stcc pidsh -s 2
```

```
Partition Serial Number:          1588965732
Partition Identity Public Key SHA1 Hash: 31aec4e3bc2cc3b441aebce3cce32a3aa24df3fd
```

stcconfig rekeythresholdset

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

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

This command is available only if the current slot is a PPSO partition.

Syntax

stcconfig rekeythresholdset [-slot <slot_id>] -value <threshold>

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

Example

Current slot

```
lunacm:> stcc rkse -v 200
```

Successfully changed the rekey threshold for slot 3 to 200 million messages.

Specified slot

```
lunacm:> stcc rkse -s 2 -v 200
```

Successfully changed the rekey threshold for the current slot to 200 million messages.

stccconfig rekeythresholdshow

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

This command is available only if the current slot is a PPSO partition.

Syntax

stccconfig rekeythresholdset [-slot <slot_id>]

| Parameter | Shortcut | Description |
|------------------------|---------------------|--|
| -slot <slot_id> | -s <slot_id> | Specifies the slot containing the partition for which you want to display the rekey threshold. This parameter is available only if you are logged into the HSM's Admin partition. |

Example

Current slot

```
lunacm:> stcc rksh
```

```
Current rekey threshold for HSM is 400 million messages.
```

Specified slot

```
lunacm:> stcc rksh -s 2
```

```
Current rekey threshold for HSM is 400 million messages.
```

stccconfig replaywindowset

Set the size of the packet replay window for an STC link. This value specifies the number of packets in the window of sequenced packets that are tracked to provide anti-replay protection.

This command is available only if the current slot is a PPSO partition.

About the Replay Window

All packets sent over the STC link are sequenced and tracked. This allows the receiver to reject old or duplicate packets, thus preventing an attacker from attempting to insert or replay packets on the link. STC employs a sliding window for replay prevention. The receiver remembers which packets it has received within the specified window, and rejects any packets that have already been received or that are older than the oldest packet in the window. Some flexibility is allowed in accepting packets ahead of the sequence window, as valid packets in a short range ahead of the window cause the window to slide forward.



Note: Each STC packet corresponds to a single command. That is, each command sent to the HSM is encapsulated within a single STC packet.

Syntax

stccconfig replaywindowset [-slot <slot_id>] -size <number_of_messages>

| Parameter | Shortcut | Description |
|---------------------------|------------------------|--|
| -slot <slot_id> | -s <slot_id> | Specifies the slot containing the partition for which you want to set the size of the replay window. This parameter is available only if you are logged into the HSM's Admin partition. |
| -size <number_of_packets> | -m <number_of_packets> | Specifies the number of packets in the replay window. Range: 100-1000 Default: 120 |

Example

Current slot

```
lunacm:> stcc rwse -s 500
```

Successfully changed the replay window size for slot 3 to 500 commands.

Specified slot

```
lunacm:> stcc rws -s 4 -s 500
```

Successfully changed the replay window size for slot 4 to 500 commands.

stcconfig replaywindowshow

Display the size of the packet replay window for an STC link. This value specifies the number of packets in the window of sequenced packets that are tracked to provide anti-replay protection.

This command is available only if the current slot is a PPSO partition.

About the Replay Window

All packets sent over the STC link are sequenced and tracked. This allows the receiver to reject old or duplicate packets, thus preventing an attacker from attempting to insert or replay packets on the link. STC employs a sliding window for replay prevention. The receiver remembers which packets it has received within the specified window, and rejects any packets that have already been received or that are older than the oldest packet in the window. Some flexibility is allowed in accepting packets ahead of the sequence window, as valid packets in a short range ahead of the window cause the window to slide forward.



Note: Each STC packet corresponds to a single command. That is, each command sent to the HSM is encapsulated within a single STC packet.

Syntax

stcconfig replaywindowshow [-slot <slot_id>]

| Parameter | Shortcut | Description |
|-----------------|--------------|--|
| -slot <slot_id> | -s <slot_id> | Specifies the slot containing the partition for which you want to display the size of the replay window. This parameter is available only if you are logged into the HSM's Admin partition. |

Example

Current slot

```
lunacm:> stcc rwsh
```

The current replay window size for slot 2 is 120 commands.

Specified slot

```
lunacm:> stcc rwsh
```

The current replay window size for slot 3 is 120 commands.