Luna SA

LunaSH Command Reference Guide

SafeNet

THE
DATA
PROTECTION
COMPANY

Document Information

Product Version	6.0
Document Part Number	007-011136-008
Release Date	29 May 2015

Revision History

Revision	Date	Reason
A	29 May 2015	Initial release.

Trademarks

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.

Note: 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; CISPR22and IEC801. This product satisfies the CLASS B limits of EN 55022.

Disclaimer

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

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

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

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

CONTENTS

PREFACE

About the LunaSH Command Reference Guide

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

- "Using LunaSH" on page 18
- "LunaSH Commands" on page 20

This preface also includes the following information about this document:

- "Customer Release Notes" on page 14
- "Audience" on page 14
- "Document Conventions" on page 14
- "Support Contacts" on page 16

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

Customer Release Notes

The customer release notes (CRN) provide important information about this release that is not included in the customer documentation. It is strongly recommended that you read the CRN to fully understand the capabilities, limitations, and known issues for this release. You can view or download the latest version of the CRN for this release at the following location:

- http://www.securedbysafenet.com/releasenotes/luna/crn_luna_hsm_6-0.pdf

Audience

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

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

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

Document Conventions

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

Notes

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

Note: Take note. Contains important or helpful information.

Cautions

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

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

Warnings

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

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

Command Syntax and Typeface Conventions

Format	Convention
bold	The bold attribute is used to indicate the following: • Command-line commands and options (Type dir /p.) • Button names (Click Save As.) • Check box and radio button names (Select the Print Duplex check box.) • Dialog box titles (On the Protect Document dialog box, click Yes.) • Field names (User Name: Enter the name of the user.) • Menu names (On the File menu, click Save.) (Click Menu > Go To > Folders.) • User input (In the Date box, type April 1.)
italics	In type, the italic attribute is used for emphasis or to indicate a related document. (See the *Installation Guide* for more information.)
<variable>	In command descriptions, angle brackets represent variables. You must substitute a value for command line arguments that are enclosed in angle brackets.
[**optional**] [<optional>]	Represent optional **keywords** or <variables> in a command line description. Optionally enter the keyword or <variable> that is enclosed in square brackets, if it is necessary or desirable to complete the task.

{**a**|**b**|**c**}
{<a>|<b>|<c>}
	Represent required alternate **keywords** or <variables> in a command line description. You must choose one command line argument enclosed within the braces. Choices are separated by vertical (OR) bars.

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

Support Contacts

Contact method	Contact	
Address	SafeNet, Inc. 4690 Millennium Drive Belcamp, Maryland 21017 USA	
Phone	Global	+1 410-931-7520
	Australia	1800.020.183
	China	(86) 10 8851 9191
	France	0825 341000
	Germany	01803 7246269
	India	000.800.100.4290
	Netherlands	0800.022.2996
	New Zealand	0800.440.359
	Portugal	800.1302.029
	Singapore	800.863.499
	Spain	900.938.717
	Sweden	020.791.028
	Switzerland	0800.564.849
	United Kingdom	0800.056.3158
	United States	(800) 545-6608
Web	www.safenet-inc.com	
Support and Downloads	www.safenet-inc.com/support Provides access to the SafeNet Knowledge Base and quick downloads for various products.	
Technical Support Customer Portal	https://serviceportal.safenet-inc.com Existing customers with a Technical Support Customer Portal account can log in	

Contact method	Contact
	to manage incidents, get the latest software upgrades, and access the SafeNet Knowledge Base.

CHAPTER 1

Using LunaSH

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

LunaSH Features

LunaSH provides the following features:

- Command history is supported, using up/down arrows, [Home], [End], [Page Up], [Page Down].
- Command shortnames are supported. You must type sufficient letters of a command or sub-command to make the input unique in the current syntax. For example, you could invoke system syntax help with “help”, “hel”, “he”, but not just “h” (because there is also an "hsm" command and typing just "h" is not sufficient to indicate whether you want "help" or "hsm"). Additionally, for syntax help, the alias “?” is available.
- When the logging function is active, the full name of a command is recorded in the log, not the short version.
- If you supply a short form that is ambiguous, an error message is presented, followed by the list of available commands, sub-commands, or options at the current level.
- Context-sensitive command completion is supported, using [Tab].
- Commands and options are case-insensitive.

Note: Sub-commands do not take a leading dash; options must be typed with a leading single dash. If a command is refused, retry, being careful to type correct syntax. If you are unsure, type the command name followed by a question mark, to force a syntax error and a summary of the proper syntax for that command.

Accessing LunaSH

The Luna Shell (`lunash`) is the command interface for Luna SA.

Connect to the Luna appliance using any ssh-capable communication utility (Windows users can use the provided putty.exe).

When a successful connection is made, a terminal window opens and the prompt "login as:" appears.

For maximum access, type "admin" and press enter.

You are prompted for the admin password. If this is the first time you have connected, the default password is "PASSWORD", and you are required to change it to something more secure.

Once you have logged in, the system presents the Luna Shell prompt, which includes the hostname that you have assigned to your Luna appliance:

[myLuna] lunash:>

You can now issue any `lunash` command. For a summary, type "?" or "help" and press [Enter].

If the admin user has previously created other users, and you know the relevant password, you can log in as a named user instead of "admin".

Seeing More Commands

All of the top-level LunaSH commands (except "exit") have sub-commands and options.

To view a syntax summary of a command, type "help" or "?" followed by the command name. You can also type a command name followed by a space, followed by a character that is unlikely to appear in the sub-commands or options, like "?" or "h".

Exiting LunaSH

Any time you wish to leave your lunash:> session, type "e", "ex", "exi", or "exit" at the prompt and press [Enter]. Your session terminates and the terminal window closes.

To return to lunash:>, you will need to open a new terminal session (with PuTTY.exe or SSH, as appropriate) and login as admin when the "login as:" prompt appears.

CHAPTER 2

LunaSH Commands

This chapter describes the commands available in the Luna SA command shell (lunash). The commands are described in alphabetical order and provide:

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

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

- "audit " on page 21. The audit command menu is available to the authenticated (logged in) Audit user, only.
- "client" on page 51
- "hsm" on page 64
- "htl" on page 165
- "my" on page 174
- "network" on page 187
- "ntls" on page 210
- "package" on page 242
- "partition" on page 249
- "service" on page 291
- "status" on page 298
- "stc" on page 315
- "sysconf" on page 336
- "syslog" on page 455
- "token" on page 472
- "user" on page 528

audit

Access commands that allow the **audit** user to perform HSM auditing tasks.

Note: Audit commands control HSM audit logging. They are visible only to the audit user, and are hidden from the appliance admin, operator, monitor, or any other non-auditor user.

The audit user also has access to a limited set of commands grouped under the following command menus:

hsm	Provides access to the following: • the **hsm show** command. See "hsm show" on page 115. • all **hsm ped** commands, except for the **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. See "hsm ped" on page 98.
my	Provides a set of commands equivalent to those provided to other non-admin users. See "my" on page 174
network	Provides only the **show** and **ping** commands. See "network" on page 187.

Syntax

audit

changepwd
config
init
log
login
logout
remotehost
secret
show
sync

Parameter	Shortcut	Description
changepwd	**-ch**	Changes the audit user password or PED key. See "audit changepwd" on page 23.
config	**-co**	Set the audit parameters. See "audit config " on page 24.
init	**-i**	Initialize the audit role. See "audit init" on page 26.
log	**-log**	Access commands that allow you to manage audit log files. See "audit log" on page 28.
login	**-logi**	Login as the audit user. See "audit login" on page 39
logout	**-logo**	Logout the audit user. See "audit logout " on page 40

Parameter	Shortcut	Description
remotehost	**-r**	Configure audit logging remote hosts. See "audit remotehost" on page 41.
secret	**-se**	Export or import the audit logging secret. See "audit secret" on page 46.
show	**-sh**	Display the current audit logging configuration. See "audit show" on page 49
sync	**-sy**	Synchronizes the HSM time to the host time. See "audit sync" on page 50

audit changepwd

Change the password or PED key contents for the HSM Audit role. Both the old and the new PED key are required for Luna SA with PED authentication.

Syntax

audit changepwd [**-serial** <serialnum>] **[-oldpw** <password>] **[-newpw** <password>]

Parameter	Shortcut	Description
-newpw	**-n**	Specifies the new password for the Audit role. If you do not use this parameter, you are prompted to enter and confirm the password. A valid password should be a mix of upper and lower-case letters, digits, and other characters, and must be a minimum of 8 characters long.
-oldpw	**-o**	Specifies the current password for the HSM Audit role. If you do not use this parameter, you are prompted for the password. This parameter applies to password-authenticated HSMs only.
-serial	**-s**	Specifies the serial number of the HSM. This option allows the system to distinguish between two connected HSMs, as might occur with a PKI bundle configuration (secondary USB-attached Luna G5 HSM).

Example

```
lunash:>audit changepwd

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

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


  Please re-enter the new password:
  > ********


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

audit config

Set the configuration parameters for audit logging.

Syntax

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

Parameter	Shortcut	Description
-parameter	**-p**	Specifies the type of parameter to set. **Valid values** (the value enclosed in parentheses [**n**] indicates a shortcut): • [**e**]**vent** - Include the list of events specified using the **-value** parameter in the log. • [**r**]**otation** - Rotate the logs as specified by the **-value** parameter.
-serial	**-s**	RESERVED FOR FUTURE USE. Specifies the serial number of the HSM. This option allows the system to distinguish between two connected HSMs, as might occur with a PKI bundle configuration (secondary USB-attached Luna G5 HSM).
-value	**-v**	• If **-parameter** is set to **event**, this specifies a comma-separated list of events to include in the log. **Note:** 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. See the examples. **Valid values** (the value enclosed in parentheses [] indicates a shortcut): – **[f]ailure**: log command failures – **[s]uccess**: log command successes – **[a]ccess**: log access attempts (logins) – **[m]anage**: log HSM management (init/reset/etc) – **[k]eymanage**: key management events (key create/delete) – **[u]sage**: key usage (enc/dec/sig/ver) – **fi[r]st**: first key usage only (enc/dec/sig/ver) – **e[x]ternal**: log messages from CA_LogExternal lo[g] manage: log events relating to log configuration a**[l]l**: log everything (user will be warned) [n]one: turn logging off • If **-parameter** is set to **rotation**, this specifies the log rotation interval. **Valid values** (the value enclosed in parentheses [] indicates a shortcut):

Parameter	Shortcut	Description
		– **[h]ourly** – **[d]aily** – **[w]eekly** – **[m]onthly** – **[n]ever**

Example

The following table provides some command usage examples:

Command	Description
audit config -p e -v all	Log everything.
audit config -p e -v none	Log nothing.
audit config -p e -v f	Log all command failures.
audit config -p e -v u,f,s	Log all key usage requests, both success and failure.
audit config -p r -v daily	Rotate the log daily.

The following example shows the warning displayed when you use the **all** option:

```
lunash:>audit config -p e -v all

        Warning:: You have chosen to log all successful key usage events.
        This can result in an extremely high volume of log messages, which
        will significantly degrade the overall performance of the HSM.

Command Result : 0 (Success)
```

audit init

Initialize the Audit role. The **audit init** command is available only to the **audit** user of the HSM appliance and initializes 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-auth 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.

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

Syntax

audit init [**-serial** <serialnum>] [**-domain** <auditdomain>] [**-defaultdomain**] [**-password** <password>] [**-force**]

(Option)	Parameter	Description
-defaultdomain	**-de**	Specifies that the default domain string is to be used as key cloning domain for the HSM. Using the default domain implies that the HSM can be used in HSM Audit Log file validation operations with any other HSM in the world that retains the default domain - retaining the default domain is not recommended. This option is deprecated and will be discontinued in a future release. -defaultdomain and -domain are mutually exclusive -defaultdomain is ignored for PED-authenticated HSMs
-domain	**-do**	Specifies the string to be used as key cloning domain for the HSM. If no value is given for a Luna HSM with Password Authentication, you are prompted interactively. -defaultdomain and -domain are mutually exclusive -domain is ignored for PED-authenticated HSMs
-force	**-f**	Force the action without prompting.
-password	**-p**	Specifies the current password for the HSM Audit role. If you do not use this parameter, you are prompted for the password. This parameter applies to password-authenticated HSMs only.
-serial	**-s**	Specifies the serial number of the HSM. This option allows the system to distinguish between two connected HSMs, as might occur with a PKI bundle configuration (secondary USB-attached Luna G5 HSM).

Example

```
[mypwlunasa] lunash:>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 a domain to use for initializing the Audit role:
  > ********

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

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

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


Command Result : 0 (Success)
```

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 log

Access commands that allow you to manage the audit logs.

Syntax

audit log

clear
list
tail
tarlogs
untarlogs
verify

Parameter	Shortcut	Description
clear	**c**	Clears all of the audit logs from an HSM. See "audit log clear" on page 29.
list	**l**	Lists all of the audit logs on an HSM. See "audit log list" on page 30.
tail	**tai**	Displays the most recent entries in an audit log. See "audit log tail" on page 31.
tarlogs	**tar**	Archives an audit log. See "audit log tarlogs" on page 33
untarlogs	**u**	Unarchives a previously archived audit log. See "audit log untarlogs" on page 34.
verify	**v**	Verifies a set of records within an audit log. See "audit log verify" on page 35.

audit log clear

Clear all of the audit log files from an HSM.

Syntax

audit log clear [**-serial** <serialnum>] [**-force**]

Parameter	Shortcut	Description
-force	**-f**	Force the action without prompting.
-serial	**-s**	Specifies the serial number of the HSM from which you want to clear the logs. This option s required only when there are multiple attached HSMs.

Example

```
lunash:>audit log clear -serial 150718 -f

Log files cleared.

Command Result : 0 (Success)
```

audit log list

Display a list of the audit log files.

Syntax

audit log list [**-serial** <serialnum>]

Parameter	Shortcut	Description
-serial	**-s**	Specifies the serial number of the HSM from which you want to list the logs. This option is required only when there are multiple attached HSMs. Default is the embedded HSM.

Example

```
lunash:>>audit log list

The current log file is:
6872 Dec 17 20:28 hsm_153722_00000001.log

Logs that are ready for archive:
586872 Dec 17 20:58 hsm_153722_00000000.log

Command Result : 0 (Success)
```

audit log tail

Display the last several entries of the named log file, with options to narrow the selection of the displayed entries.

Syntax

audit log tail -file <filename> [**-serial** <serialnum>] [**-entries** <logentries>] [**-search** <string>]

Parameter	Shortcut	Description
-entries	**-e**	Specifies the number of log entries to display.
-file	**-f**	Specifies the name of the log file to view.
-search	**-sea**	Specifies a search string, such that only log entries containing that string are returned, from the named file, and from the specified range of "-entries" within that file (if the "-entries" option is provided - otherwise, the entire file is searched).
-serial	**-ser**	Specifies the serial number of the HSM from which you want to clear the logs. This option s required only when there are multiple attached HSMs.

Example

The following example lists the twenty most recent log entries.

```
[sa5] lunash:>>audit log tail -file hsm_153722_00000000.log -entries 20

1472,12/12/18 02:27:12,S/N 153722 session 2 Access 2147483651:3 SO container operation LUNA_
OPEN_SESSION returned RC_OK(0x00000000) session handle 2
1473,12/12/18 02:27:12,S/N 153722 session 2 Access 2147483651:3 SO container operation LUNA_
CLOSE_SESSION returned RC_OK(0x00000000) session handle 2
1474,12/12/18 02:27:32,S/N 153722 session 2 Access 2147483651:3 SO container operation LUNA_
OPEN_SESSION returned RC_OK(0x00000000) session handle 2
1475,12/12/18 02:27:32,S/N 153722 session 2 Access 2147483651:3 SO container operation LUNA_
CLOSE_SESSION returned RC_OK(0x00000000) session handle 2
1476,12/12/18 02:27:47,S/N 153722 session 2 Access 2147483651:3 SO container operation LUNA_
OPEN_SESSION returned RC_OK(0x00000000) session handle 2
1477,12/12/18 02:27:52,S/N 153722 session 2 Access 2147483651:3 SO container operation LUNA_
CLOSE_SESSION returned RC_OK(0x00000000) session handle 2
1478,12/12/18 02:28:07,S/N 153722 session 2 Access 2147483651:3 SO container operation LUNA_
OPEN_SESSION returned RC_OK(0x00000000) session handle 2
1479,12/12/18 02:28:07,S/N 153722 session 2 Access 2147483651:3 SO container operation LUNA_
CLOSE_SESSION returned RC_OK(0x00000000) session handle 2
1480,12/12/18 02:28:27,S/N 153722 session 2 Access 2147483651:3 SO container operation LUNA_
OPEN_SESSION returned RC_OK(0x00000000) session handle 2
1481,12/12/18 02:28:27,S/N 153722 session 2 Access 2147483651:3 SO container operation LUNA_
CLOSE_SESSION returned RC_OK(0x00000000) session handle 2
1482,12/12/18 02:28:47,S/N 153722 session 2 Access 2147483651:3 SO container operation LUNA_
OPEN_SESSION returned RC_OK(0x00000000) session handle 2
1483,12/12/18 02:28:47,S/N 153722 session 2 Access 2147483651:3 SO container operation LUNA_
CLOSE_SESSION returned RC_OK(0x00000000) session handle 2
1484,12/12/18 02:29:02,S/N 153722 session 2 Access 2147483651:3 SO container operation LUNA_
```

```
OPEN_SESSION returned RC_OK(0x00000000) session handle 2
1485,12/12/18 02:29:02,S/N 153722 session 2 Access 2147483651:3 SO container operation LUNA_
CLOSE_SESSION returned RC_OK(0x00000000) session handle 2
1486,12/12/18 02:29:22,S/N 153722 session 2 Access 2147483651:3 SO container operation LUNA_
OPEN_SESSION returned RC_OK(0x00000000) session handle 2
1487,12/12/18 02:29:22,S/N 153722 session 2 Access 2147483651:3 SO container operation LUNA_
CLOSE_SESSION returned RC_OK(0x00000000) session handle 2
1488,12/12/18 02:29:42,S/N 153722 session 2 Access 2147483651:3 SO container operation LUNA_
OPEN_SESSION returned RC_OK(0x00000000) session handle 2
1489,12/12/18 02:29:42,S/N 153722 session 2 Access 2147483651:3 SO container operation LUNA_
CLOSE_SESSION returned RC_OK(0x00000000) session handle 2
1490,12/12/18 02:29:47,S/N 153722 session 2 Access 2147483651:22817 SO container operation LUNA_
OPEN_SESSION returned RC_OK(0x00000000) session handle 2
1491,12/12/18 02:29:47,S/N 153722 session 2 Access 2147483651:22817 SO container operation LUNA_
CLOSE_SESSION returned RC_OK(0x00000000) session handle 2

Command Result : 0 (Success)
```

The following example lists only those entries that contain the string "OPEN_SESSION", within the twenty most recent entries in the log.

```
[sa5] lunash:>>audit log tail -file hsm_153722_00000000.log -entries 20 -search OPEN_SESSION

1492,12/12/18 02:29:57,S/N 153722 session 2 Access 2147483651:3 SO container operation LUNA_
OPEN_SESSION returned RC_OK(0x00000000) session handle 2
1494,12/12/18 02:30:17,S/N 153722 session 2 Access 2147483651:3 SO container operation LUNA_
OPEN_SESSION returned RC_OK(0x00000000) session handle 2
1496,12/12/18 02:30:37,S/N 153722 session 2 Access 2147483651:3 SO container operation LUNA_
OPEN_SESSION returned RC_OK(0x00000000) session handle 2
1498,12/12/18 02:30:57,S/N 153722 session 2 Access 2147483651:3 SO container operation LUNA_
OPEN_SESSION returned RC_OK(0x00000000) session handle 2
1500,12/12/18 02:31:12,S/N 153722 session 2 Access 2147483651:3 SO container operation LUNA_
OPEN_SESSION returned RC_OK(0x00000000) session handle 2
1502,12/12/18 02:31:32,S/N 153722 session 2 Access 2147483651:3 SO container operation LUNA_
OPEN_SESSION returned RC_OK(0x00000000) session handle 2
1504,12/12/18 02:31:52,S/N 153722 session 2 Access 2147483651:3 SO container operation LUNA_
OPEN_SESSION returned RC_OK(0x00000000) session handle 2
1506,12/12/18 02:32:12,S/N 153722 session 2 Access 2147483651:3 SO container operation LUNA_
OPEN_SESSION returned RC_OK(0x00000000) session handle 2
1508,12/12/18 02:32:27,S/N 153722 session 2 Access 2147483651:3 SO container operation LUNA_
OPEN_SESSION returned RC_OK(0x00000000) session handle 2
1510,12/12/18 02:32:27,S/N 153722 session 2 Access 2147483651:22817 SO container operation LUNA_
OPEN_SESSION returned RC_OK(0x00000000) session handle 2

Command Result : 0 (Success)
[sa5] lunash:>
```

audit log tarlogs

Archives log files to audit.tgz file in the user local directory.

Syntax

audit log tarlogs [**-serial** <serialnum>]

Parameter	Shortcut	Description
-serial	**-s**	Specifies the serial number of the HSM from which you want to clear the logs. This option is required only when there are multiple attached HSMs.The default is to use the embedded HSM.

Example

```
lunash:>audit log tarlogs -serial 153593
Compressing log files:

153593/
153593/hsm_153593_0000000a.log
153593/ready_for_archive/
153593/ready_for_archive/hsm_153593_00000003.log
153593/ready_for_archive/hsm_153593_00000002.log
153593/ready_for_archive/hsm_153593_00000007.log
153593/ready_for_archive/hsm_153593_00000005.log
153593/ready_for_archive/hsm_153593_00000004.log
153593/ready_for_archive/hsm_153593_00000009.log
153593/ready_for_archive/hsm_153593_00000008.log
153593/ready_for_archive/hsm_153593_00000006.log
153593/ready_for_archive/hsm_153593_00000001.log


Command Result : 0 (Success)
```

audit log untarlogs

Un-archives a previously archived log file to the local directory. The log file is restored to a subdirectory named with the HSM's serial number.

Syntax

audit log untarlogs [**-file** <logfilename>]

Parameter	Shortcut	Description
-file	**-f**	Specifies the name of the archived log file to restore.

Example

```
[mylunasa] lunash:>audit log untarlogs -file x.tgz

Cannot find the file in /home/audit/lush_files/
Found files:
153593.lws  audit-153593.tgz

Command Result : 65535 (Luna Shell execution)
[mylunasa] lunash:>audit log untarlogs -file audit-153593.tgz

Extracting logs to audit home:

153593/
153593/hsm_153593_0000000a.log
153593/ready_for_archive/
153593/ready_for_archive/hsm_153593_00000003.log
153593/ready_for_archive/hsm_153593_00000002.log
153593/ready_for_archive/hsm_153593_00000007.log
153593/ready_for_archive/hsm_153593_00000005.log
153593/ready_for_archive/hsm_153593_00000004.log
153593/ready_for_archive/hsm_153593_00000009.log
153593/ready_for_archive/hsm_153593_00000008.log
153593/ready_for_archive/hsm_153593_00000006.log
153593/ready_for_archive/hsm_153593_00000001.log

To verify these logs see the 'audit secret import' command to import the HSM's
log secret.

Command Result : 0 (Success)
```

audit log verify

Verify the audit log records.

Syntax

audit log verify -file <filename> [**-serialtarget** <serialnum>] [**-serialsource** <serialnum>] [**-start** <number>] [**-end** <number>] [**-external**]

Parameter	Shortcut	Description
-end	**-en**	Specifies the final record of the subset of records to be verified from the file.
-external	**-ex**	Specifies that the file from which log entries are to be verified is from an external HSM. In this case, the audit secret for that HSM must either be the same secret (white PED Key) as is used on the current HSM, or must have been imported to the current HSM. The current HSM's own audit secret cannot verify log files from other HSMs if those were created using independent secrets. The HSM holds only one audit secret at a time, so the secret for the relevant HSM's logs must be brought into the HSM when needed for log verification, if it is not already present.
-file	**-f**	Specifies the name of the log file to verify.
-serialsource	**-serials**	Specifies the serial number of the HSM that generated the log file that is being verified.
-serialtarget	**-serialt**	Specifies the serial number of the HSM that is performing the verification.
-start	**-st**	Specifies the starting record of the subset of records to be verified from the file.

Example

Verification of my own log file, with my own secret

```
lunash:>audit log verify -f hsm_150073_00000011.log

Log file being verified hsm_150073_00000011.log.

Verifying log on HSM with serial 150073

Verified messages 236 to 236

Command Result : 0 (Success)
```

Attempted verification of external log, with my own secret

```
lunash:>audit log verify -f hsm_100548_000004a3.log

Log file being verified /home/audit/lush_files/hsm_100548_000004a3.log.

Verifying log from HSM with serial 150073 on HSM with serial 150073
Make sure that you have already imported the audit log secret.

Verify failed on record 10760271

If you have imported a log secret from another HSM please export then re-import
your own log secret. For security reasons it is not possible to verify logs
using two difference secrets at the same time. One or more messages did not verify.

The audit sub-command failed. (LUNA_RET_LOG_BAD_RECORD_HMAC)

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

Verification of external log with external secret:

In this example, we show the process from both HSMs.

```
[myluna72] lunash:> audit secret export

The encrypted log secret file 153593.lws now available for scp.

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

Command Result : 0 (Success)
[myluna72] lunash:>audit log tar


Compressing log files:

153593/
153593/hsm_153593_00000019.log
153593/153593.lws
153593/ready_for_archive/
153593/ready_for_archive/hsm_153593_0000000b.log
153593/ready_for_archive/hsm_153593_00000003.log
153593/ready_for_archive/hsm_153593_00000002.log
153593/ready_for_archive/hsm_153593_00000011.log
153593/ready_for_archive/hsm_153593_00000010.log
153593/ready_for_archive/hsm_153593_00000007.log
153593/ready_for_archive/hsm_153593_00000005.log
153593/ready_for_archive/hsm_153593_00000004.log
153593/ready_for_archive/hsm_153593_00000016.log
153593/ready_for_archive/hsm_153593_0000000a.log
153593/ready_for_archive/hsm_153593_0000000d.log
153593/ready_for_archive/hsm_153593_00000009.log
153593/ready_for_archive/hsm_153593_00000008.log
153593/ready_for_archive/hsm_153593_00000013.log
153593/ready_for_archive/hsm_153593_0000000f.log
153593/ready_for_archive/hsm_153593_00000014.log
153593/ready_for_archive/hsm_153593_00000015.log
153593/ready_for_archive/hsm_153593_00000018.log
```

```
153593/ready_for_archive/hsm_153593_0000000c.log
153593/ready_for_archive/hsm_153593_0000000e.log
153593/ready_for_archive/hsm_153593_00000012.log
153593/ready_for_archive/hsm_153593_00000017.log
153593/ready_for_archive/hsm_153593_00000006.log
153593/ready_for_archive/hsm_153593_00000001.log

The tar file containing logs is now available as file 'audit-153593.tgz'.
If you wish to verify your logs on another SA, scp them to another SA's audit
directory then use the 'audit log untar' command.

Command Result : 0 (Success)
```

Here is where we scp the secret file and the .tgz file to a different Luna SA

```
lunash:> audit secret import -serialtarget 150825 -file 153593.lws -serialsource 153593

Successfully imported the encrypted log secret 153593.lws

Now that you have imported a log secret if you wish to verify
your logs please see the 'audit log verify' command.

Command Result : 0 (Success)
[myluna73] lunash:> audit log untarlogs -file audit-153593.tgz

Extracting logs to audit home:

153593/
153593/hsm_153593_00000019.log
153593/153593.lws
153593/ready_for_archive/
153593/ready_for_archive/hsm_153593_0000000b.log
153593/ready_for_archive/hsm_153593_00000003.log
153593/ready_for_archive/hsm_153593_00000002.log
153593/ready_for_archive/hsm_153593_00000011.log
153593/ready_for_archive/hsm_153593_00000010.log
153593/ready_for_archive/hsm_153593_00000007.log
153593/ready_for_archive/hsm_153593_00000005.log
153593/ready_for_archive/hsm_153593_00000004.log
153593/ready_for_archive/hsm_153593_00000016.log
153593/ready_for_archive/hsm_153593_0000000a.log
153593/ready_for_archive/hsm_153593_0000000d.log
153593/ready_for_archive/hsm_153593_00000009.log
153593/ready_for_archive/hsm_153593_00000008.log
153593/ready_for_archive/hsm_153593_00000013.log
153593/ready_for_archive/hsm_153593_0000000f.log
153593/ready_for_archive/hsm_153593_00000014.log
153593/ready_for_archive/hsm_153593_00000015.log
153593/ready_for_archive/hsm_153593_00000018.log
153593/ready_for_archive/hsm_153593_0000000c.log
153593/ready_for_archive/hsm_153593_0000000e.log
153593/ready_for_archive/hsm_153593_00000012.log
153593/ready_for_archive/hsm_153593_00000017.log
153593/ready_for_archive/hsm_153593_00000006.log
153593/ready_for_archive/hsm_153593_00000001.log

To verify these logs see the 'audit secret import' command to import the HSM's
log secret.
```

```
Command Result : 0 (Success)
[myluna73] lunash:> audit log verify -serialtarget 150825 -file hsm_153593_00000001.log -seri-
alsource 153593


Log file being verified /home/audit/lush_files/153593/ready_for_archive/hsm_153593_00000001.log.

Verifying log from HSM with serial 153593 on HSM with serial 150825
 Make sure that you have already imported the audit log secret.

Verified messages 39638 to 39641

Command Result : 0 (Success)
[myluna73]
```

On the verifying HSM ([myluna73] in the example), you just imported a secret (displacing the native secret of the local HSM) and used it to verify logs that were transported from a different HSM ([myluna**72**] in the example).

If you now wished to verify the second HSM's ([myluna73]) own log files, you would need to re-import that HSM's secret, having replaced it with the other HSM's ([myluna72]'s0 secret for the example operation.

That is, [myluna72]'s log secret that was imported into [myluna73] to allow [myluna73] to verify logs received from [myluna72], is not useful to verify [myluna73]'s own logs. An HSM can have only one log secret at a time, so [myluna73] needs its own secret back if it is to verify its own logs, rather than the logs it received from [myluna72].

Attempted Verification of local log with external secret:

```
[myluna] lunash:>audit log verify -f hsm_150073_00000011.log

Log file being verified hsm_150073_00000011.log.

Verifying log on HSM with serial 150073

Verify failed on record 236

If you have imported a log secret from another HSM please export then re-import
your own log secret. For security reasons it is not possible to verify logs
using two difference secrets at the same time. One or more messages did not verify.
The log file you specified was either open by the logger daemon, or was
improperly terminated.  If the file was open by the logger daemon, the
content of it may have changed as the result of new messages being logged.
In this case, running the query again will succeed.

The audit sub-command failed. (LUNA_RET_LOG_BAD_RECORD_HMAC)


Command Result : 65535 (Luna Shell execution)
[myluna] lunash:>
```

audit login

Log in the HSM Audit user.

For Luna SA with PED (Trusted Path) Authentication, a new Audit secret is created on the HSM and imprinted on a white PED Key, or an existing Audit secret is retrieved from a presented white PED Key and imprinted onto the HSM. After initialization, the appropriate white PED Key is needed for HSM Audit role login.

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 multiple HSMs (for example a Backup HSM or a Luna G5 HSM locally connected to your host).
-password	-p <password>	The password of the HSM you are logging into. Used for Password-authenticated HSMs. If you prefer not to write the password, in the clear, on the command line, leave it out and you are prompted for it. Ignored for PED-authenticated HSMs. If the audit log area in the HSM becomes full, the HSM stops accepting most commands, and does not prompt for password when login is requested. In that case, provide the password with the command, and the login is accepted. Audit log full does not affect login for PED-auth HSMs.

Example

PED-Authenticated HSM

```
lunash:>audit login

Luna PED operation required to login as HSM Auditor - use Audit user (white) PED key.

'audit

lunash:>
```

Password authenticated HSM

```
lunash:>audit login

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

Command Result : 0 (Success)
```

audit logout

Log out the HSM Audit user.

Syntax

audit logout

Example

```
lunash:>audit logout

'audit logout' successful.
Command Result : 0 (Success)
```

audit remotehost

Access commands that allow you to add, delete, or view the remote logging servers.

Syntax

audit remotehost

> **add**
> **clear**
> **delete**
> **list**

Parameter	Shortcut	Description
add	**a**	Adds a Remote Logging Server. See "audit remotehost add" on page 42.
clear	**c**	Deletes all Remote Logging Servers. See "audit remotehost clear" on page 43.
delete	**d**	Delete a Remote Logging Server. See "audit remotehost delete" on page 44.
list	**l**	Display a list of all currently configured Remote Logging Servers. See "audit remotehost list" on page 45.

audit remotehost add

Add an identified Remote Logging Server.

Syntax

audit remotehost add -host <hostnameoripaddress> [**-protocol** <protocol>] [**-port** <port>]

Parameter	Shortcut	Description
-host	**-h**	Specifies the Remote Logging Server Host Name or IP address.
-port	**-po**	Specifies the server port to use for the Remote Logging Server. Range: 0 to 65535 Default: 514.
-protocol	**-pr**	Specifies the protocol for remote logging with the specified server. Valid values: tcp, udp Default: udp

Example

```
lunash:>audit remotehost add -host myloggingshost -protocol tcp -port 1660
Remote logging server added.

Shutting down kernel logger:                                [  OK  ]
Shutting down system logger:                                [  OK  ]
Starting system logger:                                     [  OK  ]
Starting kernel logger:                                     [  OK  ]
Saving firewall rules to /etc/sysconfig/iptables:           [  OK  ]

Command Result : 0 (Success)
```

audit remotehost clear

Delete all of the currently configured Remote Logging Servers.

Syntax

audit remotehost clear [**-force**]

Parameter	Shortcut	Description
-force	**-f**	Force the action without prompting.

Example

With the -force option

```
lunash:>audit remotehost clear -f

Shutting down kernel logger:                               [  OK  ]
Shutting down system logger:                               [  OK  ]
Starting system logger:                                    [  OK  ]
Starting kernel logger:                                    [  OK  ]

Command Result : 0 (Success)
[myluna] lunash:>
```

Without the -force option

```
[myluna] lunash:>audit remotehost clear

        All remote hosts receiving the audit logs will be deleted.
        Are you sure you wish to continue?

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

Shutting down kernel logger:                               [  OK  ]
Shutting down system logger:                               [  OK  ]
Starting system logger:                                    [  OK  ]
Starting kernel logger:                                    [  OK  ]

Command Result : 0 (Success)
```

audit remotehost delete

Delete an identified remote logging server.

Syntax

audit remotehost delete -host <hostnameoripaddress>

Parameter	Shortcut	Description
-host	**-h**	Specifies the host name or IP address of the remote logging server.

Example

```
[myluna] lunash:>audit remotehost delete -host myotherluna

Shutting down kernel logger:                               [  OK  ]
Shutting down system logger:                               [  OK  ]
Starting system logger:                                    [  OK  ]
Starting kernel logger:                                    [  OK  ]

Command Result : 0 (Success)
```

audit remotehost list

Display a list of the currently configured remote logging servers.

Syntax

audit remotehost list

Example

```
lunash:>audit remotehost list

Remote logging server(s):
=========================

  172.20.10.201:514, udp

Command Result : 0 (Success)
```

audit secret

Access commands that allow you to import or export the audit logging secret.

Syntax

audit secret

> **export**
> **import**

Parameter	Shortcut	Description
export	**e**	Export the audit logging secret. See "audit secret export" on page 47
import	**i**	Import the audit logging secret. See "audit secret import" on page 48.

audit secret export

Export the audit logging secret to the user's local directory and log archive directory. This is the secret that can later be used to verify log files and log records produced by the HSM identified by the serial number provided with this command.

Syntax

audit secret export [**-serial** <serialnum>]

Parameter	Shortcut	Description
-serial	**-s**	Specifies the serial number of the HSM whose logging secret you want to export. The default is to use the embedded HSM.

Example

```
lunash:>audit secret export -serial 150718

The encrypted log secret file 150718.lws now available for scp.

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

Command Result : 0 (Success)
```

audit secret import

Imports the audit logging secret from another HSM, in order to verify log records and log files from that other HSM. The logging secret must first have been exported from the originating (source) HSM using the audit secret export command, and the resulting audit-secret file transported to the location/host of the current (target) HSM.

Syntax

audit secret import -serialtarget <serialnum> **-serialsource** <serialnum> **-file** <filename>

Parameter	Shortcut	Description
-file	**-f**	Specifies the name of the audit secret file to import.
-serialsource	**-serials**	Specifies the serial number of the source HSM from which the logging secret was exported.
-serialtarget	**-serialt**	Specifies the serial number of the target HSM to which the logging secret will be imported.

Example

```
lunash:>audit secret import -serialt 150719 -serials 150718 -file 150718.lws

Command Result : 0 (Success)
```

audit show

Display the current audit logging information. The displayed information varies, depending on whether or not the 'audit' role is logged in.

Syntax

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

Parameter	Shortcut	Description
-serial	**-s**	Specifies the serial number of the HSM whose audit logging information you want to display. The default is to use the embedded HSM.

Example

```
lunash:>audit show

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 sync

Synchronize the HSM time to the host time.

Any computer's onboard time is subject to drift. This command causes the HSM to adjust its time to match that of the host computer (such as the Luna SA appliance). 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 sync

Example

```
lunash:>audit sync

Command Result : 0 (Success)
```

client

Access commands that allow you to manage the Luna clients that are able to use partitions on the appliance.

Syntax

client

assignpartition
delete
fingerprint
hostip
list
register
revokepartition
show

Parameter	Shortcut	Description
assignpartition	**a**	Assign partition access rights to a client. See "client assignpartition" on page 52.
delete	**d**	Delete a client. See "client delete" on page 53.
fingerprint	**f**	Display the certificate fingerprint for a registered client. See "client fingerprint" on page 54.
hostip	**h**	Display or configure the client-to-IP mapping. See "client hostip" on page 55.
list	**l**	Display a list of the registered clients by client name. See "client list" on page 59.
register	**reg**	Add a client to the list of clients that can access the Luna appliance's NTLS. See "client register" on page 60.
revokepartition	**rev**	Revoke access privileges to the specified partition from the specified client. See "client revokepartition" on page 62.
show	**s**	Display the hostname or IP address of a client, and any partitions assigned to the client. See "client show" on page 63.

client assignpartition

Assign access privileges for a registered client to the specified partitions. To assign a partition to a client, the client must be registered using the **client register** command and the partition must first be created using the **partition create** command.

This command is issued by the Luna appliance admin user.

Partitions can be 'unassigned' via revocation (**client revokePartition**), deletion of a Client association (**client delete**), deletion of the partition from the HSM (**partition delete**), or reinitialization of the HSM (**hsm init**).

Syntax

client assignpartition -client <clientname> **-partition** <name>

Parameter	Shortcut	Description
-client	**-c**	Specifies the name of the client to which a partition will be assigned. Use the **client list** command to display a list of registered clients,
-partition	**-p**	Specifies the name of the partition to which the client will gain access. Use the **partition list** command to obtain the partition name. Or if you are attempting to make a deployed token available to a client, use **token pki listDeployed** to see labels of deployed PKI tokens.

Example

```
 lunash:>client assignPartition -client myPC -partition myPartition2

'client assignPartition' successful.

Command Result : 0 (Success)
```

client delete

Remove a client from the list of clients registered to use the Luna appliance. The command requires user interaction to verify that deletion should occur. This can be overridden with the **-force** option.

Syntax

client delete -client <clientname> [**-force**]

Parameter	Shortcut	Description
-client	**-c**	Specifies the name of the client to delete. Use the **client list** command to display a list of registered clients,
-force	**-f**	Force the action without prompting.

Example

```
lunash:>client delete -client myPC

CAUTION:  Are you sure you wish to delete client named: myPC
Type 'proceed' to delete the client, or 'quit' to quit now.
> proceed
'client delete' successful.

Command Result : 0 (Success)
```

client fingerprint

Display the certificate fingerprint for a registered client. Compare this with the client's known certificate fingerprint to verify that the correct client was registered before assigning partitions to the client.

This command is executed by the (Luna appliance) admin.

Syntax

client fingerprint -client <clientname>

Parameter	Shortcut	Description
-client	**-c**	Specifies the name of the client whose certificate you want to display. Use the **client list** command to display a list of registered clients,

Example

```
lunash:> client -fingerprint -client myPC

Certificate fingerprint: D4:0F:8E:4C:CC:F2:49:FA:B7:3E:07:CB:0B:AE:1E:42

Command Result : 0 (Success)
```

client hostip

Access commands that allow you to display or configure the client-to-IP mapping.

Syntax

client hostip

map
show
unmap

Parameter	Shortcut	Description
map	**m**	Map a client to an IP address. See "client hostip map" on page 56.
show	**s**	Display the current client-to-IP mapping. See "client hostip show" on page 57.
unmap	**u**	Remove a client-to-IP mapping. See "client hostip unmap" on page 58.

client hostip map

Create an association between a client name and an IP address.

Syntax

client hostip map -clientname <client_name> **-ipaddress** <ip_address>

Parameter	Shortcut	Description
-clientname	-c	Specifies the name of the client for which you want to create the association.
-ipaddress	-i	Specifies the IP address of the client for which you want to create the association.

Example

```
lunash:>client hostip map -c myPC -i 168.10.10.254

Command Result : 0 (Success)
```

client hostip show

Display the current client-to-IP mapping.

Syntax

client hostip show

Example

```
lunash:>client hostip show

Client Name                 Host Name                 Host IP
----------------------------------------------------------------------
myPC                        myPC                      168.10.10.254

Command Result : 0 (Success)
```

client hostip unmap

Remove an association between a client name and an IP address.

Syntax

client hostip unmap <clientname>

Parameter	Shortcut	Description
<clientname>		Specifies the name of the client for which you want to remove the association . Use the **client list** command to display a list of registered clients,

Example

```
lunash:>client hostip unmap myPC

Command Result : 0 (Success)
```

client list

Display a list of the registered clients by client name.

Syntax

client list

Example

```
lunash:> client list

registered client 1: brigitte
registered client 2: suzanne
registered client 3: pierre
registered client 4: dan
```

client register

Add a client to the list of clients that can access the Luna appliance's NTLS. A client must be registered before you can assign partitions to it.

Note: The client's certificate file is needed to perform the registration.

Syntax

client register -client <clientname> [**-hostname** <hostname>] [**-ip** <ipaddress>] [**-requirehtl**] [**-ottexpiry** <seconds>] [**-generateott**] [**-force**]

Parameter	Shortcut	Description
-client	**-c**	The new client's name. The user may choose any name, so long as it is less than 255 characters, and is unique among all clients on the Luna HSM appliance. The client name need not be the hostname of the client.
-force	**-f**	Force the action without prompting.
-generateott	**-g**	Specifies creation of a one-time token as the client is registered. The name of the created file is the client name that you provided (above). Requires the -requirehtl option. Selecting this option is the equivalent of running the command **htl generateott -client** <clientname>.
-hostname	**-h**	The hostname of the new client. Use this parameter if the client certificate (and server certificates) were created with hostnames. If the certificates were created with IP addresses, use the **-ip** parameter instead.
-ip	**-i**	The IP address of the new client. Use this parameter if the client certificate (and server certificates) were created with IP addresses. If the certificates were created with hostnames, use the **-hostname** parameter instead.
-ottexpiry	**-o**	Sets the time, in seconds, before a one-time token (OTT) expires (values can be positive integers in the range of 0-to-3600 seconds). For practical reasons, you must allow at least enough time for certificate transfer, or the OTT could expire before it is ready to use. Requires the -requireHtl option. If the -ottExpiry option is not specified, the system-default OTT expiry for that client is used.
-requirehtl	**-r**	Specifies that the HTL protocol is required for all interactions between this client and the HSM appliance.

Example

```
lunash:>client register -c someclient -h someclient -r -g -f

Force option used. All proceed prompts bypassed.
'client register' successful.
Generating one-time token...
One-time token for client someclient is ready to use.
Filename is someclient.ott
```

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

client revokepartition

Revoke access privileges to the specified partition from the specified client. Obtain a list of clients and the partitions they have access to using the **client -list** and **client -show** commands.

This command is executed by the (Luna appliance) admin.

Syntax

client revokepartition -client <name> **-partition** <partitionname>

Parameter	Shortcut	Description
-client	**-c**	Specifies the name of the client from which the partition will be revoked. Use the **client list** command to display a list of registered clients,
-partition	**-p**	Specifies the name of the partition to which the client will lose access. Use the **partition list** command to display a list of partitions.

Example

```
lunash:> client -revokePartition -client dan -partition test1

'client -revokePartition' successful.
```

client show

Display the hostname or IP address of a client, and any partitions assigned to the client.

Syntax

client show -client <name>

Parameter	Shortcut	Description
-client	**-c**	Specifies the name of the client for which you want to see additional information. Use the **client list** command to display a list of registered clients,

Example

Without DNS

```
lunash:> client -show -client myclient

ClientID: myclient
IPAddress:    121.22.35.4
HTL Required: yes
OTT Expiry: 160 sec (default)
Partitions: "mypart1"
```

With DNS

```
lunash:> client -show -client suzanne

ClientID: myclient
Hostname: myclient.sfnt.local
HTL Required: yes
OTT Expiry: 160 sec (default)
Partitions: "mypart1"
```

hsm

Access commands that allow you to manage the HSM on the appliance.

> **Note:** HSM commands from the Luna shell are queued along with other demands on the HSM (such as cryptographic operations), and can run more slowly than normal if the HSM is very busy, such as when it is performing high-volume ECDSA signing operations.

Syntax

hsm

backup
changepolicy
changepw
checkcertificates
debug
displaylicenses
factoryreset
firmware
fwupdateinfo
generatedak
information
init
loadcustomercert
login
logout
ped
restore
selftest
setlegacydomain
show
showpolicies
srk
stc
supportinfo
update
zeroize

Parameter	Shortcut	Description
backup	**b**	Backs up data or objects in the HSM's SO (or HSM Admin) space, such as the HSM's masking key (used in SIM) information, to a backup token. See "hsm backup" on page 67.
changepolicy	**changepo**	Sets a policy on or off, or to set it to a certain value if it is a numerical policy. See "hsm changepolicy" on page 69.
changepw	**changepw**	Changes the password or PED key contents for the HSM Admin. See "hsm changepw" on page 70.

Parameter	Shortcut	Description
checkcertificates	**che**	Checks the HSM for presence of MAC and DAC. See "hsm checkcertificates" on page 71.
debug	**de**	Display debug information. See "hsm debug show" on page 72.
displaylicenses	**di**	Display a list of all licenses on the HSM. See "hsm displaylicenses" on page 73.
factoryreset	**fa**	Set the HSM back to its factory default settings. Zeroize partitions, roles, and objects, delete the RPV (if any), and reset partition policies to original settings. See "hsm factoryreset" on page 75.
firmware	**fi**	Update or rollback the HSM firmware. See "hsm firmware" on page 77 .
fwupdateinfo	**fw**	Saves HSM firmware update support information to a file. See "hsm fwupdateinfo" on page 84.
generatedak	**ge**	Generate a new DAK pair. See "hsm generatedak" on page 85.
information	**inf**	Display HSM information, reset the HSM counters, or monitor HSM performance. see "hsm information" on page 86.
init	**ini**	Initialize the HSM. See "hsm init" on page 92.
loadcustomercert	**loa**	Load the customer-signed MAC and DAC. See "hsm loadcustomercert" on page 95.
login	**logi**	Log in as the HSM Admin. See "hsm login" on page 96.
logout	**logo**	Log out the HSM Admin account. See "hsm logout" on page 97.
ped	**p**	Display or change the configuration of the PED. See "hsm ped" on page 98.
restore	**r**	Restore the contents of the HSM from a backup token. See "hsm restore [reserved]" on page 112.
selftest	**sel**	Test the cryptographic capabilities of the HSM. See "hsm selftest" on page 113.
setlegacydomain	**set**	Set the legacy cloning domain on an HSM. See "hsm setlegacydomain" on page 114
show	**sh**	Display a list showing the current configuration of the HSM. See "hsm show" on page 115.
showpolicies	**showp**	Display the current settings for all hsm capabilities and policies, or optionally restrict the listing to only the policies that are configurable. See "hsm showpolicies" on page 117.
srk	**sr**	Configure, or display information about, secure recovery keys

Parameter	Shortcut	Description
		(SRK) and secure transport mode. See "hsm srk" on page 119.
stc	**st**	Configure and manage the secure trusted channel (STC) link that is local to the appliance, that is, from the LunaSH shell to the HSM SO partition. See "hsm stc" on page 129.
supportinfo	**su**	Get HSM support information. See "hsm supportinfo" on page 159.
update	**u**	Display or install any available capability or firmware updates. See "hsm update " on page 160.
zeroize	**z**	Zeroize the HSM. Destroy all partitions, roles and objects, but preserve the RPV (if one exists) and preserve HSM policy settings. See "hsm zeroize" on page 163.

hsm backup

Backup data or objects in the HSM's SO (or HSM Admin) space, such as the HSM's masking key (used in SIM) information, to a backup token. The **hsm backup** command copies crucial HSM backup information to a special SafeNet backup device. The connected backup HSM, indicated by its serial number, is initialized and used during this process. The user is prompted to confirm that this destructive command should continue ("destructive" to any contents currently on the backup device, not destructive to the source HSM).

The hsm backup command backs up only data or objects in the HSM's SO (or HSM Admin) space. It does not back up the partition data. For that, you must use the **partition backup** commands.

Dual mode backup tokens are initialized to the same level (Luna HSM with Password Authentication **or** Luna HSM with PED (Trusted Path) Authentication) as the HSM.

When labeling HSMs or partitions, never use a numeral as the first, or only, character in the name/label. Token backup commands allow slot-number OR label as identifier which can lead to confusion if the label is a string version of a slot number.

For example, if the token is initialized with the label "1" then the user cannot use the label to identify the target for purposes of backup, because VTL parses "1" as signifying the numeric ID of the first slot rather than as a text label for the target in whatever slot it really occupies (the target is unlikely to be in the first slot), so backup fails.

Syntax

hsm backup -serial <serialnumber> [**-password** <password>] [**-tokenAdminPw** <password>] [**-force**]

Parameter	Shortcut	Description
-serial	**-s**	Specifies the serial number of the target backup HSM. This indicates which backup device to work with.
-password	**-p**	Specifies the source HSM Admin's (or SO's) text password. This parameter is required on password-authenticated HSMs. It is ignored on PED-authenticated HSMs.
-tokenAdminPw	**-t**	Specifies the password of the backup target HSM. On PED-authenticated HSMs, the Luna PED is used for the PIN and this value is ignored. The token password need not be the same password or PED key as used for the HSM partition.
-force	**-f**	Force the action without prompting.

Example

```
lunash:>hsm backup -serial 667788

CAUTION:  Are you sure you wish to initialize the backup
    token named:
      no label
    Type 'proceed' to continue, or 'quit' to quit now.
    >  proceed
Luna PED operation required to initialize backup token - use Security Officer (blue) PED key.
Luna PED operation required to login to backup token - use Security Officer (blue) PED key.
Luna PED operation required to generate cloning domain on backup token - use Domain (red) PED
key.
Luna PED operation required to login as HSM Administrator - use Security Officer (blue) PED key.

Luna PED operation required to login to backup token - use Security Officer (blue) PED key.
'hsm backup' successful.

Command Result : 0 (Success)
```

hsm changepolicy

Change HSM Admin-modifiable elements from the HSM policy set. Use this command to set a policy on or off, or to set it to a certain value if it is a numerical policy. Only certain portions of the policy set are user-modifiable. These policies and their current values can be determined using the hsm showPolicies command. After a successful policy change, the command displays the new policy value.

Note: This command must be executed by the HSM Admin. If the HSM Admin is not authenticated, a “user not logged in” error message is returned.

If the policy is destructive, the user is given the choice to proceed or quit. Once a policy is changed, the program reports back the new value of the policy.

Syntax

hsm changePolicy -policy <hsm_policy_number> **-value** <hsm_policy_value> [**-force**]

Parameter	Shortcut	Description
-force	**-f**	Force the action without prompting. If this option is included in the list for a destructive policy change, the policy will be changed without prompting the user for a confirmation of zeroizing the HSM.
-policy	**-po**	Specifies the policy code of the policy to alter. Policy descriptions and codes are obtained with the **hsm showpolicies** command.
-value	**-v**	Specifies the value to assign to the specified policy. When specifying values for a on/off type policy, use '1' for on and '0' for off.

Example

```
lunash:> hsm changePolicy -policy 6 -value 0
CAUTION:  Are you sure you wish to change the destructive policy named:
Allow masking
Changing this policy will result in erasing all partitions on the HSM (zeroization)!
Type 'proceed' to zeroize your HSM and change the policy, or 'quit' to quit now.
>  quit
'hsm changePolicy' aborted.
lunash:> hsm changePolicy -policy 16 -value 0
'hsm changePolicy' successful.
Policy Allow network replication is now set to value: 0
```

hsm changepw

Change the password or PED key contents for the HSM Admin. Both the old and the new PED key are required for PED-authenticated HSMs.

Syntax

hsm -changepw [**-oldpw** <password> **-newpw** <password>]

Parameter	Shortcut	Description
-newpw	**-n**	Specifies the new password that is used as the HSM Admin's login credential to the HSM. If the new password is not provided on the command line, the you are interactively prompted for the new password, and for confirmation of the new password. A valid password should be a mix of upper and lower-case letters, digits, and other characters, and must be a minimum of 8 characters long.
-oldpw	**-o**	Specifies the current password for the HSM Admin. If the current password is not provided on the command line, the user is interactively prompted for the current password.

hsm checkcertificates

Check the HSM for presence of MAC and DAC.

Syntax

hsm checkcertificates

Example

```
lunash:>hsm checkCertificates

 MAC found -- certificatePolicies: evaluated to FIPS 140-2 Level 3
 DAC found -- certificatePolicies: meets requirements of FIPS 140-2 Level 3

Command Result : 0 (Success)
```

hsm debug show

Display HSM debug information. This command can dump many hundreds of lines of information to your display. In SSH/PuTTY sessions, you can stop and start the flow of output with Ctrl-S and Ctrl-Q respectively.

Syntax

hsm debug show

Example

```
[luna23] lunash:>hsm debug show

HSM Dualport dump:

Current dualport:
0000:  01 ff 03 ff     dc ff 01 ff     ff ff 15 ff     21 ff 04 ff     ...........!...
0010:  01 ff 43 ff     68 ff 72 ff     79 ff 73 ff     61 ff 6c ff     ..C.h.r.y.s.a.l.
0020:  69 ff 73 ff     20 ff 49 ff     54 ff 53 ff     2c ff 20 ff     . i.s. .I.T.S.,.
0030:  49 ff 6e ff     63 ff 2e ff     00 ff 4c ff     75 ff 6e ff     I.n.c.....L.u.n.
0040:  61 ff 00 ff     4b ff 36 ff     2e ff 30 ff     00 ff ff ff     a...K.6...0.....
0050:  20 ff 04 ff     01 ff 89 ff     00 ff 01 ff     ff ff ff ff     ...............
0060:  03 00 00 00     10 00 00 00     46 54 53 49     a5 83 02 02     ........FTSI....
0070:  c0 00 00 00     c0 ff 01 ff     01 ff ff ff     40 00 00 00     ...........@...
0080:  40 01 00 00     40 6b 00 00     80 6c 00 00     40 6b 00 00     @...@k...l..@k..
0090:  00 00 00 00     00 00 00 00     30 02 90 32     ff ff ff ff     .......0..2....
00a0:  ff ff ff ff     ff ff ff ff     ff ff ff ff     ff ff ff ff     ...............
00b0:  ff ff ff ff     c0 d7 00 00     40 00 00 00     02 00 00 00     .......@.......
00c0:  c0 08 00 00     40 ca 00 00     ff ff ff ff     ff ff ff ff     ....@..........
00d0:  ff ff ff ff     ff ff ff ff     ff ff ff ff     ff ff ff ff     ...............
...
```

[Sample truncated]

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

hsm displaylicenses

Display a list of all licenses on the HSM. Licenses are either HSM upgrade licenses (which may be destructive), or HSM partition creation licenses. This command may be used by the HSM Admin to determine if they have available HSM partition licences, before attempting to create a new HSM partition using the **partition create** command.

Syntax

hsm displaylicenses

Example

```
lunash:> hsm -displaylicenses

HSM UPGRADE LICENSES
License ID Destructive  Description
========== ===========  ===========
No HSM Upgrade licenses found
PARTITION LICENSES
License ID  Total  Avail  Description
==========  ====== ====== ===========
0,   0      12     12     Generic or Secure Authentication & Access Control configuration
```

hsm duplicatemofn

Duplicate MofN PED Keys. This command starts a Luna PED operation that prompts for the existing set of green MofN PED Keys that are imprinted for this HSM. You must present the full set (all N of them - quantity M of those keys is not sufficient for this task). You must have enough blank green keys to make a full new set of N keys. This command requires HSM Admin or SO login (blue PED Key).

The command does not duplicate random MofN keys from another Luna SA.

Syntax

hsm duplicatemofn

Example

```
lunash:>hsm duplicateMofN
You will need all N of your green MofN keys, and
a second set of N green keys to be used as duplicates.
Each of the N ORIGINAL keys will be prompted for, one
at a time, then each of the N DUPLICATE keys will be
prompted for.
If you are ready to start this operation, type 'proceed',

otherwise, type 'quit'
> proceed
Proceeding...
PED operation required
Command Result : 0 (success)
```

hsm factoryreset

Set the HSM back to its factory default settings, deleting the HSM SO, all users, and all objects. This command can be run via a local serial connection only; it is not accepted via SSH.

WARNING! This command deletes all objects and users on the HSM, leaving it in a zeroized state.

This command does not require HSM login. The assumption is that your organization's physical security protocols prevent unauthorized physical access to the HSM. If those protocols failed, an unauthorized person would have no access to the HSM contents, and would be limited to temporary denial of service by destruction of HSM contents.

Because this is a destructive command, you asked to “proceed” unless the **-force** switch is provided at the command line. See "Comparison of destruction/denial actions" on page 1 in the *Administration Guide* to view a table that compares and contrasts various "deny access" events or actions that are sometimes confused.

How the firmware version affects behavior

The behavior of this command differs depending on the HSM firmware, as follows:

- On firmware earlier than version 6.22.0, this command
  - **does not** erase the RPV (Remote PED Vector or orange PED Key authentication data), and
  - **does not** erase the Auditor role, from the HSM, and
  - **does not** reset HSM policies.
- On firmware 6.22.0, or higher, this command
  - **does** erase the RPV (Remote PED Vector or orange PED Key authentication data), and
  - **does** erase the Auditor role, from the HSM, and
  - **does** reset HSM policies.

  The RPV data is required for Remote PED operations to function, including remote HSM initialization, if needed, so RPV must be reinstated after **hsm factoryreset** if you want to do any remote administration of the HSM.

Note: If the operation erased the RPV as described above, and you previously established a remote PED connection (using "hsm ped connect" on page 99), you must tear down the remote PED connection (using "hsm ped disconnect" on page 101) before you reinitialize the RPV and establish a new remote PED connection. The **hsm factoryReset** command operates on the internal HSM only, and not on software processes responsible for the remote PED connection.

Related commands

This command affects only the HSM, and not the settings for other components of the appliance. The command "sysconf config factoryreset" on page 364 affects appliance settings external to the HSM. To bring your entire Luna SA as close as possible to original configuration, as shipped from the factory, run both commands.

If you wish to zeroize (remove all partitions, roles (except Auditor), and contents) while preserving HSM policies and the RPV - that is, zeroize before shipping the HSM off to be remotely configured - use the command "hsm zeroize" on page 163 instead.

Syntax

hsm factoryreset [**-force**]

Parameter	Shortcut	Description
-force	**-f**	Force the action without prompting.

Example

Non-local (network connection) attempt:

```
lunash:>hsm factoryReset
Error:  'hsm
 factoryReset' can only be run from the local console.
 Login as 'admin' using the serial port on the
 Luna SA before running this command.
Command Result : 0 (Success)
lunash:>
```

Local attempt:

```
lunash:>hsm factoryReset
CAUTION: Are you sure you wish to reset this HSM to factory
 default settings? All partitions and data will be erased.
 Partition policies will be reverted to factory settings.
 HSM level policies will be reverted to factory settings.
 If you want to erase partitions and data only, use zeroize.
 Remote PED vector will be erased.
 Type 'proceed' to return the HSM to factory default, or
 'quit' to quit now.
 > proceed
'hsm factoryReset' successful.
Please wait while the HSM is reset to complete the process.
The remote PED vector (RPV) has been erased on HSM.
Command Result : 0 (success)
```

hsm firmware

Upgrade to the version of HSM firmware that is currently on standby in the Luna SA appliance.

Rollback to the previous version of HSM firmware, retained in the Luna SA appliance.

Syntax

hsm firmware

rollback
upgrade
show

Parameter	Shortcut	Description
show	**s**	Show HSM firmware version info. See "hsm firmware show " on page 81.
upgrade	**u**	Update HSM firmware. See "hsm firmware upgrade " on page 82.
rollback	**r**	Rollback HSM firmware. See "hsm firmware rollback " on page 78.

hsm firmware rollback

This command rolls back (downgrades) the HSM firmware to the previously installed version. You do not need to obtain the previously installed version - it was automatically saved to a special rollback holding area when you used the command "hsm firmware upgrade " on page 82.

Note: This command is intended primarily for SafeNet internal use (for example, for automated testing). It is recommended that you use this command only when instructed to do so by SafeNet technical support. The HSM capabilities and performance following a firmware rollback are uncertain.

⚠ **CAUTION:** This command is considered destructive, because an earlier firmware version can have fewer or older mechanisms and might have security vulnerabilities that a newer version does not. Therefore, the HSM requires that the SO be logged in to perform the **hsm firmware rollback** operation.

After rollback is complete, the command "hsm show" on page 115 indicates that you cannot rollback from the rolled-back firmware.

If you wish to reassert the newer firmware that was in the HSM before you rolled back, then use command "hsm firmware upgrade " on page 82, to [re-]upgrade to the newer firmware version. That version remains on standby in the appliance, so there is no need to re-upload or to re-install appliance software.

Syntax

hsm firmware rollback [password] <password>

Parameter	Shortcut	Description
-force	**-f**	Force the action

Example

The following example show the HSM configuration before and after the firmware rollback.

```
[local_host] lunash:>hsm show

   Appliance Details:
   ==================
   Software Version:                5.4.0-5

   HSM Details:
   ============
   HSM Label:                          mysa5
   Serial #:                           700022
   Firmware:                           6.21.0
   Rollback Version:                   6.20.0
   Hardware Model:                     Luna K6
   Authentication Method:              PED keys
   HSM Admin login status:             Not Logged In
   HSM Admin login attempts left:      3 before HSM zeroization!
   RPV Initialized:                    Yes
   Audit Role Initialized:             No
   Remote Login Initialized:           No
   Manually Zeroized:                  No

   Partitions created on HSM:
   ==========================

.... (snip)...

Command Result : 0 (Success)

lunash:>
[local_host] lunash:>hsm firmware rollback

WARNING: This operation will rollback your HSM to the previous firmware version !!!

         (1) This is a destructive operation.
         (2) You will lose all your partitions.
         (3) You may lose some capabilities.
         (4) You may have to re-initialize the HSM.

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

> proceed
Proceeding...

Rolling back firmware.  This may take several minutes.


Command Result : 0 (Success)
[local_host] lunash:>hsm show


   Appliance Details:
   ==================
   Software Version:                5.4.0-5

   HSM Details:
   ============
   HSM Label:                          mysa5
   Serial #:                           700022
   Firmware:                           6.20.0
   Rollback Version:                   Cannot Rollback!    <<=======
   Hardware Model:                     Luna K6
   Authentication Method:              PED keys
   HSM Admin login status:             Not Logged In
   HSM Admin login attempts left:      3 before HSM zeroization!
   RPV Initialized:                    Yes
   Audit Role Initialized:             No
   Remote Login Initialized:           No
   Manually Zeroized:                  No

   Partitions created on HSM:
   ==========================
.... (snip)...

Command Result : 0 (Success)
```

hsm firmware show

This command displays the current HSM firmware version, the rollback version, and the version (if any) that is on standby for upgrade.

Syntax

hsm firmware show

Example

```
[mylunaSA1] lunash:>hsm firmware show

   Current Firmware:                   6.20.0
   Rollback Firmware:                  6.2.1
   Upgrade Firmware:                   6.22.0

Command Result : 0 (Success)
[mylunaSA1] lunash:>
```

hsm firmware upgrade

This command updates the HSM firmware by applying the Firmware Update File that was saved in the standby location by the SafeNet factory, or by your most recent Luna SA appliance update. The current HSM firmware version (before this command is run), becomes the rollback version after the command is run. See command "hsm firmware rollback " on page 78, to roll back to the previous firmware version.

The command example, below, shows that the command offers guidance about re-sizing of partitions, before you update the HSM firmware, in anticipation of the increased partition overhead with the newer firmware (and therefore slightly reduced space for objects in each partition) :

- Always archive your partition contents before manipulating the partition(s).
- Resizing is needed only if you intend to keep the partition contents.

> **Note:** If you are both
> \- upgrading from an earlier firmware version to HSM firmware 6.22.0 (or newer)
> AND
> \- applying the Per-Partition SO (PPSO) capability update,
> be aware that the PPSO capability update is destructive. Therefore, there is no need to re-size partitions.
>
> Instead, to avoid unnecessary duplication of effort, you should
> \- safeguard (archive) any existing partition contents,
> \- then zeroize the HSM for a clean update,
> \- then perform both the firmware AND capability updates,
> \- and finally restore to new partitions.

Syntax

hsm firmware upgrade

Parameter	Shortcut	Description
-force	**-f**	Force the action

Example

```
[mylunaSA2] lunash:>hsm firmware update

   The HSM Administrator is logged in. Proceeding...

   WARNING: This operation will upgrade the firmware and restart NTLS/HTL/STC !!!

         (1) All current NTLS and/or STC sessions will be reset.
         (2) If the server keys are in hardware, you must re-activate them.
         (3) If the PED use is remote, you must re-connect it.

*****************************************************************************************
  IMPORTANT NOTICE WITH UPGRADE TO FIRMWARE VERSION 6.22.0+

  The architecture of the new firmware requires re-organization of memory on the HSM.
  Before updating:
    1. Backup the contents of your HSM.
    2. Delete any unused partitions and their contents.
    3. Re-size any partitions that reserved more space than needed.
    4. If you have no unused partitions and none that you can resize,
       you must free up sufficient memory for the new firmware by
       moving some partitions and their contents to another
       HSM or upgrading memory if at the factory configuration.

  Do not proceed with firmware update until you have increased the available
  memory on the HSM sufficiently.
******************************************************************************************

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

   > proceed
   Proceeding...


Upgrade firmware version has requirements for available free space on HSM.
Checking that sufficient free space exists before firmware upgrade.


        Partition #: 153182004  Name: Cryptoki User     Status: Passed
Sufficient space exists for firmware upgrade.


Update Result : 0 (Success)
resetting HSM ...
Stopping ntls:OK
Starting ntls:OK
Stopping htl:OK
Starting htl:OK
Stopping stcd:                                              [  OK  ]
Starting stcd:                                              [  OK  ]

Command Result : 0 (Success)
[mylunaSA2] lunash:>
```

hsm fwupdateinfo

Saves HSM firmware update support information to the **fwupdateInfo.txt** file. The file must then be retrieved to a client/administrative computer using scp to view the information.

Syntax

hsm fwupdateinfo

Example

```
lunash:>hsm fwupdateinfo

'hsm fwupdateinfo' successful.
Use 'scp' from a client machine to get file named: fwupdateInfo.txt

Command Result : 0 (Success)
```

hsm generatedak

Generate a new DAK pair. These can be used to create a new MAC (Manufacturer's Authentication Certificate) & DAC (Device Authentication Certificate). Use this command if you wish to replace the default objects that were shipped from the SafeNet factory. If you are not using MAC and DAC in your operation, then this command and the related commands for the certificates are not of use to you, and running them will not harm anything. If your operation does use DAK and the derived certificates, use this command only in compliance with your operational procedures.

Synopsis

hsm generatedak [**-force**]

Example

```
lunash:>hsm generatedak

CAUTION:  Are you sure you wish to re-generate the DAK?
All existing DACs on the HSM will be erased.
Type 'proceed' to generate the DAK, or 'quit' to quit now.
> proceed
'hsm generateDAK' successfully completed.
Use 'scp' from a client machine to get file named:
DAKCertRequest.bin

Command Result : 0 (Success)
```

hsm information

Access commands that allow you to display HSM information, reset the HSM counters, or monitor HSM performance.

Note: These commands require HSM firmware version 6.20.0 or newer.

Syntax

hsm information

monitor
reset
show

Parameter	Shortcut	Description
monitor	**m**	Monitors the HSM performance. See "hsm information monitor" on page 87.
reset	**r**	Resets the HSM counters. See "hsm information reset" on page 90.
show	**s**	Display HSM information. See "hsm information show" on page 91.

hsm information monitor

Sample the HSM to get some statistics, such as, HSM up-time, command counts, and utilization counters.

A single run of this command, without arguments, takes approximately five seconds to complete. One measurement is taken at launch, then after five seconds (the default minimum) a second measurement is taken and compared with the first.

The date and time in the output are derived from:

- the system time and
- the HSM count of seconds since reset.

In the examples, note the line "HSM Last Reset (+/- 5 Secs Error Margin)..." That margin is due to possible variability of the default system clock. To improve the accuracy of the input to those calculations, we suggest that you use NTP for system time. If that is inconvenient, or is blocked by your security regime, then we suggest using "sysconf drift" on page 369 to precisely set the time, and then manage/prevent clock drift.

Note: This command requires HSM firmware version 6.20.0 or newer.

Note: For ongoing/continual collection of such HSM information, we recommend using SNMP.

See "HSM Information Monitor" on page 1.

Syntax

hsm information monitor [**-serial** <integer>] [**-interval** <integer>] [**-rounds** <integer>] [**-noheader**] [**-save**]

Parameter	Shortcut	Description
-interval	**-i**	Set the interval over which the HSM is polled, in seconds **Range:** 5 to 999 **Default:** 5 seconds.
-noheader	**-n**	Turn off the header and footer that are normally provided with the displayed or saved records. You might choose to omit the header and footer in a saved file, in order to make the file cleaner for concatenation and parsing by your analysis tools.
-rounds	**-r**	Set 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 maximum number of rounds for one operation of `hsm information monitor` is 65535. **Range:** 1 to 65535 **Default:** 1
-save	**-sa**	Save the captured-and-calculated records to a file named **hsm_**

Parameter	Shortcut	Description
		stats, while also displaying the output to your terminal. The filename is not modifiable, so contents are overwritten each time the command is run. Use 'scp' to retrieve the file to a workstation for analysis.
-serial	**-se**	Specifies the serial number of HSM to monitor. The default is to use the embedded HSM. This parameter is optional if your Luna SA does not have additional HSMs attached. If you have a USB-connected HSM, such as Luna G5 for PKI, then this command defaults to showing utilization data from the embedded HSM, but the serial parameter allows you to select an HSM other than the default. Data is collected for a single HSM when the command is run.

Example

With no arguments (output to terminal):

```
 [mysa5] lunash:>hsm information 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)
[mysa5] lunash:>
```

With arguments (output to terminal):

```
 [local_host] lunash:>hsm information monitor -interval 6 -rounds 6

-------------------|---------------------------------|---------------------------------
                   |       HSM Command Counts        |        HSM Utilization (%)
 HSM Uptime (Secs) |-----------------|---------------|-----------------|---------------
                   | Since HSM Reset | Last   6 Secs | Since HSM Reset | Last   6 Secs
-------------------|-----------------|---------------|-----------------|---------------
         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)
[local_host] lunash:>
```

With arguments (output to file):

```
[local_host] lunash:>hsm information monitor -interval 6 -rounds 6 -save
```

```
-------------------|---------------------------------|----------------------------------
                   |       HSM Command Counts        |        HSM Utilization (%)
 HSM Uptime (Secs) |-----------------|---------------|-----------------|----------------
                   | Since HSM Reset | Last   6 Secs | Since HSM Reset | Last   6 Secs
-------------------|-----------------|---------------|-----------------|----------------
         1,117,227 |      57,471,775 |             1 |            1.27 |           0.00
         1,117,233 |      57,471,805 |            30 |            1.27 |           0.18
         1,117,239 |      57,471,806 |             1 |            1.27 |           0.00
         1,117,245 |      57,471,807 |             1 |            1.27 |           0.00
         1,117,251 |      57,471,837 |            30 |            1.27 |           0.18
         1,117,257 |      57,471,838 |             1 |            1.27 |           0.00
-------------------|-----------------|---------------|-----------------|----------------

    Average HSM Utilization In This Period :  0.06%
    HSM Last Reset                         :  Fri May 31 14:59:46 2013


The HSM untilization counters are saved to file hsm_stats.
Please run `my file list` command to see it. You may also
want to `scp` the file out for further analysis.

Command Result : 0 (Success)
```

hsm information reset

Reset the HSM counters.

Syntax

hsm information reset

Example

```
lunash:>hsm info reset

Command Result : 0 (Success)
```

hsm information show

Display the contents of he HSM counters.

Note: The "Operation Requests" counter increments rapidly (often by 42 or 47 counts) because even relatively simple Luna Shell commands trigger a number of low-level operations, including checking of firmware version, checking of HSM status, and other actions, before the current high-level command is completed.

Syntax

hsm information show

Example

```
lunash:>hsm information show

HSM Information:
Operation Requests:                            3083
Operation Errors:                                 0
Critical Events:                                  0
Non-Critical Events:                              0

Command Result : 0 (Success)
```

hsm init

Initialize the HSM (K6 key card) in the Luna HSM Server. Initialization assigns an HSM label, creates or associates Security Officer (SO) or HSM Admin authentication for the HSM, creates or associates a Cloning Domain (with authentication) for the HSM, and applies other settings that make the HSM available for use.

⚠ **CAUTION:** Initializing the HSM erases all existing data on the key card, including all HSM Partitions and their data. HSM Partitions 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.

⚠ **CAUTION:** Invoking the **hsm init** command results in the HSM Admin being logged out, and all partitions being deactivated. These preparatory actions take place before the warning prompt appears, with its request for you to type "Proceed" or "Quit". That is, if you invoke **hsm init** and then type **quit** at the prompt, initialization does not take place (meaning that you do not lose existing token/HSM contents), but any current login or activation state is closed, whether you abort the command or not.

For more information, see "What is initialization? (PED-authentication)" on page 1in the *Administration Guide*.

Syntax

hsm init -label <hsm_label> [**-domain** <hsm_domain>] [**-password** <hsm_admin_password>] [**-defaultdomain**] [**-authtimeconfig**] [**-force**]

Parameter	Shortcut	Description
-authtimeconfig	**-a**	Specifies that the SO role must be logged in to configure the time.
-defaultdomain	**-de**	This option is deprecated. The current and future HSM versions do not allow you to omit providing a domain, unless you include this "-defaultdomain" option, which is an insecure choice and generally not recommended. It is retained for benefit of existing customers who have previously set the default domain, and are constrained to continue with it until they create new objects on an HSM with a proper domain. The "-defaultdomain" option applies to Password-authenticated HSMs only. For PED-authenticated HSMs the PED always prompts for a physical PED Key and either reuses the value on the key that you insert, or generates a new value and imprints it on the PED Key.
-domain	**-do**	Specifies the string to be used as key cloning domain for the HSM. If no value is given for a Luna HSM with Password Authentication, you are prompted interactively. The HSM must support cloning, or this value is ignored. This parameter is considered mandatory in password-authenticated HSMs (except if the discouraged and deprecated -defaultdomain is specified). The -domain parameter is

Parameter	Shortcut	Description
		ignored in PED-authenticated HSMs.
-force	**-f**	Force the action without prompting.
-label	**-l**	Specifies the label to assign to the HSM. The label has a maximum length of 32 characters. Any data input over 32 characters is truncated.
-password	**-p**	Specifies the password to be used as login credential by the HSM Admin. For PED-authenticated HSMs, the Luna PED is used for the HSM Admin PIN/password, and data input for this value is ignored. This parameter is required in password-authenticated HSMs. It is ignored in PED-authenticated HSMs.

Example

PED-authenticated HSMs

If the HSM has been factory reset, then a complete "hard" initialization is performed when you invoke the **hsm init** command.

```
lunash:> hsm -init -label myluna
CAUTION:  Are you sure you wish to re-initialize this HSM?
 All partitions and data will be erased.
 Type 'proceed' to initialize the HSM, or 'quit'
 to quit now.
  > proceed
Luna PED operation required to initialize HSM - use Security Officer (blue) PED Key
Luna PED operation required to login as HSM Administrator - use Security Officer (blue) PED Key
Luna PED operation required to generate cloning domain - use Domain (red) PED Key

'hsm -init successful'

Command result : 0 (Success)
lunash:>
```

If the HSM is NOT in factory reset condition when you invoke the **hsm init** command, then a "soft" initialization is performed - while the partitions and contents are destroyed, the Security officer/HSM Administrator identity and the Domain are preserved. The SO must be logged into the HSM to run HSM init when the HSM is not in factory reset condition.

```
lunash:> hsm -init -label myluna

CAUTION:  Are you sure you wish to re-initialize this HSM?
All partitions and data will be erased.
Type 'proceed' to initialize the HSM, or 'quit' to quit now.
> proceed

Luna PED operation required to initialize HSM - use Security Officer (blue) PED Key
'hsm -init successful'

Command result : 0 (Success)
```

Password-authenticated HSMs

```
lunash:> hsm -init -label “new hsm” -sopw somepin -domain newdomain
CAUTION:  Are you sure you wish to re-initialize this HSM?
All partitions and data will be erased.
Type 'proceed' to initialize the HSM, or 'quit' to quit now.
> proceed

'hsm -init successful'
```

hsm loadcustomercert

Load the customer-signed MAC (Manufacturer's Authentication Certificate) & DAC (Device Authentication Certificate) certificates in the specified file onto the HSM.

Syntax

hsm loadcustomercert -certfilename <filename>

hsm login

Log in as the HSM Admin.

- For Luna SA with Password Authentication, the default password is 'PASSWORD'.
- For Luna SA with PED (Trusted Path) Authentication, a default login is performed by the PED when you first begin to initialize a new or factory-reset HSM. After initialization, the appropriate blue PED Key is needed for HSM Admin login.

Syntax

lunash:> **hsm login** [**-password** <hsm_admin_password>]

Parameter	Shortcut	Description
-password	**-p**	HSM Admin Password (for password-authenticated HSM, only; ignored for PED-authenticated HSM

Example

```
lunash:>hsm login

Luna PED operation required to login as HSM Administrator - use Security Officer (blue) PED key.
'hsm login' successful.

Command Result : 0 (Success)
```

hsm logout

Log out the HSM Admin account.

Syntax

lunash:> hsm logout

Example

```
lunash:>hsm logout

'hsm logout' successful.
Command Result : 0 (Success)
```

hsm ped

Access commands that allow you to display or change the configuration of the PED.

Syntax

hsm ped

```
    connect
    disconnect
    set
    show
    timeout
    vector
```

Parameter	Shortcut	Description
connect	**c**	Connect to a remote PED. See "hsm ped connect" on page 99.
disconnect	**d**	Disconnect the current/active remote PED. See "hsm ped disconnect" on page 101.
set	**se**	Configure a default IP address and/or port that are used by the **hsm ped connect** command when establishing a connection to a Remote PED Server. See "hsm ped set" on page 102.
show	**sh**	Display information for the current HSM PED connection. See "hsm ped show" on page 104.
timeout	**t**	Set or display the remote PED connection timeout. See "hsm ped timeout" on page 105.
vector	**v**	Initialize or erase a remote PED vector. See "hsm ped vector" on page 108.

hsm 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 **hsm ped set** command. See "hsm ped set" on page 102 for more information.

Behavior when defaults are configured using hsm ped set

The **hsm 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 **hsm ped connect** command. The behavior of the **hsm ped connect** command when defaults are configured using **hsm 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 **hsm ped set**.	Port configured with **hsm ped set**.
	IP address	IP address specified by **hsm ped connect**	Port configured with **hsm ped set**.
	Port	IP address configured with **hsm ped set**.	Port specified by **hsm ped connect**
	IP address and port	IP address specified by **hsm ped connect**	Port specified by **hsm ped connect**
IP address only	None	IP address configured with **hsm ped set**.	Port 1503 (default).
	IP address	IP address specified by **hsm ped connect**	Port 1503 (default).
	Port	IP address configured with **hsm ped set**.	Port specified by **hsm ped connect**.
	IP address and port	IP address specified by **hsm ped connect**	Port specified by **hsm ped connect**.
Port only	None	Error. You must use the **-ip** parameter to specify an IP address.	Port configured with **hsm ped set**.
	IP address	IP address specified by **hsm ped connect**	Port configured with **hsm ped set**.
	Port	Error. You must use the **-ip** parameter to specify an IP address..	Port specified by **hsm ped connect**
	IP address and port	IP address specified by **hsm ped connect**	Port specified by **hsm ped connect**

Behavior when no defaults are configured using hsm ped set

If no defaults are configured using **hsm ped set**, you must specifiy at least an IP address. If no port is specified, the default port (1503) is used.

> **Note:** To set up or erase a PED vector, or to make or break the Remote PED connection, on an HSM that is externally connected to the Luna SA, use the "-serial" option to specify the target HSM.
>
> If "-serial" is not specified, then the command acts on the Luna SA's internal HSM card.

Syntax

hsm 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

```
lunash:>hsm ped connect -ip 172.20.10.155

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

Command Result : 0 (Success)
```

hsm ped disconnect

Disconnect the current/active remote PED. No address information is required since only one remote PED connection can exist at one time.

Note: To set up or erase a PED vector, or to make or break the Remote PED connection, on an HSM that is externally connected to the Luna SA, use the "-serial" option to specify the target HSM.

If "-serial" is not specified, then the command acts on the Luna SA's internal HSM card.

Syntax

hsm ped disconnect [**-serial** <serialnum>] [**-force**]

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

Example

```
lunash:>hsm 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)
```

hsm ped set

Configure a default IP address and/or port that are used by the **hsm ped connect** command when establishing a connection to a Remote PED Server. See "hsm ped connect" on page 99 for more information.

Syntax

hsm ped set [-ip <ip_address>] [**-port** <port>]

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

Example

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

Command Result : 0 (Success)

lunash:>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 : 0 (Success)
```

hsm ped show

Display information for the current HSM PED connection.

Syntax

hsm ped show

Example

```
lunash:>hsm 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 : 0 (Success)
```

hsm ped timeout

Access commands that allow you to set or display the remote PED connection timeout.

Syntax

hsm ped timeout

set
show

Parameter	Shortcut	Description
set	**se**	Set the remote PED connection timeouts. See "hsm ped timeout set" on page 106.
show	**sh**	Display the currently configured remote PED connection timeout values. See "hsm ped timeout show" on page 107.

hsm ped timeout set

Set the remote PED connection (**rped**) or PED key interaction (**pedk**) timeout values:

- **rped** - is the connection inactivity timeout. The default is 1800 seconds (30 minutes). While we do not anticipate any great security risk from having a Remote PED connection left open and unused for long periods, we do suggest that having sessions open indefinitely might be an invitation, so set the **rped** value as long as you realistically need, but not more.
- **pedk** - is for PED Key activities in particular. The default is 100 seconds. It might be useful to increase that timeout if you are initializing your HSM with large values for MofN on some-or-all PED Keys. We have tested initializations with all secrets set to the maximum Mof N, equal to 16 of 16, and a pedk value of 900 seconds (15 minutes) was adequate to complete the necessary interactions. If you are not using MofN, then leave 'pedk' at its default value.

After **rped** expires, you must re-establish the Remote PED link with **hsm ped disconnect** and **hsm ped connect** before issuing any HSM or application partition commands that require PED interaction. We recommend running disconnect before reconnecting because, although the link normally disconnects cleanly upon timeout, it can happen that the link is left in an indeterminate state, and a disconnect before a connect corrects that.

Syntax

hsm ped timeout set -type <type> **-seconds** <seconds>

Parameter	Shortcut	Description
-seconds	**-s**	Specifies the timeout value, in seconds, for the specified type. **Range:** 1 to 99999 **Defaults:** 1800 (rped), 100 (pedk)
-type	**-t**	Specifies the timeout type. **Valid values:** • **rped** - set the remote PED connection inactivity timeout. • **pedk** - set the PED key timeout.

Example

```
lunash:>hsm ped timeout set -type rped -seconds 2000

Set the timeout value to 2000 seconds.

Command Result : 0 (Success)
```

hsm ped timeout show

Display the currently configured remote PED connection timeout values.

Syntax

hsm ped timeout show

Example

```
lunash:>hsm ped timeout show

The remote PED connection timeout value (seconds) =  7200
The PED key interaction timeout value (seconds)     =  50

Command Result : 0 (Success)
```

hsm ped vector

Access commands that allow you to initialize or erase a remote PED vector (RPV) on the HSM.

Note: To set up or erase a PED vector, or to make or break the Remote PED connection, on an HSM that is externally connected to the Luna SA, use the "-serial" option to specify the target HSM.

If "-serial" is not specified, then the command acts on the Luna SA's internal HSM card.

Syntax

hsm ped vector

erase
init

Parameter	Shortcut	Description
erase	**e**	Erase a remote PED vector. See "hsm ped vector erase" on page 109.
init	**i**	Initialize a remote PED vector. See "hsm ped vector init" on page 110.

hsm ped vector erase

Erase a Remote PED vector (RPV) from the current HSM so that it can no longer establish a Remote PED connection with any workstation that has that RPV on an orange PED Key.

Note: To set up or erase a PED vector, or to make or break the Remote PED connection, on an HSM that is externally connected to the Luna SA, use the "-serial" option to specify the target HSM.

If "-serial" is not specified, then the command acts on the Luna SA's internal HSM card.

Syntax

hsm ped vector erase [**-serial** <serialnum>] [**-force**]

Parameter	Shortcut	Description
-force	**-f**	Force the action without prompting.
-serial	**-s**	Specifies the serial number of the remote PED for which you want to erase the remote PED vector.

Example

```
lunash:>hsm ped vector erase

If you are sure that you wish to erase remote PED vector (RPV), then enter 'proceed', otherwise
type 'quit'.
> proceed

Command Result : 0 (Success)
```

hsm ped vector init

Initialize a Remote PED vector. This command creates a new Remote PED Key by doing the following:

- initializing a Remote PED vector (RPV)
- imprinting the RPV onto the current HSM as well as onto an orange PED Key (RPK).
  - The RPK is kept with the Remote PED, when you set up a Remote PED workstation. The RPK allows a Luna SA with that RPV to connect to a Remote PED workstation where the attached PED provides the matching RPV, via the orange RPK.]
  - The RPV is a secret that facilitates the secure connection between a particular HSM that has that secret, and a Remote PED Server computer that has the RPK containing the identical secret. The HSM must be connected to a computer that runs Remote PED client, to manage the HSM's end of the Remote PED connection. More than one HSM can be imprinted with the same RPV, but a single Remote PED Server can connect with only one such remotely located HSM (via its client) at one time.

Note: You must be logged into the HSM as SO/HSM Admin (with the blue SO PED Key), before you can run this command.

Note: To set up or erase a PED vector, or to make or break the Remote PED connection, on an HSM that is externally connected to the Luna SA, use the "-serial" option to specify the target HSM.

If "-serial" is not specified, then the command acts on the Luna SA's internal HSM card.

Syntax

hsm ped vector init [**-serial** <serialnum>] [**-force**]

Parameter	Shortcut	Description
-force	**-f**	Force the action without prompting.
-serial	**-s**	Specifies the serial number of the remote PED for which you want to erase the remote PED vector.

Example

```
lunash:>hsm ped vector init

If you are sure that you wish to initialize remote PED vector (RPV), then enter 'proceed', oth-
erwise type 'quit'.
> proceed
Proceeding...
Luna PED operation required to initialize remote PED key vector - use orange PED key(s).
Ped Client Version 1.0.5 (10005)
Ped Client launched in shutdown mode.
PED client local IP : 172.20.9.77/192.168.255.223
Shutdown passed.
Command Result : 0 (Success)

[mylunasa] lunash:>
```

hsm restore [reserved]

Restore the contents of the HSM from a backup token.

Syntax

hsm restore -serial <serialnum> [**-password** <password>] [**-tokenAdminPw** <password>] [**-force**]

Parameter	Shortcut	Description
-force	**-f .**	Force the action without prompting.
-password	**-p**	Specifies the HSM Admin Password. Passwords are needed only for password-authenticated HSMs, and are not required at the command line. If a password is needed, you are prompted for it, and your response is hidden by asterisk characters (*).
-serial	**-s**	Specifies the Token Serial Number. The serial number of the backup token is required.
-tokenAdminPw	**-t**	Specifies the Token Admin Password. Passwords are needed only for password-authenticated HSMs, and are not required at the command line. If a password is needed, you are prompted for it, and your response is hidden by asterisk characters (*).

Example

```
lunash:>token backup list

Token Details:
============
Token Label:                            SA78_SIM-21/12/2011
Slot:                                          1
Serial #:                                   300555
Firmware:                                  4.8.6
Hardware Model:                       Luna PCM G4
Command Result : 0 (Success)

lunash:>hsm restore -s 300555

CAUTION:  This process will erase the current masking key on
       this HSM and replace it with the one on the backup
       token. Any keys masked off any partition on the
       HSM with the existing masking key will be irretrievable.
       Type 'proceed' to replace the masking key, or 'quit'
       to quit now.
       > proceed
Luna PED operation required to login as HSM Administrator - use Security Officer (blue) PED key.
Warning:  You will need to connect Luna PED to the Luna Backup HSM to complete this operation.
       You may use the same Luna PED that you used for Luna SA.
       Please type 'proceed' and hit <enter> when you are ready to proceed>  proceed
Luna PED operation required to login to token - use token Security Officer (blue) PED key.
Masking key successfully cloned.
'hsm restore' successful.
Command Result : 0 (Success)
```

hsm selftest

Test the cryptographic capabilities of the HSM.

Syntax

hsm selftest

Example

```
lunash:>hsm selftest

Self Test. Testing HSM cryptographic capabilities.
'hsm selfTest' passed.
HSM working as expected.

Command Result : 0 (Success)
```

hsm setlegacydomain

Set the legacy cloning domain on an HSM:

- for password-authenticated HSMs, this is the text string that was used as a cloning domain on the legacy token HSM whose contents are to be migrated to the Luna SA HSM.
- for PED-authenticated HSMs, this is the cloning domain secret on the red PED Key for the legacy PED-authenticated token HSM whose contents are to be migrated to the Luna SA HSM.

Your **target** Luna SA HSM has, and retains, whatever modern HSM cloning domain was imprinted (on a red PED Key) when the HSM was initialized. This command takes the domain value from your legacy HSM's red PED Key and associates that with the modern-format domain of the current HSM, to allow the HSM to be the cloning (restore...) recipient of objects from the legacy (token) HSM. The legacy domain associated with your Luna SA HSM is attached until the HSM is reinitialized.

Objects from legacy token/HSMs can only be migrated (restored) onto Luna SA HSMs configured to use their legacy domain. In other words, you cannot defeat the security provision that prevents cloning of objects across different domains.

As well, you cannot migrate objects from a Password authenticated token/HSM to a PED authenticated Luna SA HSM, and you cannot migrate objects from a PED authenticated token/HSM to a Password authenticated Luna SA HSM. 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) HSMs and the disposition of token objects from one to the other.

Syntax

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

Parameter	Shortcut	Description
-domain	**-d**	Specifies the Legacy Cloning Domain name. This parameter is required on password-authenticated HSMs. It is ignored on PED-authenticated HSMs, which retreive the legacy domain name from the red PED key.

Example

```
lunash:> hsm  setLegacyDomain

Luna PED operation required to set legacy cloning domain - use Domain (red) PED Key.
The PED prompts for the legacy red domain PED Key (notice mention of "raw data" in the
PED message).

Command result: Success!
```

hsm show

Display a list showing the current configuration of the HSM.

Syntax

lunash:> hsm show

Example

HSM is in a non-zeroized state

```
lunash:>hsm show
Appliance Details:
==================
Software Version:       5.2.0-1

HSM Details:
==================
HSM Label:     myluna
Serial #:      700022
Firmware       6.2.1
Hardware Model:        Luna K6
Authentication Method:         PED Keys
HSM Admin login status:        Logged In
HSM Admin login attempts left:         3 before HSM zeroization!
RPV Initialized:       Yes
Audit Role Initialized:        Yes
Remote Login Initialized:      Yes
Manually Zeroized:     No


Partitions created on HSM:
==========================
Partition: 700022006,  Name: mypar2
Partition: 700022008,  Name: mypar1

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

HSM Storage Information:
==========================
Maximum HSM Storage Space (Bytes):     2097152
Space In Use (Bytes):  209714
Free Space Left (Bytes):       1887438

Command Result : 0 (Success)
```

HSM is in a zeroized state

```
lunash:>hsm show
Appliance Details:
==================
Software Version:       5.1.0-25
```

```
HSM Details:
==================
HSM Label:     no label
Serial #:      700022
Firmware       6.2.1
Hardware Model:        Luna K6
Authentication Method:         PED Keys
HSM Admin login status:        Not Logged In
HSM Admin login attempts left:         HSM is zeroized!
Audit Role Initialized:        Yes
RPV Initialized:       Yes
Manually Zeroized:     Yes


Partitions created on HSM:
==========================
There are no partitions

   FIPS 140-2 Operation

====================

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



HSM Storage Information:
==========================
Maximum HSM Storage Space (Bytes):     2097152
Space In Use (Bytes):       0
Free Space Left (Bytes):       2097152

Command Result : 0 (Success)
```

hsm showpolicies

Display the current settings for all hsm capabilities and policies, or optionally restrict the listing to only the policies that are configurable.

Luna SA 5 does not currently have a secure identity management (SIM) configuration. Certain HSM policy settings exist to enable migration from Luna SA 4.x to Luna SA 5.x, specifically the “Enable masking” and “Enable portable masking key” values.

Syntax

hsm showpolicies [**-configonly**]

Parameter	Shortcut	Description
-configonly	**-c**	Restrict the list to configurable policies only.

Example

```
[myluna] lunash:>hsm showPolicies
HSM Label: myhsm
Serial #: 700022
Firmware: 6.2.1
The following capabilities describe this HSM, and cannot be altered
except via firmware or capability updates.
Description                            Value
===========                            =====
Enable PIN-based authentication        Disallowed
Enable PED-based authentication        Allowed
Performance level                      15
Enable domestic mechanisms & key sizes Allowed
Enable masking                         Allowed
Enable cloning                         Allowed
Enable special cloning certificate     Disallowed
Enable full (non-backup) functionality Allowed
Enable ECC mechanisms                  Allowed
Enable non-FIPS algorithms             Allowed
Enable SO reset of partition PIN       Allowed
Enable network replication             Allowed
Enable Korean Algorithms               Allowed
FIPS evaluated                         Disallowed
Manufacturing Token                    Disallowed
Enable Remote Authentication           Allowed
Enable forcing user PIN change         Allowed
Enable portable masking key            Allowed
Enable partition groups                Disallowed
Enable Remote PED usage                Allowed
Enable external storage of MTK split   Allowed
HSM non-volatile storage space         2097152
Enable HA mode CGX                     Disallowed
Enable Acceleration                    Allowed
Enable unmasking                       Allowed

The following policies are set due to current configuration of
this HSM and cannot be altered directly by the user.
Description                            Value
===========                            =====
PED-based authentication                True
Store MTK split externally              False

The following policies describe the current configuration of
this HSM and may by changed by the HSM Administrator.
Changing policies marked "destructive" will zeroize (erase
completely) the entire HSM.

Description                             Value   Code    Destructive
============                            =====   ====    ===========
Allow masking                           On      6       Yes
Allow cloning                           On      7       Yes
Allow non-FIPS algorithms               On      12      Yes
SO can reset partition PIN              On      15      Yes
Allow network replication               On      16      No
Allow Remote Authentication             On      20      Yes
Force user PIN change after set/reset   Off     21      No
Allow offboard storage                  On      22      Yes
Allow remote PED usage                  On      25      No
Allow Acceleration                      On      29      Yes
Allow unmasking                         On      30      Yes
Command Result : 0 (Success)
```

hsm srk

Access commands that allow you to configure, or display information about, secure recovery keys (SRK) and secure transport mode.

Syntax

hsm srk

> **disable**
> **enable**
> **keys**
> **show**
> **transportmode**

Parameter	Shortcut	Description
disable	**d**	Disables external secure recovery keys. See "hsm srk disable" on page 120.
enable	**e**	Enables external secure recovery keys. See "hsm srk enable" on page 121.
keys	**k**	Access commands that allow you to resplit or verify secure recovery keys. See "hsm srk keys" on page 122.
show	**s**	Displays the current SRK state. See "hsm srk show " on page 125.
transportmode	**t**	Access commands that allow you to enable or disable secure transport mode. See "hsm srk transportmode" on page 126.

hsm srk disable

Disable the use of external split(s) of the SRK (secure recovery key) on purple PED Keys. The SO must be logged in to the HSM to issue this command.

Syntax

hsm srk disable

Example

```
lunash:> hsm srk disable

Command Result : 0 (Success)
```

hsm srk enable

Enables the use of external split(s) of the SRK (secure recovery key) on purple PED Keys. The SO must be logged in to the HSM to issue this command.

Syntax

lunash:> hsm srk enable

Example

```
lunash:> hsm srk enable

Command Result : 0 (Success)
```

hsm srk keys

Access commands that allow you to resplit or verify secure recovery keys (SRK).

Syntax

hsm srk keys

resplit
verify

Parameter	Shortcut	Description
resplit	**r**	Re-splits the Secure Recovery Key. See "hsm srk keys resplit" on page 123
verify	**v**	Verifies an existing Secure Recovery Key. See "hsm srk keys verify" on page 124.

hsm srk keys resplit

Generate a new split of the Secure Recovery Key. Internal splits are stored in secure memory areas on the HSM. The external split is imprinted upon a purple PED Key (or multiple purple keys if you have chosen 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 splitting operation. For safety reasons, the HSM and PED detect and refuse to overwrite the current purple PED Key(s) for the current HSM.

Syntax

hsm srk keys resplit

Example

```
lunash:> hsm srk keys resplit
Luna PED operation required to resplit the SRK - use Secure Recovery (purple) PED key.
SRK resplit succeeded.
Command Result : 0 (Success)
```

hsm srk keys verify

Verify an existing secure recovery key. This command displays the verification string for the current SRK, allowing you to compare it with the text string that was generated when Transport Mode was set.

- If the strings do not match, then someone has performed a recovery and re-split on the HSM (and likely other operations) since the split that generated your verification string.
- If the string match, then the HSM has not been altered since it was placed in transport mode.

Syntax

hsm srk keys verify

Example

```
lunash:> hsm srk keys verify

Luna PED operation required to verify the SRK split - use Secure Recovery (purple) PED key.
SRK verified.

Command Result : 0 (Success)
```

hsm srk show

hsm srk show - Display the current status of the Secure Recovery flags.

Syntax

hsm srk show

Example

```
lunash:> hsm srk show


Secure Recovery State flags:
=================================

External split enabled:           yes

SRK resplit required:             no

Hardware tampered:                no

Transport mode:                   o

Command Result : 0 (Success)
```

hsm srk transportmode

Access commands that allow you to put the HSM into, or out of, secure transport mode.

Syntax

hsm srk transportmode

enter
recover

Parameter	Shortcut	Description
enter	**e**	Places the HSM in Transport Mode. See "hsm srk transportmode enter" on page 127.
recover	**r**	Takes the HSM out of Transport Mode. See "hsm srk transportmode recover" on page 128.

hsm srk transportmode enter

Place the HSM in transport mode, invalidating 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 must be logged in to the HSM to issue this command.

Syntax

hsm srk transportmode enter

Example

```
lunash:> hsm srk transportMode enter

CAUTION:  You are about configure the HSM in transport mode.
       If you proceed, the HSM will be inoperable until it
       is recovered with the Secure Recovery Key.
       Type 'proceed' to continue, or 'quit' to quit now.
       > proceed
Configuring the HSM for transport mode...
Luna PED operation required to enter transport mode - use Secure Recovery (purple) PED key.
Be sure to record the verification string that is displayed after the MTK is zeroized.
HSM is now in Transport Mode.

Command Result : 0 (Success)

lunash:>hsm srk show

Secure Recovery State flags:
=================================
External split enabled:       yes
SRK resplit required:         no
Hardware tampered:            no
Transport mode:               yes

Command Result : 0 (Success)
```

hsm srk transportmode recover

Exit transport or tamper mode. This command reconstitutes the Master Key on the HSM, using the SRV (secure recovery vector) split(s) on the purple SRK PED Key(s), 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

hsm srk transportmode recover

Example

```
lunash:> hsm srk transportMode recover

Attempting to recover from Transport Mode...
Luna PED operation required to recover the HSM - use Secure Recovery (purple) PED key.
Successfully recovered from transport mode.
HSM restored to normal operation.

Command Result : 0 (Success)

lunash:>hsm srk show

Secure Recovery State flags:
=================================
External split enabled:        yes
SRK resplit required:          no
Hardware tampered:             no
Transport mode:                no

Command Result : 0 (Success)
```

hsm stc

Access the HSM STC-level commands. Use these commands to configure and manage the secure trusted channel (STC) admin channel. The STC admin channel is local to the appliance, and is used to transmit data between the local services and applications running on the appliance (such as LunaSH, NTLS, and the STC service) and the HSM SO partition.

Syntax

hsm stc

activationtimeout set
activationtimeout show
cipher disable
cipher enable
cipher show
client deregister
client list
client register
disable
enable
hmac disable
hmac enable
hmac show
identity create
identity delete
identity initialize
identity partition deregister
identity partition register
identity show
partition export
partition show
rekeythreshold set
rekeythreshold show
replaywindow set
replaywindow show
status

Parameter	Shortcut	Description
activationtimeout set	**a se**	Set the activation timeout for an STC link. See "hsm stc activationtimeout set" on page 132.
activationtimeout show	**a sh**	Display the STC link activation timeout for the specified partition. See "hsm stc activationtimeout show" on page 133
cipher disable	**ci d**	Disable the use of a symmetric encryption cipher algorithm for data encryption on the link. See "hsm stc cipher disable" on page 134.
cipher enable	**ci e**	Enable the use of a symmetric encryption cipher algorithm for data encryption on the link. See "hsm stc cipher enable" on page 136

Parameter	Shortcut	Description
cipher show	**ci s**	List the symmetric encryption cipher algorithms you can use for STC data encryption on the specified partition. See "hsm stc cipher show" on page 138.
client deregister	**cl d**	Deregister a client's STC public key from the specified partition. See "hsm stc client deregister" on page 139.
client list	**cl l**	List the clients registered to the specified partition. See "hsm stc client list" on page 140.
client register	**cl r**	Register a client's STC public key to the specified partition. See "hsm stc client register" on page 141.
disable	**d**	Disable the secure trusted channel (STC) link that is local to the appliance, that is, from the LunaSH shell to the HSM SO partition. See "hsm stc disable" on page 142.
enable	**e**	Establish a local secure trusted channel (STC) link from the LunaSH shell to the HSM SO partition, and set all the local HSM-related applications in the appliance to communicate to the HSM via this STC link. See "hsm stc enable" on page 143.
hmac disable	**h d**	Disable the use of an HMAC message digest algorithm for message integrity verification on the secure trusted channel (STC) link that is local to the appliance, that is, from the LunaSH shell to the HSM. See "hsm stc hmac disable" on page 144.
hmac enable	**h e**	Enable the use of an HMAC message digest algorithm used for message integrity verification on the specified partition. See "hsm stc hmac enable" on page 145
hmac show	**h s**	List the HMAC message digest algorithms you can use for STC message integrity verification on the specified partition. See "hsm stc hmac show" on page 146.
identity create	**i c**	Create a STC client identity for the LunaSH client. See "hsm stc identity create" on page 147.
identity delete	**i d**	Delete the LunaSH STC client identity. See "hsm stc identity delete" on page 148.
identity initialize	**i i**	Initialize the LunaSH STC client token. See
identity partition deregister	**i p d**	Remove the HSM SO partition identity public key that is currently registered with the LunaSH STC client token. See "hsm stc identity partition deregister" on page 150
identity partition register	**i p r**	Register the HSM SO partition identity public key with the LunaSH STC client token. See "hsm stc identity partition register" on page 151.
identity show	**i s**	Display the client name, public key hash, and registered partitions for the

Parameter	Shortcut	Description
		LunaSH STC client token. See "hsm stc identity show" on page 152.
partition export	**p i e**	Export the specified partition's public key to a file. See "hsm stc partition export" on page 153.
partition show	**p i s**	Display the public key and serial number for the current partition. See "hsm stc partition show" on page 154.
rekeythreshold set	**rek se**	Set the key life for the symmetric key used to encrypt data on the STC link for the specified partition. See "hsm stc rekeythreshold set" on page 155.
rekeythreshold show	**rek sh**	Display the key life for the symmetric key used to encrypt data on the STC link for the specified partition. See "hsm stc rekeythreshold show" on page 156.
replaywindow set	**rep se**	Set the size of the packet replay window. See "hsm stc replaywindow set" on page 157.
replaywindow show	**rep sh**	Display the current setting for the size of the packet replay window. See "hsm stc replaywindow show" on page 158.
status	**st**	Display status and configuration information for an STC link. See "stc status" on page 1.

hsm stc activationtimeout set

Set the activation timeout for the secure trusted channel (STC) admin channel. The STC admin channel is local to the appliance, and is used to transmit data between the local services and applications running on the appliance (such as LunaSH, NTLS, and the STC service) and the HSM SO partition. The activation timeout is the maximum time allowed to establish the STC link before the channel request is dropped.

Syntax

hsm stc activationtimeout set -time <timeout>

Parameter	Shortcut	Description
-time <timeout>	**-t** <timeout>	Specifies the activation timeout, in seconds. **Range:**1-240 **Default:** 120

Example

```
lunash:> hsm stc a se -t 30

Successfully changed the activation timeout for HSM to 30 seconds.
```

hsm stc activationtimeout show

Display the activation timeout for the secure trusted channel (STC) admin channel. The STC admin channel is local to the appliance, and is used to transmit data between the local services and applications running on the appliance (such as LunaSH, NTLS, and the STC service) and the HSM SO partition. The activation timeout is the maximum time allowed to establish the STC link before the channel request is dropped.

Syntax

stc activationtimeout show

Example

```
lunash:>hsm stc a sh

The channel activation timeout for HSM is 120 seconds.
```

hsm stc cipher disable

Disable the use of a symmetric encryption cipher algorithm for data encryption on the secure trusted channel (STC) admin channel.The STC admin channel is local to the appliance, and is used to transmit data between the local services and applications running on the appliance (such as LunaSH, NTLS, and the STC service) and the HSM SO partition.

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 "hsm stc cipher show" on page 138 to show which ciphers are currently enabled/disabled and the command "stc status" on page 1 to display the cipher that is currently being used.

Note: Performance is reduced for larger ciphers.

Syntax

hsm stc cipher disable -all -id <cipher_id>

Parameter	Shortcut	Description
-all	**-a**	Disable all ciphers.
-id <cipher_id>	**-id** <cipher_id>	Specifies the numerical identifier of the cipher you want to disable, as listed using the command "stc configuration cipher show" on page 1.

Example

```
lunash:>hsm stc cipher show

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

STC Encryption: On

Cipher ID    Cipher Name                              Enabled

1            AES 128 Bit with Cipher Block Chaining   Yes
2            AES 192 Bit with Cipher Block Chaining   Yes
3            AES 256 Bit with Cipher Block Chaining   Yes

Command Result : 0 (Success)

lunash:>hsm stc cipher disable -id 3

AES 256 Bit with Cipher Block Chaining is now disabled.

Command Result : 0 (Success)

lunash:>hsm stc cipher show

This table lists the ciphers supported for STC links to the HSAM SO partition. Enabled
ciphers are accepted during STC link negotiation with a client. If all ciphers
are disabled, STC links to the HSM SO 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    No

Command Result : 0 (Success)
```

hsm stc cipher enable

Enable the use of a symmetric encryption cipher algorithm for data encryption on the secure trusted channel (STC) admin channel. The STC admin channel is local to the appliance, and is used to transmit data between the local services and applications running on the appliance (such as LunaSH, NTLS, and the STC service) and the HSM SO partition.

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 "hsm stc cipher show" on page 138 to show which ciphers are currently enabled/disabled and the command "stc status" on page 1 to display the cipher that is currently being used.

Note: Performance is reduced for larger ciphers.

Syntax

hsm stc cipher enable -all -id <cipher_id>

Parameter	Shortcut	Description
-all	**-a**	Enable all ciphers.
-id <cipher_id>	**-id** <cipher_id>	Specifies the numerical identifier of the cipher you want to use, as listed using the command "stc configuration cipher show" on page 1.

Example

```
lunash:>hsm stc cipher show

This table lists the ciphers supported for STC links to the HSM SO partition. 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      No

Command Result : 0 (Success)

lunash:>hsm stc cipher enable -id 3

AES 256 Bit with Cipher Block Chaining is now enabled.

lunash:>hsm stc cipher show

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

STC Encryption: On
```

```
Cipher ID    Cipher Name                              Enabled
_________________________________________________________________
1            AES 128 Bit with Cipher Block Chaining   Yes
2            AES 192 Bit with Cipher Block Chaining   Yes
3            AES 256 Bit with Cipher Block Chaining   Yes

Command Result : 0 (Success)
```

hsm stc cipher show

List the symmetric encryption cipher algorithms you can use for data encryption on the secure trusted channel (STC) admin channel. The STC admin channel is local to the appliance, and is used to transmit data between the local services and applications running on the appliance (such as LunaSH, NTLS, and the STC service) and the HSM SO partition.

You can use the command "stc status" on page 1 to display the cipher that is currently being used.

Syntax

hsm stc cipher show

Example

```
lunash:>hsm stc cipher show

This table lists the ciphers supported for STC links to the partition. 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   No

Command Result : 0 (Success)
```

hsm stc client deregister

Deregister the STC public key for LunaSH from the HSM SO partition. You must be HSM SO to use this command.

⚠ **CAUTION:** Deregistering the Luna SH client's public key disables the STC link to that client.

Syntax

hsm stc client deregister -label <client_label>

Parameter	Shortcut	Description
-label <client_label>	**-l** <client_ label>	A string used to identify the client being deregistered.

Example

```
lunash:> hsm stc client deregister

Successfully deregistered the client public key for the admin channel
```

hsm stc client list

List the clients registered to the HSM SO partition. You must be logged in as the HSM SO to use this command.

Syntax

hsm stc client list

Example

```
lunash:> hsm stc client list

Client Name   Client Identity Public Key SHA1 Hash
rellis        2fd4e1c67a2d28fced849ee1bb76e7391b93eb1
```

hsm stc client register

Register the STC public key for LunaSH to the HSM SO partition. You must be logged in as the HSM SO to use this command.

Syntax

hsm stc client register -label <client_label> **-file** <client_public_key>

Parameter	Shortcut	Description
-name <client_name>	**-n** <client_label>	A string used to identify the client being registered.
-file <client_public_key>	**-f** <client_public_key>	The full path to the client public key file.

Example

```
lunash:> stc client register -l bsalming -f 45021294.pem

Successfully registered the client public key of bsalming
```

hsm stc disable

Disable the secure trusted channel (STC) admin channel link. The STC admin channel is local to the appliance, and is used to transmit data between the local services and applications running on the appliance (such as LunaSH, NTLS, and the STC service) and the HSM SO partition.

This command terminates the STC link, so that all communications between LunaSH and the HSM are transmitted over a non-encrypted link local to the appliance.

> **Note:** Disabling the local STC link is service affecting. It causes an STC service restart, which temporarily terminates all existing STC links to the appliance. It also terminates the existing HSM login session.

Syntax

hsm stc disable [**-force**]

Parameter	Shortcut	Description
-force	**-f**	Force the action without prompting.

Example

```
lunash:>hsm stc disable

Disabling STC on the admin channel will require a restart of STC service.
Any existing STC connections will be terminated.

Type 'proceed' to disable STC on the admin channel, or 'quit'
to quit now.
> proceed

Successfully disabled STC on the admin channel.

Command Result : 0 (Success)
```

hsm stc enable

Enable the secure trusted channel (STC) admin channel. The STC admin channel is local to the appliance, and is used to transmit data between the local services and applications running on the appliance (such as LunaSH, NTLS, and the STC service) and the HSM SO partition.

Note: Enabling the local STC link is service affecting. It causes an STC service restart, which temporarily terminates all existing STC links to the appliance. It also terminates the existing HSM login session.

Syntax

hsm stc enable [**-force**]

Parameter	Shortcut	Description
-force	**-f**	Force the action without prompting.

Example

```
lunash:>hsm stc enable

Enabling local STC will require a restart of STC service.
Any existing STC connections will be terminated.

Type 'proceed' to enable STC on the admin channel, or 'quit'
to quit now.
> proceed

Successfully enabled STC on the admin channel.

Command Result : 0 (Success)
```

hsm stc hmac disable

Disable the use of an HMAC message digest algorithm for message integrity verification on the secure trusted channel (STC) admin channel. The STC admin channel is local to the appliance, and is used to transmit data between the local services and applications running on the appliance (such as LunaSH, NTLS, and the STC service) and the HSM SO partition.

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 "hsm stc hmac show" on page 146 to show which HMAC message digest algorithms are currently enabled/disabled.

Note: You cannot disable all HMAC message digest algorithms.

Syntax

hsm stc hmac disable -id <hmac_id>

Parameter	Shortcut	Description
-id <hmac_id>	**-i** <hmac_id>	Specifies the numerical identifier of the HMAC algorithm you want to disable, as listed using the command "hsm stc hmac show" on page 146.

Example

```
lunash:> hsm stc hmac show

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

Command Result : 0 (Success)

lunash:> hsm stc hmac disable -id 0

HMAC with SHA 256 Bit is now disabled for HSM.

Command Result : 0 (Success)

lunash:> hsm stc hmac show

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

Command Result : 0 (Success)
```

hsm stc hmac enable

Enable the use of an HMAC message digest algorithm for message integrity verification on the secure trusted channel (STC) admin channel. The STC admin channel is local to the appliance, and is used to transmit data between the local services and applications running on the appliance (such as LunaSH, NTLS, and the STC service) and the HSM SO partition.

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 "hsm stc hmac show" on page 146 to show which HMAC message digest algorithms are currently enabled/disabled.

Note: You must enable at least one HMAC message digest algorithm.

Syntax

hsm stc hmac enable -id <hmac_id>

Parameter	Shortcut	Description
-id <hmac_id>	**-i** <hmac_id>	Specifies the numerical identifier of the HMAC algorithm you want to enable, as listed using the command "hsm stc hmac show" on page 146.

Example

```
lunash:>hsm stc hmac show

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

Command Result : 0 (Success)

lunash:>hsm stc hmac enable -id 0

Command Result : 0 (Success)

HMAC with SHA 256 Bit is now enabled for HSM.

lunash:>hsm stc hmac show

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

Command Result : 0 (Success)
```

hsm stc hmac show

List the HMAC message digest algorithms you can use for message integrity verification on the secure trusted channel (STC) admin channel. The STC admin channel is local to the appliance, and is used to transmit data between the local services and applications running on the appliance (such as LunaSH, NTLS, and the STC service) and the HSM SO partition.

Syntax

hsm stc hmac show

Example

```
lunash:>hsm stc hmac show

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

hsm stc identity create

Create a client identity for the STC admin channel client token. The STC admin channel is local to the appliance, and is used to transmit data between the local services and applications running on the appliance (such as LunaSH, NTLS, and the STC service) and the HSM SO partition.

After it is created, the LunaSH client identity is exported to the file **HsmClientId.cid**.

WARNING! Do not execute this command if STC is currently enabled. If you do, you will lose the ability to communicate with the HSM, and will need to decommission the HSM to recover.

Syntax

hsm stc identity create

Example

```
lunash:> hsm stc identity create

The client identity successfully created and exported to file: HsmClientId.cid.
```

hsm stc identity delete

Delete the client identity from the STC admin channel identity token. The STC admin channel is local to the appliance, and is used to transmit data between the local services and applications running on the appliance (such as LunaSH, NTLS, and the STC service) and the HSM SO partition.

This command, in conjunction with "hsm stc identity create" on page 147 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 LunaSH STC client identity public key in the HSM SO partition.
2. Deletes the HSM SO partition identity.
3. Deletes the LunaSH STC 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.

WARNING! Do not execute this command if STC is currently enabled. If you do, you will lose the ability to communicate with the HSM, and will need to decommission the HSM to recover.

Syntax

stc identity delete [**-force**]

Parameter	Shortcut	Description
-force	**-f**	Force the action without prompting.

Example

```
lunash:> hsm stc identity delete

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

All registered HSM partitions will no longer be available to this client token.

Type ‘proceed’ to continue, or ‘quit’ to quit now -> proceed

Successfully deleted client identity.
```

hsm stc identity initialize

Re-initialize the STC identity for the secure trusted channel (STC) admin channel. The STC admin channel is local to the appliance, and is used to transmit data between the local services and applications running on the appliance (such as LunaSH, NTLS, and the STC service) and the HSM SO partition.

The STC identity for the secure trusted channel (STC) admin channel is automatically initialized when the STC admin channel is enabled. You should only use this command if you need to manually re-establish the STC admin channel.

WARNING! Do not execute this command if STC is currently enabled. If you do, you will lose the ability to communicate with the HSM, and will need to decommission the HSM to recover.

Syntax

hsm stc identity initialize [**-force**]

Parameter	Shortcut	Description
-force	**-f**	Force the action without prompting.

Example

```
lunash:>hsm stc identity initialize
The client token is already initialized with the following client identity:
Public Key SHA1 Hash:              f3ac60ea5b8cef87b34ddf7dc71416c0d565824e
Registered Partition Identity:
Partition Serial Number:        154487
Partition Public Key SHA1 Hash: 543f73564ff7137897b7d8433b2df2e3b79ddfc3
Re-initialization will delete the client identity and remove existing partition registrations.
Type 'proceed' to continue, or 'quit'
to quit now.
>
```

hsm stc identity partition deregister

Remove the HSM SO partition identity public key that is currently registered to the STC admin channel client token. The STC admin channel is local to the appliance, and is used to transmit data between the local services and applications running on the appliance (such as LunaSH, NTLS, and the STC service) and the HSM SO partition.

Use this command only if you need to reconfigure the secure trusted channel (STC) admin channel. The STC admin channel is local to the appliance, and is used to transmit data between the appliance operating system and the HSM SO partition for local services and applications, such as LunaSH and NTLS.

⚠ **CAUTION:** Deregistering the HSM SO partition disables the LunaSH STC link.

Syntax

hsm stc identity partition deregister [**-force**]

Parameter	Shortcut	Description
-force	**-f**	Force the action without prompting.

Example

```
lunash:>hsm stc identity partition deregister

Are you sure you want to deregister the TBD?
Type 'proceed' to continue, or 'quit' to quit now -> proceed

TBD successfully deregistered from the client token.
```

hsm stc identity partition register

Register the HSM SO partition in the current slot to the STC admin channel client token. The STC admin channel is local to the appliance, and is used to transmit data between the local services and applications running on the appliance (such as LunaSH, NTLS, and the STC service) and the HSM SO partition.

Use this command only if you need to re-register the partition to the client token, for example if the token has been re-initialized.

Syntax

hsm stc identity partition register -file <file_path>

Parameter	Shortcut	Description
-file <file_path>	**-f** <file_path>	Specifies the full path to the partition identity file.

Example

```
lunash:> hsm stc identity partition register -f <file>

Partition Identity successfully registered
```

hsm stc identity show

Display the following information for the STC admin channel client token:

- the public key SHA1 hash for the client identity
- whether the HSM SO partition is registered or not

The STC admin channel is local to the appliance, and is used to transmit data between the local services and applications running on the appliance (such as LunaSH, NTLS, and the STC service) and the HSM SO partition.

Syntax

hsm stc identity show

Example

```
lunash:> hsm stc identity show

Public Key SHA1 Hash:           aa8983ae3c65b4e4bac24f374153f8dfffec0c2c
Registered Partition:           Yes
```

hsm stc partition export

Export the public key for the HSM SO partition to a file to be used to configure the STC admin channel. The STC admin channel is local to the appliance, and is used to transmit data between the local services and applications running on the appliance (such as LunaSH, NTLS, and the STC service) and the HSM SO partition.

You must be logged in to the HSM as the SO to perform this command.

Syntax

hsm stc partition export

Example

```
lunash:>hsm stc partition export

Successfully exported partition identity for HSM to file: 359693009023.pid
```

hsm stc partition show

Display the public key and serial number for the HSM SO partition. You must be logged into the partition as the SO to perform this command.

Syntax

hsm stc partition show

Example

```
lunash:>hsm stc partiton show

Partition Serial Number:                 359693009023
Partition Identity Public Key SHA1 Hash: ee27ac0376af538a6f15523002c43c7b6febdf34
```

hsm stc rekeythreshold set

Set the rekey threshold for the symmetric key used to encrypt data on the STC admin channel. The STC admin channel is local to the appliance, and is used to transmit data between the local services and applications running on the appliance (such as LunaSH, NTLS, and the STC service) and the HSM SO partition.

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. Each command sent to the HSM over the HSM STC link uses one life.

Syntax

hsm stc rekeythreshold set -partition <partition> **-value** <key_life>

Parameter	Shortcut	Description
-value <key_life>	**-v** <key_life>	An integer that specifies the key life for the STC symmetric key, in millions of messages. Each message sent to the HSM over the STC link uses one life. **Range:** 0 - 4000 **Default:** 400

Example

```
lunash:>hsm stc rekeythreshold set -par mapleleafs -v 500

Successfully changed the rekey threshold for HSM to 500 million commands.
```

hsm stc rekeythreshold show

Display the rekey threshold for the symmetric key used to encrypt data on the secure trusted channel (STC) admin channel. The STC admin channel is local to the appliance, and is used to transmit data between the local services and applications running on the appliance (such as LunaSH, NTLS, and the STC service) and the HSM SO partition.

The symmetric key is used the number of times specified by the threshold value, after which it is regenerated and the counter is reset to 0. Each command sent to the HSM over the STC link uses one life.

Syntax

hsm stc rekeythreshold show

Example

```
lunash:>hsm stc rekeythreshold show

Current rekey threshold for HSM is 400 million messages.
```

hsm stc replaywindow set

Set the size of the packet replay window for the STC admin channel. The STC admin channel is local to the appliance, and is used to transmit data between the local services and applications running on the appliance (such as LunaSH, NTLS, and the STC service) and the HSM SO partition.

This value specifies the number of packets in the window of sequenced packets that are tracked to provide anti-replay protection.

About the Replay Window

All packets sent over an 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. The receiver remembers which packets it has received within a specified window, and rejects any packets that have already been received or that are older than the oldest packet in the window.

The replay window is dynamic and is defined by the packets in the range {(X-N+1) to X}, where X is the current packet number and N is the replay window size. Any packets numbered X-N or older are discarded. Any packets in the range of the replay window {(X-N+1) to X} that have already been received are discarded. All other packets are accepted.

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

hsm stc replaywindow set -size <number_of_packets>

Parameter	Shortcut	Description
-size <number_of_packets>	**-s** <number_of_packets>	Specifies the number of packets (commands) in the replay window. **Range:**100-1000 **Default:**120

Example

```
lunash:>hsm stc replaywindow set -size 500

Successfully changed the size of the replay window for HSM to 500 commands.
```

hsm stc replaywindow show

Display the size of the packet replay window for the STC admin channel. The STC admin channel is local to the appliance, and is used to transmit data between the local services and applications running on the appliance (such as LunaSH, NTLS, and the STC service) and the HSM SO partition.

This value specifies the number of packets in the window of sequenced packets that are tracked to provide anti-replay protection.

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. The receiver remembers which packets it has received within a specified window, and rejects any packets that have already been received or that are older than the oldest packet in the window.

The replay window is dynamic and is defined by the packets in the range {(X-N+1) to X}, where X is the current packet number and N is the replay window size. Any packets numbered X-N or older are discarded. Any packets in the range of the replay window {(X-N+1) to X} that have already been received are discarded. All other packets are accepted.

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

hsm stc replaywindow show

Example

```
lunash:>hsm stc replaywindow show

The current replay window size for HSM is 120 commands.
```

hsm supportinfo

Get HSM support information in the **supportInfo.txt** file. The collected information includes a variety of information about the state and settings of the HSM, as well as other important appliance info such as the network settings and negotiated link status.The file must be transferred from the Luna appliance to you client using scp, and sent to Customer Support.

The file **supportinfo.txt** is generated by any of the following events:

- sysconf appliance reboot
- sysconf appliance power off
- a press of the Start/Stop button on the Luna SA front panel

Syntax

hsm supportInfo

Example

```
lunash:>hsm supportInfo

'hsm supportInfo' successful.
Use 'scp' from a client machine to get file named:
supportInfo.txt

Command Result : 0 (Success)
```

hsm update

Access commands that allow you to display or install any available capability or firmware updates.

A capability update or a firmware update is meant to be applied just one time to an HSM. If you attempt to re-apply a capability update to an HSM that already has the capability installed, the system throws an error like " C0000002 : RC_ GENERAL_ERROR ". A similar result occurs if you attempt to install a particular firmware update more than once on one HSM. This is expected behavior.

Syntax

hsm update

capability
show

Parameter	Shortcut	Description
capability	c	Apply a capability update. See "hsm update capability" on page 161.
show	s	Display a list of the available HSM updates. See "hsm update show" on page 162.

hsm update capability

Apply a capability update. You must use **scp** to transfer the capability update from your Luna client workstation to the appliance before you can apply it. You can view any packages that have been transferred, but not yet installed, using the **hsm update show** command.

A capability update or a firmware update is meant to be applied just one time to an HSM. If you attempt to re-apply a capability update to an HSM that already has the capability installed, the system throws an error like " C0000002 : RC_GENERAL_ERROR ". A similar result occurs if you attempt to install a particular firmware update more than once on one HSM. This is expected behavior.

Note: The command dialog prompts for a slot on which to act. This is not currently used. Always select slot 0.

Syntax

hsm update capability -capability <capability_name> [**-force**]

Parameter	Shortcut	Description
-capability	**-c**	Specifies the name of the capability update to apply.
-force	**-f**	Force the action without prompting.

Example

```
lunash:> hsm update capability -capability brandnewcapability [-force]

SafeNet Firmware/Capability Update Utility for G5 and K6 moodules
Enter slot number (0 for the first slot found) : 0
Success
Capability "brandnewcapability" updated.
```

hsm update show

Display the HSM capability update packages that have been transferred onto the Luna appliance; shows both capability packages that have not yet been applied using the **hsm update capability** command, and packages that have been applied.

> **Note:** Formerly, when a capability had been applied, it no longer appeared in the list. This changed with release 6.0 and firmware 6.22.0, to accommodate firmware rollback, which can remove any capabilities that were not applied in earlier firmware, or that are not supported by earlier firmware.
>
> After rollback or update, the system retains the full list that you had purchased, allowing you to re-install where appropriate.

To verify if a capability has been successfully added, use the **hsm showpolicies** command.or the **hsm displaylicenses** command.

Syntax

hsm update show

Example

```
lunash:> hsm update show

Capability Updates:
621000021-001    Performance level 15
621000045-001    15.5 megabytes of object storage
621000046-001    Maximum 100 partitions
621000099-001    Per-partition Security Officer

Command result : 0 (Success)
```

hsm zeroize

Removes all partitions and keys from the HSM.

CAUTION: This command puts the HSM in a zeroized state.

- This command destroys the HSM SO and all users (except Auditor), and their objects.
- This command can be run only via a local serial connection; it is not accepted via SSH. Because this is a destructive command, the user is asked to “proceed” unless the -force switch is provided at the command line. See "Comparison of destruction/denial actions" on page 1 in the *Administration Guide* to view a table that compares and contrasts various "deny access" events or actions that are sometimes confused.
- This command does not require HSM login. The assumption is that your organization's physical security protocols prevent unauthorized physical access to the HSM. Nevertheless, if those protocols failed, an unauthorized person would have no access to HSM contents, and would be limited to temporary denial of service by destruction of HSM contents.
- This command was added with HSM firmware 6.22.0. It does not appear in the command list when the current slot is an older firmware version.
- This command does not reset HSM policies, except for policy 39: Allow Secure Trusted Channel. After zeroization, you will need to re-establish your STC links, as described in "Restoring STC After HSM Zeroization" on page 1 in the *Administration Guide*, and in "Creating an STC Link Between a Client and a Partition" on page 1 in the *Configuration Guide*.
- This command does not erase the RPV (Remote PED Vector or orange PED Key authentication data) from the HSM.
- This command does not delete the Auditor role.

To also reset HSM policies and destroy the RPV and destroy the Auditor, on HSMs with firmware 6.22.0 or newer, see "hsm factoryreset" on page 75.

Syntax

hsm zeroize [**-force**]

Parameter	Shortcut	Description
-force	**-f**	Force the action without prompting.

Example

Non-local (network connection) attempt

```
lunash:>hsm zeroize
Error:  'hsm zeroize' can only be run from the local console.
 Login as 'admin' using the serial port on the
 Luna SA before running this command.
Command Result : 0 (Success)
lunash:>
```

Local attempt

```
lunash:>hsm zeroize
```

```
CAUTION: Are you sure you wish to zeroize this HSM?
          All partitions and data will be erased.
          HSM level policies will not be changed.
          All current NTLS and/or STC sessions will be terminated.
          If you want policies reverted as well, use factory reset.
          Type 'proceed' to return the HSM to factory default, or
          'quit' to quit now.
          >
 > proceed
'hsm zeroize' successful.
Please wait while the HSM is reset to complete the process.
Command Result : 0 (success)
```

htl

Access commands that allow you to view or configure a host trust link (HTL) for a client. Use these commands, combined with the client-side commands, to set up a host trust link.

For example, the command **vtl addserver** has the optional parameter **-htl**, to require a host trust link between the client where that command is run and the specified Luna HSM server. That is, this side (Luna HSM server) sets the parameters for HTL linking, and the client side determines whether that HTL is required when NTLS connections are made with that client.

Syntax

htl

```
clearott
generateott
set
show
```

Parameter	Shortcut	Description
clearott	**c**	Deletes an HTL client one-time token. See "htl clearott command" on page 166.
generateott	**d**	Generates an HTL client one-time token. See "htl generateott" on page 167.
set	**l**	Access commands that allow you to configure the attributes for an HTL client one-time token. See "htl set" on page 168.
show	**r**	Displays information for the currently configured HTL client one-time tokens. See "htl show" on page 172.

htl clearott command

Delete an HTL client one-time token. This command warns you if the one-time token is in use, that is, if the connection is not down, terminated, or in an unknown state. If the one-time token is in use, you can elect to delete it. If you do, however, recovery within the grace period would not work.

Syntax

htl clearott -client <client_name> [**-force**]

Parameter	Shortcut	Description
-client	**-c**	Specifies the client for which you want to delete the HTL one-time token. This is the client name provided when you registered the client using the **client register** command.
-force	**-f**	Force the action without prompting

Example

```
lunacm:> htl clearott -client myclient -force

Command Result : 0 (Success)
```

htl generateott

Generate an HTL client one-time token. This token is used to initiate the HTL strong-binding connection.

The command allows the user to regenerate the one-time token only if there is not already an one-time token for that client (that is, if the output of the **htl show** says "No file" for that user's one-time token status). This avoids the case where an existing HTL connection cannot resume operation during the grace period because the client's one-time token was overwritten with a new one.

Synopsis

htl generateott -client <clientname>

Parameter	Shortcut	Description
-client	**-c**	Specifies the client for which you want to generate the HTL one-time token. This is the client name provided when you registered the client using the **client register** command.

Example

```
lunacm:> htl generateOtt -client myclient

Command Result : 0 (Success)
```

htl set

Access commands that allow you to configure the attributes for an HTL client one-time token.

Syntax

htl set

defaultottexpiry
graceperiod
ottexpiry

Parameter	Shortcut	Description
defaultottexpiry	**d**	Sets the HTL one-time token default expiry time for a client. See "htl set defaultottexpiry" on page 169.
graceperiod	**g**	Sets the HTL grace period. See "htl set graceperiod" on page 170.
ottexpiry	**o**	Set the HTL one-time token expiry time for a client. See "htl set ottexpiry" on page 171.

htl set defaultottexpiry

Set the HTL one-time token default expiry time for all clients. This command sets the system default that will be used for all HTL clients. You can use the **htl set ottexpiry command** to override the default for a specific HTL client.

Syntax

htl set defaultottexpiry -timeout

Parameter	Shortcut	Description
-timeout <seconds>	**-t**	**Specifies the** default timeout for all HTL clients, in seconds. Use a value of 0 to indicate that the that the one-time token never times out. **Range:** 0 to 3600

Example

```
lunacm:> htl set defaultOttExpiry  -timeout 160

ottExpiry set to 160 seconds

Command Result : 0 (Success)
```

htl set graceperiod

Set the HTL grace period. The value that you set here applies to all clients of this Luna HSM appliance.

Synopsis

htl set graceperiod -timeout <seconds>

Parameter	Shortcut	Description
-timeout	**-t**	Specifies the grace period for all HTL clients, in seconds. Use a value of 0 to set grace period off. **Range:** 0 to 200

Example

```
lunacm:> htl set gracePeriod -timeout 200

Grace period set to 200 seconds

Command Result : 0 (Success)
```

htl set ottexpiry

Set the HTL one-time token expiry time for a client.

Syntax

htl set ottExpiry -client <clientname> {**-timeout** <seconds> | **-default**}

Parameter	Shortcut	Description
-client	**-c**	Specifies the client for which you want to specify the timeout. This is the client name provided when you registered the client using the **client register** command.
-default	**-d**	specifes that you want to use the system default specified by the **htl set defaultottexpiry** command, rather than the values specified by the **-timeout** parameter. This parameter is just a toggle.
-timeout	**-t**	Specifies the timeout for the specified client, in seconds. Use a value of 0 to indicate that the that the one-time token never times out. **Range:** 0 to 3600

Example

```
lunacm:> htl set ottExpiry -client myclient -timeout 45

'htl set ottExpiry' successful.

Command Result : 0 (Success)
```

htl show

Shows HTL information for all clients, unless a specific client is named, in which case HTL information for the named client, only, is shown. he following information is displayed:

HTL Grace Period	The system-level provisionable grace period, in seconds, as set with the **htl set graceperiod** command.
Default OTT Expiry	The system-level provisionable default OTT expiry period, in seconds, as set with the **htl set defaulttottexpiry** command.
Client name	The client name, as set with the **client register** command.
HTL Status	Can be one of the following: • **Up** - the HTL link is up and operational. • **Grace Period** - the HTL link is down but the connection is still in the grace period for re-establishment without a new OTT. • **Unknown** - couldn't determine the HTL state (probably the HTL server is down). • **Down** - any other case, including an HTL link that's in the negotiation phase.
OTT Status	Can be one of the following: • **Ready for d/l** - the OTT file is available for download by the admin or operator users (currently available via scp only) • **In use** - there is an OTT file for this user in the HTL directory, which implies that it's being used by HTL at the moment • **No file** - there's no OTT file for this user on the system
OTT Expiry Time	Shows the provisioned OTT expiry time in seconds. If a user doesn't have a specifically provisioned OTT expiry time, it will show the system default with "(default") after it.

Syntax

htl show [**-client** <clientname>]

Parameter	Shortcut	Description
-client	**-c**	Specifies the client for which you want to show HTL configuration information. This is the client name provided when you registered the client using the **client register** command.

Example

```
lunash:> htl show
HTL Grace period : 30 seconds
Default OTT expiry : 30 seconds
Client Name     HTL Status      OTT Status      OTT Expiry Time
localhost       Up              In use          30 (default)
```

```
myclient        Down            No file         60
Command Result : 0 (Success)
```

my

Access commands that allow the currently logged in user to manage their files, passwords, and public keys.

Syntax

```
my
    file
    password
    public-key
```

Parameter	Shortcut	Description
file	**f**	Access commands that allow the currently logged in user to manage their files. See "my file" on page 175.
password	**pa**	Access commands that allow the currently logged in user to manage their password. See "my password" on page 179.
public-key	**pu**	Access commands that allow the currently logged in user to manage their public keys. See "my public-key" on page 182.

my file

Access commands that allow the currently logged in user to manage their files.

Syntax

my file

clear
delete
list
run

Parameter	Shortcut	Description
clear	**c**	Delete all of the files owned by the currently logged in user. See "my file clear" on page 176.
delete	**d**	Delete a file owned by the currently logged in user. See "my file delete" on page 177.
list	**l**	List the files owned by the currently logged in user. See "my file list" on page 178.

my file clear

Deletes all of the files owned by the currently logged in user.

Syntax

my file clear [**-force**]

Parameter	Shortcut	Description
-force	**-f**	Force the action without prompting.

Example

```
lunash:>my file clear

WARNING !!  This command will delete all user files.
If you are sure that you wish to proceed, then enter 'proceed', otherwise this command will
abort.
> proceed
Proceeding...

Command Result : 0 (Success)
```

my file delete

Delete a file owned by the currently logged in user.

Syntax

my file delete <filename>

Parameter	Shortcut	Description
<filename>		Specifies the name of the file to delete.

Example

```
lunash:>my file delete somefilename

 somefilename deleted

Command Result : 0 (Success)
```

my file list

List the files owned by the currently logged in user.

Synopsis

my file list

Example

```
lunash:>my file list

375368 Oct 21 11:36 supportInfo.txt
21751010 Oct 21 11:25 lunasa_update-5.1.0-15.spkg
145054 Oct 17 10:29 logs.tgz
90615 Oct 13 10:28 syslog
294 Oct   5 15:23 pub.pub
294 Oct  5 15:22 pub

Command Result : 0 (Success)
```

my password

Access commands that allow the currently logged in user to manage their password.

Syntax

my password

expiry show
set

Parameter	Shortcut	Description
expiry show	**e s**	Displays password expiry information for the currently logged in user. See "my password expiry show" on page 180.
set	**s**	Change the password for the currently logged in user. See "my password set" on page 181.

my password expiry show

Display password expiry information for the currently logged in user.

Syntax

my password expiry show

Example

```
lunash:>my password expiry show

Last password change        : Sep 14, 2010
Password expires            : never

Command Result : 0 (Success)
```

my password set

Change the password for the currently logged in user.

Syntax

my password set

Example

```
lunash:>my password set
Changing password for user admin.

You can now choose the new password.

A valid password should be a mix of upper and lower case letters,
digits, and other characters.  You can use a minimum 8 character long
password with characters from at least 3 of these 4 classes.
An upper case letter that begins the password and a digit that
ends it do not count towards the number of character classes used.
Enter new password:
Re-type new password:

passwd: all authentication tokens updated successfully.

Command Result : 0 (Success)
```

my public-key

Access commands that allow the currently logged in user to manage their public keys. Add a public key for your user if you wish to authenticate your sessions using public-key authentication rather than password. The Luna SA is shipped with public-key authentication allowed, by default. However, you nevertheless must make your first connections using password authentication, until you have imported a public key from your computer and added it to the appliance with **my public-key add** command.

Note: The my public-key commands manage the existence of the public keys for use by ssh sessions, but the commands to enable and disable their use on Luna SA are still at:
"sysconf ssh publickey enable" on page 450
and
"sysconf ssh publickey disable" on page 449

Syntax

my public-key

add
clear
delete
list

Parameter	Shortcut	Description
add	**a**	Adds an SSH public key for the currently logged in user. See "my public-key add" on page 183.
clear	**c**	Deletes all SSH public keys for the currently logged in user. See "my public-key clear" on page 184.
delete	**d**	Deletes an SSH public key for the currently logged in user. See "my public-key delete" on page 185.
list	**l**	Lists the SSH public keys owned by the currently logged in user. See "my public-key list" on page 186.

my public-key add

Add an SSH public key for the currently logged in user.

Note: The my public-key commands manage the existence of the public keys for use by ssh sessions, but the commands to enable and disable their use on Luna SA are still at:
"sysconf ssh publickey enable" on page 450
and
"sysconf ssh publickey disable" on page 449

Syntax

my public-key add <lunash_user_public_key>

Parameter	Shortcut	Description
<lunash_user_public_key>		Specifies the name of the public key to add.

Example

```
lunash:>my public-key add somekey

Command Result : 0 (Success)
```

my public-key clear

Delete all SSH public keys for the currently logged in user.

Note: The my public-key commands manage the existence of the public keys for use by ssh sessions, but the commands to enable and disable their use on Luna SA are still at:
"sysconf ssh publickey enable" on page 450
and
"sysconf ssh publickey disable" on page 449

Syntax

my public-key clear [-force]

Parameter	Shortcut	Description
-force	**-f**	Force the action without prompting.

Example

```
lunash:>my public-key clear

WARNING !!  This command will delete all User SSH Public Keys.
If you are sure that you wish to proceed, then enter 'proceed', otherwise this command will
abort.
> proceed
Proceeding...

Command Result : 0 (Success)
```

my public-key delete

Delete an SSH public key for the currently logged in user.

Note: The my public-key commands manage the existence of the public keys for use by ssh sessions, but the commands to enable and disable their use on Luna SA are still at:
"sysconf ssh publickey enable" on page 450
and
"sysconf ssh publickey disable" on page 449

Syntax

my public-key delete <lunash_user_public_key>

Parameter	Shortcut	Description
<lunash_user_public_key>		Specifies the name of the public key to delete.

Example

```
lunash:>my public-key delete somekey

Command Result : 0 (Success)
```

my public-key list

List the SSH public keys owned by the currently logged in user.

Note: The my public-key commands manage the existence of the public keys for use by ssh sessions, but the commands to enable and disable their use on Luna SA are still at:
"sysconf ssh publickey enable" on page 450
and
"sysconf ssh publickey disable" on page 449

Syntax

my public-key list

Example

```
lunash:>my public-key list

SSH Public Keys for user 'admin':

Name        Type     Bits    Fingerprint
------------------------------------------------------------------------------
pub1        ssh-rsa  1024    08:95:7b:9c:57:27:2e:cc:6f:f2:99:e4:19:41:1c:e9

Command Result : 0 (Success)
```

network

Access commands that allow you to view and configure the network settings for the appliance.

Syntax

```
network
    dns
    domain
    hostname
    interface
    ping
    route
    show
```

Parameter	Shortcut	Description
dns	**dn**	Access commands that allow you to configure the appliance DNS settings. See "network dns" on page 188.
domain	**do**	Set the network domain. See "network domain" on page 191.
hostname	**h**	Set the appliance hostname. See "network hostname" on page 192.
interface	**i**	Configure the network interfaces. See "network interface" on page 193.
ping	**p**	Test the network connectivity. See "network ping" on page 203.
route	**r**	Access commands that allow you to configure the network routes for the appliance. See "network route" on page 204.
show	**s**	Display the current network configuration. See "network show" on page 209.

network dns

Access commands that allow you to configure the appliance DNS settings.

Syntax

network dns

add
delete

Parameter	Shortcut	Description
add	**a**	Add domain name servers and search domains to the network configuration. See "network dns add" on page 189.
delete	**d**	Delete domain name servers and search domains from the network configuration. See "network dns delete" on page 190.

network dns add

This command adds a domain name server or search domain to the system.

The user must execute the command once for each name server or search domain being added. To see the existing DNS settings, use the **network show** command.

Syntax

network dns add {[**-nameserver** <ip_address>] | [**-searchdomain** <net_domain>]}

Parameter	Shortcut	Description
-nameserver	**-n**	Add the specified name server to the DNS table.
-searchdomain	**-s**	Add the specified search domain to the DNS table.

Example

```
lunash:> net dns add -nameserver 192.16.0.2
Success: Nameserver 192.16.0.2 added

lunash:> net dns add -searchdomain 192.16.0.0
Success: Searchdomain entry 192.16.0.0 added
```

network dns delete

This command deletes or removes a domain name server or search domain from the system.

The user must execute the command once for each name server or search domain being deleted. To see the existing DNS settings, use the **network show** command.

Syntax

network dns delete {[**-nameserver** <ip_address>] | [**-searchdomain** <net_domain>]}

Parameter	Shortcut	Description
-nameserver	**-n**	Delete the specified name server from the DNS table.
-searchdomain	**-s**	Delete the specified search domain from the DNS table.

Example

```
lunash:> net dns delete -nameserver 192.16.0.2
Success: Nameserver 192.16.0.2 deleted

lunash:> net dns delete -searchdomain 192.16.0.0
Success: Searchdomain entry 192.16.0.0 deleted
```

network domain

Set the network domain for this system. Note that the new domain will not be completely in effect until the network service is restarted (see the **service -start** command). To see the existing domain, use the **net show** command.

Syntax

network domain <netdomain>

Parameter	Shortcut	Description
<netdomain>		Set system domain name to the specified value.

Example

```
lunash:> net domain safenet-inc.com

Success: DomainName safenet-inc.com set.
```

network hostname

Set the system hostname. Note that the new hostname will not be completely in effect until the network service is restarted (see the **service -start** command). To see existing hostname, use the **network show** command.

Syntax

lunash:> network hostname <hostname>

Parameter	Shortcut	Description
<hostname>		Set system host name to the specified value.

Example

```
lunash:> net hostname Luna10

Success: Hostname Luna10 set.
```

network interface

Configure the network interface for the system. This command should be issued at least once for each Ethernet interface (Eth0 and Eth1) that will be connected to the network.

The delete sub-command can be used to remove the settings applied to a specific network interface.

Syntax

network interface

static
dhcp
delete
bonding

Parameter	Shortcut	Description
static	**s**	Set static IP configuration. See "network interface static " on page 195.
dhcp	**dh**	Set dynamic IP configuration. See "network interface dhcp " on page 196.
delete	**del**	Delete IP configuration. See "network interface delete " on page 197.
bonding	**b**	> Network interface bonding. See "network interface bonding" on page 198.

Syntax

network interface -device <netdevice> **-ip** <ipaddress> **-netmask** <ipaddress> [**-force**] [**-gateway** <ipaddress>]

net -interface -delete <ipaddress> **-device** <devicename>

```
 Name        (short)    Description
---------------------------------------------------------
delete          del     Delete IP Configuration
dhcp            dh      Set DHCP IP Configuration
static          s       Set  Static IP Configuration
bonding         b       > Network Interface Bonding*
```

delete This command may be issued to disable a network interface (eth0 or eth1). Note that NTLS always uses eth0 (the top ethernet jack at the back of the Luna SA).

dhcp [if adding, must specify one of -static or -dhcp] Indicate that this ethernet device will have a dynamic IP address. (Not recommended - note that using dhcp will automatically update the Luna appliance's system name servers and other network settings that are transmitted via DHCP). In general, we recommend **against** using DHCP for Luna appliances.

static [if adding, must specify one of -static or -dhcp] Indicate that this ethernet device will have a static IP address. (Recommended)

Options

The following options are available:

Name	(short)	Description
-device	-d	Network Device
-ip	-i	IP Address
-gateway	-g	Gateway IP Address
-netmask	-n	Network IP Address Mask
-force	-f	Force action

-device [mandatory] Indicate which ethernet device is currently being set up. Must select one of eth0 or eth1. Recommended that you always use eth0 for NTLS, and that you set it up first.

-gateway [mandatory] The gateway that this device will use (obtain from the network administrator).

-force [optional] The command is performed without prompting.

-ip [mandatory if using -static] The network device's new static IP address (obtain from the network administrator).

-netmask [mandatory if using -static] The IP address's netmask (obtain from the network administrator)

Sample Output

```
lunash:> net -interface -delete 192.22.101.77 -device eth1

Interface eth1 removed successfully.

'net -interface' successful. Ethernet device eth1 set to ip address (null).

lunash:> net -interface -static -device eth1 -ip 192.22.101.77 -gateway 192.16.0.2  -netmask 255.255.0.0

'net -interface' successful. Ethernet device eth1 set to ip address 192.22.101.77.
```

network interface static

Directs the specified Ethernet device to use the specified static IP address.

Syntax

network interface static -device <netdevice> **-ip** <ipaddress> **-netmask** <ipaddress> [**-gateway** <ipaddress>] [**-force**]

When setting "network interface" configuration, one of "static" or "dhcp" or "bonding" is required.

(Option)	Parameter	Description
-device	**-dev** <netdevice>	Network Device (Eth0,Eth1).
-ip	**-i** <ipaddress>	IP address assigned to the device.
-netmask	**-n** <ipaddress>	Enable network interface bonding.
-gateway	**-g** <ipaddress>	Disable network interface bonding.
-force	**-f**	Force action.

Sample Output

```
lunash:> net -interface -static -device eth1 -ip 192.22.101.77 -gateway
         192.16.0.2   -netmask  255.255.0.0
         'net -interface' successful.
         Ethernet device eth1 set to ip address 192.22.101.77.
```

network interface dhcp

Directs this Ethernet device to request a dynamic IP address. (Not recommended - note that using dhcp will automatically update the Luna appliance's system name servers and other network settings that are transmitted via DHCP).

Note: In general, we recommend against using DHCP for Luna appliances. Do not specify DHCP if you intend to use Network Interface Port Bonding - a change to the leased IP address disrupts port bonding, which must be manually disabled and then reconfigured before it can be re-enabled.

When setting "network interface" configuration, one or the other of "static" or "dhcp" or "bonding" is required.

Syntax

network interface dhcp -device <netdevice> [**-force**]

(Option)	Parameter	Description
-device	**-dev** <netdevice>	Network Device (Eth0,Eth1).
-force	**-f**	Force action.

network interface delete

This command disables a network interface (Eth0 or Eth1). Note that NTLS always uses Eth0 (the top Ethernet jack at the back of the Luna SA appliance).

Syntax

network interface delete -device <netdevice>

(Option)	Parameter	Description
-device	**-dev <netdevice>**	Network Device (Eth0,Eth1).

Sample Output

```
lunash:> net -interface -delete 192.22.101.77 -device eth1
       Interface eth1 removed successfully.
       'net -interface' successful. Ethernet device eth1 set to ip address (null).
```

network interface bonding

Access commands that allow you to configure bonding of the two network interfaces as a single virtual device.

Use port bonding only with static addressing. If you set bonding where dynamically allocated addressing is in use, then any future change in a DHCP lease would break interface bonding.

Syntax

network interface bonding

config
show
enable
disable

Parameter	Shortcut	Description
config	**c**	Add network bonding interface. See "network interface bonding config" on page 199 .
show	**s**	Show network interface bonding information. See "network interface bonding show" on page 202 .
enable	**e**	Enable network interface bonding. See "network interface bonding enable" on page 201 .
disable	**d**	Disable network interface bonding. See "network interface bonding disable" on page 200 .

network interface bonding config

Configure a network bonding interface - a virtual device that bonds Eth0 and Eth1.

Use port bonding only with static addressing. If you set bonding where dynamically allocated addressing is in use, then any future change in a DHCP lease would break interface bonding.

Syntax

network interface bonding config -ip <ipaddress> [**-gateway** <ipaddress>] **-netmask** <ipaddress>

Parameter	Shortcut	Description
-ip	**-i**	Specifies the IP address of the bonded virtual network device.
-gateway	**-g**	Specifies the gateway/router IP address. (This is indicated as "optional" in the command syntax, but the appropriate gateway address must always be supplied unless you and your clients are on the same subnet as the Luna SA appliance.)
-netmask	**-n**	Specifies the network address mask.

Example

```
lunash:> network interface bonding config -ip 192.20.17.200 -netmask 255.255.255.0 -gateway
192.20.17.10

Command Result : 0 (Success)
```

network interface bonding disable

Disable network interface bonding.

Syntax

network interface bonding disable

Example

```
lunash:> >network interface bonding disable

Shutting down interface eth0:
```

At this point, the ssh session disconnects, and must be re-established, including login to the Luna SA appliance.

```
lunash:>
```

network interface bonding enable

Enable network interface bonding.

Syntax

network interface bonding enable

Example

```
[172.20.9.127] lunash:>network interface bonding enable

Shutting down interface eth0: [ OK ]
 Shutting down loopback interface: [ OK ]
 Bringing up loopback interface: [ OK ]
 Bringing up interface bond0: RTNETLINK answers: File exists
 Error adding address 172.20.9.127 for bond0.
 [ OK ]
 MUST RESTART SYSTEM TO SET THE CORRECT BONDING PARAMETERS!!!

Command Result : 0 (Success)
 [172.20.9.127] lunash:>
```

At this point, the ssh session disconnects, and must be re-established, including login to the Luna SA appliance.

Note: Restart the system after the **network interface bonding enable** command, with **sysconf appliance restart**, to allow the system to begin using the new configuration.

network interface bonding show

Display the current network bonding interface status.

Syntax

network interface bonding show

Example

```
lunash:> >network interface bonding show

Bonding is configured, but not enabled.

========== Bonding Interface ==========
BOOTPROTO=static
IPADDR=172.20.17.200
NETMASK=255.255.255.0
=======================================

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

network ping

Test the network connectivity to the specified host. This command sends an ICMP ECHO message to another computer, to verify the presence and alertness of the target computer on the network.

Syntax

network ping <hostname_or_ipaddress>

Parameter	Shortcut	Description
<hostname_or_ ipaddress>		Specifies the host name or IP address to ping.

Example

```
lunash:>network ping yourLuna
PING 192.12.11.102 (192.12.11.102) from 192.12.11.77 : 56(84) bytes of data.
64 bytes from 192.12.11.102: icmp_seq=0 ttl=255 time=163 usec
--- 192.12.11.102 ping statistics ---
1 packets transmitted, 1 packets received, 0% packet loss
round-trip min/avg/max/mdev = 0.163/0.163/0.163/0.000 ms

Command Result : 0 (Success)
```

network route

Access commands that allow you to configure the network routes for the appliance.

Syntax

network route

add
clear
delete
show

Parameter	Shortcut	Description
add	**a**	Add a network route. See "network route add" on page 205.
clear	**c**	Delete all network routes. See "network route clear" on page 206.
delete	**d**	Delete the specified network route. See "network route delete" on page 207.
show	**s**	Display the current network route configuration. See "network route show " on page 208.

network route add

Add a manually configured network route to the current configuration. This command should be used only on the advice of a network administrator.

Syntax

network route add <routetype> <ipaddress> [**-device** <netdevice>] [**-force**] [**-gateway** <ipaddress>] [**-metric** <metric>] [**-netmask** <ipaddress>]

Parameter	Shortcut	Description
<routetype>		Set to "network" or "host" for network or host specific routes respectively.
<ipaddress>		Specifies the IP address of the target network or host.
-device	**-d**	Specifies a specific network device for the route.
-force	**-f**	Force the action without prompting
-gateway	**-g**	Specifies the gateway/router IP address if this is not a locally connected network or host.
-metric	**-m**	Specifies a routing metric **Range:** 0 to 65535 **Default:** 0
-netmask	**-n**	Specifies the network mask. This parameter should only be provided for network routes. If not specified, default is Class C netmask 255.255.255.0.

Example

```
lunash:> network route add <routetype> <ipaddress>
 [-device <netdevice>] [-force] [-gateway <ipaddress>] [-metric
 <metric>] [-netmask <ipaddress>]
Command Result : 0 (Success)
```

network route clear

Delete all manually configured static routes (as set with **network route add**). Since this operation may delete valuable configuration data, you are presented with a "Proceed/Quit" prompt unless you use the **-force** option.

Syntax

network route clear [**-force**]

Parameter	Shortcut	Description
-force	**-f**	Force the action without prompting

Example

```
lunash:> network route clear

Command Result : 0 (Success)
```

network route delete

Delete a manually configured network route from the current configuration. This command should be used only on the advice of a network administrator.

Syntax

network route delete <routetype> <ipaddress> [**-device** <netdevice>] [**-force**] [**-gateway** <ipaddress>] [**-metric** <metric>] [**-netmask** <ipaddress>]

Parameter	Shortcut	Description
<routetype>		Set to "network" or "host" for network or host specific routes respectively.
<ipaddress>		Specifies the IP address of the target network or host.
-device	**-d**	Specifies a specific network device for the route.
-force	**-f**	Force the action without prompting
-gateway	**-g**	Specifies the gateway/router IP address if this is not a locally connected network or host.
-metric	**-m**	Specifies a routing metric **Range:** 0 to 65535 **Default:** 0
-netmask	**-n**	Specifies the network mask. This parameter should only be provided for network routes. If not specified, default is Class C netmask 255.255.255.0.

Example

```
lunash:> network route delete <routetype> <ipaddress>
 [-device <netdevice>] [-force] [-gateway <ipaddress>] [-metric
 <metric>] [-netmask <ipaddress>]
Command Result : 0 (Success)
```

network route show

Display the current network route configuration.

Syntax

network route -show

Example

```
lunash:> network route show
Kernel IP routing table
Destination     Gateway  Genmask        Flags Metric Ref    Use Iface
192.168.10.0    0.0.0.0  255.255.255.0  U0    0      0      eth1
152.20.0.0      0.0.0.0  255.255.0.0    U0    0      0      eth0
127.0.0.0       0.0.0.0

Command Result : 0 (Success)
```

network show

Display the network configuration, including the currently-negotiated NIC speed setting. This information is also collected in the **hsm supportinfo** command.

Syntax

network show

Example

```
lunash:>network show

Hostname:          172.20.11.95
Domain:            "safenet-inc.com"
IP Address (eth0): 172.20.11.95
HW Address (eth0): 00:00:50:32:38:BF
Mask (eth0):       255.255.0.0
Gateway (eth0):    172.20.11.10
Name Servers:      172.20.10.20      172.16.2.14
Search Domain(s):  safenet-inc.com sfnt.local

Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
172.20.0.0      0.0.0.0         255.255.0.0     U     0      0        0 eth0
127.0.0.0       0.0.0.0         255.0.0.0       U     0      0        0 lo
0.0.0.0         172.20.11.10    0.0.0.0         UG    0      0        0 eth0

Link status
eth0: negotiated 100baseTx-HD, link ok
eth1: no link
```

ntls

Access commands that allow you to manage the network trust link service (NTLS) on the appliance.

Syntax

ntls

activatekeys
bind
certificate
deactivatekeys
information
ipcheck
show
sslopsall
sslopsrsa
tcp keepalive
threads
timer

Parameter	Shortcut	Description
activatekeys	**a**	Activate the NTLS keys container. See "ntls activatekeys" on page 211.
bind	**b**	Set the NTLS binding. See "ntls bind" on page 212.
certificate	**c**	Access commands that allow you to manage the NTLS certificates. See "ntls certificate" on page 214.
deactivatekeys	**d**	Deactivate the NTLS keys container. See "ntls deactivatekeys" on page 222.
information	**in**	Access commands that allow you to display NTLS status information. See "ntls information" on page 223.
ipcheck	**ip**	Access commands that allow you to manage the NTLS client source IP validation configuration. See "ntls ipcheck" on page 226.
show	**sh**	Show the NTLS binding. See "ntls show" on page 230.
sslopsall	**sslopsa**	Perform all NTLS SSL operations in hardware. See "ntls sslopsall " on page 231.
sslopsrsa	**sslopsr**	Perform only RSA NTLS SSLoperations in hardware. See "ntls sslopsrsa" on page 232.
tcp_keepalive	**tc**	Access commands that allow you to manage TCP keepalive. See "ntls tcp_keepalive" on page 233.
threads	**th**	Access commands that allow you to manage the NTLS worker threads. See "ntls threads" on page 236.
timer	**ti**	Access commands that allow you to manage the NTLS timer. See "ntls timer" on page 239.

ntls activatekeys

Activate the NTLS keys container. If you are using a PED-authenticated HSM, this command requires PED operation.

Syntax

ntls activatekeys

Example

```
lunash:>ntls activateKeys
Login successful.

Command Result : 0 (Success)
```

ntls bind

Binds the network trust link service (NTLS) to a network device (eth 0 or eth1) or to a hostname or IP address. You must bind to either a network device or a hostname/IP address.

The new setting takes effect only after NTLS is restarted.

If you wish, client traffic restriction could complement SSH traffic restriction using the command "sysconf ssh ip" on page 443 or "sysconf ssh device" on page 442, which restrict administrative traffic (over SSH) to a specific IP address or device name on your Luna SA.

Syntax

ntls bind [<netdevice>] [**-bind** <hostname_or_ipaddress>] [**-force**]

Parameter	Shortcut	Description
-bind	**-b**	Bind the NTLS service to a hostname or IP address, if no ethernet device was specified.
-force	**-f**	Force the action without prompting.
<netdevice>		Bind the NTLS service to this ethernet device. Can be left blank if you are binding to a hostname or ip address, otherwise must be the loopback device or an ethernet device. **Valid values:** **lo:** Bind to the loopback device. **eth0:** Bind to the eth0 device. **eth1:** Bind to eth1 device. **all:** Bind to all devices. Default: **lo**

Example

For a device

```
lunash:>ntls bind eth0

Success: NTLS binding network device eth0 set.
NOTICE: The NTLS service must be restarted for new settings to take effect.
If you are sure that you wish to restart NTLS, then type 'proceed', otherwise type 'quit'
> proceed

Proceeding...
Restarting NTLS service...
Stopping ntls:                            [  OK  ]
Starting ntls:                            [  OK  ]
Command Result : 0 (Success)
```

For an IP address

```
[myluna] lunash:>ntls bind none -bind 192.20.10.96

Success: NTLS binding hostname or IP Address 192.20.10.96 set.
NOTICE: The NTLS service must be restarted for new settings to take effect.
```

```
If you are sure that you wish to restart NTLS, then type 'proceed', otherwise type 'quit'
> proceed

Proceeding...
Restarting NTLS service...
Stopping ntls:                           [ OK  ]
Starting ntls:                           [ OK  ]
Command Result : 0 (Success)

lunash:>ntls show

NTLS bound to network device: none  IP
 Address: "192.20.10.96" (eth0)
Command Result : 0 (Success)
```

ntls certificate

Access commands that allow you to manage the NTLS certificates.

Syntax

ntls certificate

monitor
show

Parameter	Shortcut	Description
monitor	**m**	Access commands that allow you to manage certificate expiry monitoring. See "ntls certificate monitor" on page 215.
show	**s**	Show the NTLS server certificate. See "ntls certificate show" on page 220.

ntls certificate monitor

The following subcommands are available:

Parameter	Shortcut	Description
disable	**d**	Disable certificate expiry monitoring. See "ntls certificate monitor disable" on page 216.
enable	**e**	Enable certificate expiry monitoring. See "ntls certificate monitor enable" on page 217"ntls certificate monitor disable" on page 216
show	**s**	Show the certificate expiry monitor status. See "ntls certificate monitor show" on page 218.
trap trigger	**t**	Set the NTLS certificate expiry SNMP trap trigger. See "ntls certificate monitor trap trigger" on page 219.

ntls certificate monitor disable

Disable NTLS certificate expiry monitoring.

Syntax

ntls certificate monitor disable

Example

```
lunash:> ntls certificate monitor disable

NTLS Server Cert Monitor disabled
Shutting down certmonitord:                                  [  OK  ]

Command Result : 0 (Success)
```

lush ntls Commands

ntls certificate monitor enable

Enable NTLS certificate expiry monitoring. The NTLS certificate used by the Luna appliance is only valid for a limited period. This command turns on lifetime monitoring so that as the expiry date nears, an SNMP trap notifies an administrator of the impending expiry of the certificate.

The SNMP trap must be configured before the NTLS certificate expiry trap can be sent even if the monitor daemon is enabled.

Syntax

ntls certificate monitor enable

Example

```
lunash:> ntls certificate monitor enable

NTLS Server Cert Monitor enabled
Starting certmonitord:                                     [ OK ]

Command Result : 0 (Success)
```

ntls certificate monitor show

Report when the NTLS certificate will expire and whether certificate monitoring is enabled..

Syntax

ntls certificate monitor show

Example

```
lunash:>ntls certificate monitor enable

NTLS Server Certificate Expiry Monitor is enabled.
NTLS Server Certificate will expire on "Apr 4 15:58:32 2021 GMT"
Certificate expiry trap will be sent 5 days before the Certificate expiry day "Apr  4 15:58:32
2021 GMT" and on every 12 hour(s)
SNMP trap is not configured. No trap will be sent.


Command Result : 0 (Success)
```

ntls certificate monitor trap trigger

Set the NTLS certificate expiry SNMP trap. This command defines when, and how often, an SNMP trap is sent when the NTLS certificate is about to expire.

Syntax

ntls certificate monitor trap trigger -preexpiry <days> **-trapinterval** <hours>

Parameter	Shortcut	Description
-preexpiry	**-p**	Specifies the number of before the certificate expires that the trap is triggered. **Range:** 1 to 366
-trapinterval	**-t**	Specifies the interval, in hours, that the trap is sent once it has been triggered. **Range:** 1-720

Example

```
lunash:>ntls certificate monitor trap trigger -preexpiry 10 -trapinterval 36
Certificate expiry trap is configured to be sent 10 days before the Certificate expiry day "Apr
4 15:58:32 2021 GMT" and on every 36 hour(s)
Shutting down certmonitord:                           [  OK  ]
Starting certmonitord:                                [  OK  ]

Command Result : 0 (Success)
```

ntls certificate show

Display the contents of the NTLS server certificate.

Syntax

ntls certificate show

Example

```
lunash:>ntls certificate show

NTLS Server Certificate:
Data:
Version: 3 (0x2)
Serial Number: 0 (0x0)
Signature Algorithm: sha256WithRSAEncryption
Issuer: C=CA, ST=Ontario, L=Ottawa, O=Chrysalis-ITS, CN=168.20.20.254
Validity
Not Before: May  4 12:19:12 2011 GMT
Not After : May  5 12:19:12 2021 GMT
Subject: C=CA, ST=Ontario, L=Ottawa, O=Chrysalis-ITS, CN=168.20.20.254
Subject Public Key Info:
Public Key Algorithm: rsaEncryption
RSA Public Key: (2048 bit)
Modulus (2048 bit):
00:c1:4a:87:2f:0e:e0:a7:2d:01:d1:4e:d4:6c:b9:
8b:f0:67:46:34:e6:8b:6b:87:8f:90:83:53:49:cf:
af:30:a0:7e:f0:9a:04:8c:96:7e:3b:3a:9e:08:12:
ba:38:43:f3:e0:d0:52:01:25:37:04:b1:a1:71:f4:
b6:b6:cb:9a:ba:a4:9e:48:6d:a1:75:c3:60:6b:28:
ce:50:1e:8b:f4:5c:48:c9:5e:e2:4e:13:a0:36:9d:
ac:13:a6:b1:e9:cd:97:33:eb:f2:fb:45:c6:2d:2b:
65:0c:c4:7d:b8:c6:e0:6f:65:8d:79:89:c5:1c:6c:
ac:b2:dc:2f:15:55:d7:24:f1:7c:e0:97:83:e8:33:
e8:04:89:85:16:cc:1d:3e:6e:02:08:6a:16:08:d3:
f5:40:17:ac:e8:07:c0:05:40:76:c6:e5:1f:44:4d:
ca:e1:65:45:ef:75:73:76:6a:4d:ae:db:90:1e:84:
08:8f:5f:ae:48:de:10:02:88:71:b0:bc:6b:78:36:
21:ad:b4:f6:00:2a:92:17:e1:03:e0:3c:5e:55:94:
16:00:78:dc:bc:04:46:43:b3:26:35:01:80:1c:f7:
90:f5:1d:0d:04:bc:f7:80:12:3b:35:9c:e9:2e:4f:
7b:a8:ec:be:ab:44:f6:61:37:22:55:68:5c:2d:77:
e6:f1
Exponent: 65537 (0x10001)
Signature Algorithm: sha256WithRSAEncryption
7e:4d:b3:cf:95:e1:3b:8f:21:74:dc:e0:f7:c1:2a:c2:5e:5e:
c0:a7:70:9c:44:a0:b1:68:80:8c:2f:34:f2:eb:1e:5d:7c:b8:
19:75:ff:38:6a:6f:98:98:de:2a:4a:bd:88:ac:e7:12:69:62:
a2:07:78:4f:31:ed:92:0b:73:f4:6a:54:33:c9:9f:bb:16:1f:
67:6b:40:e8:01:8e:cd:52:66:b5:3c:5a:9c:00:34:88:e2:fa:
5d:a9:22:8f:28:8b:cf:56:f7:cd:4d:15:a5:25:59:c7:9a:4e:
8b:36:37:13:e3:dd:d5:8c:11:d9:1a:b5:69:54:77:30:97:ed:
23:9b:e7:f9:f3:66:b9:d0:b6:54:06:ba:46:da:44:22:08:b8:
87:ae:21:6e:3c:69:5f:5b:b5:d5:51:d4:53:61:5c:32:aa:87:
a4:1a:e2:cb:89:b9:0c:86:6a:15:23:2a:36:c8:72:da:23:76:
2d:d9:2c:c4:3d:8b:bd:75:4e:85:45:8e:ca:86:60:8a:07:ba:
2c:81:42:a7:c0:68:37:a9:7b:46:10:f1:e2:da:68:f7:7d:43:
eb:5c:6b:98:75:81:46:c0:31:b6:f9:68:1b:86:10:5f:3b:75:
```

```
4c:7b:79:41:b1:8b:eb:51:ad:ac:5e:3d:78:ba:9a:29:00:9f:
46:b5:03:a2
Command Result : 0 (Success)
```

ntls deactivatekeys

Deactivate the NTLS keys container.

Syntax

ntls deactivatekeys

Example

```
lunash:>ntls deactivateKeys

Command Result : 0 (Success)
```

ntls information

Access commands hat allow you to display information about the NTLS connection or reset the NTLS counters.

Syntax

ntls information

reset
show

Parameter	Shortcut	Description
reset	**r**	Reset the NTLS counters. See "ntls information reset" on page 224.
show	**s**	Display NTLS information. See "ntls information show" on page 225.

ntls information reset

Reset the NTLS counters.

Note: Resetting counters produces what is known as a "counter discontinuity" in the SNMP agent, therefore the use of this functionality is discouraged. Counter discontinuities may result in SNMP management applications recording large false positive or negative spikes if rates are being monitored using delta methods. If you are not using SNMP, then this is not an issue.

Syntax

ntls information reset

Example

```
lunash:>ntls information reset

Command Result : 0 (Success)
```

ntls information show

Display information about the NTLS connection. The following information is displayed:

Operational Status	An unsigned 32-bit integer that indicates that status of the NTLS connection.The status is reported as follows. Note that this value will generally agree with the output of the **service status ntls** command: **up:** The NTLS service appears to be running OK. (Should be "up" when front panel LED is green.) **down:** the NTLS service appears not to be running. This could indicate a fault or that NTLS is not started yet, or has been purposely disabled with (for example) **service stop ntls** or that there is a software upgrade in progress. **unknown:** The NTLS service status cannot be determined. This should be rare.
Connected Clients	An unsigned 32-bit integer that indicates the current number of clients using the NTLS connection.
Links	An unsigned 32-bit integer that indicates the current number of links on the NTLS connection.
Successful Client Connections	A 64-bit integer counter that indicates the number of client sessions that have sucessfully connected to the HSM using the NTLS connection. This value can be reset using the **ntls information reset** command.
Failed Client Connections	A 64-bit integer counter that indicates the number of client sessions that did not sucessfully connect to the HSM using the NTLS connection. This value can be reset using the **ntls information reset** command.

Syntax

ntls information show

Example

```
lunash:>ntls information show

NTLS Information:
Operational Status:                                 1 (up)
Connected Clients:                                  2
Links:                                              2
Successful Client Connections:                      112
Failed Client Connections:                          1

Command Result : 0 (Success)
```

ntls ipcheck

Access commands that allow you to enable, disable of view the configuration of NTLS client source IP validation.

Syntax

ntls ipcheck

disable
enable
show

Parameter	Shortcut	Description
disable	**d**	Disable NTLS client source IP validation. See "ntls ipcheck disable " on page 227.
enable	**e**	Enable NTLS client source IP validation. See "ntls ipcheck enable" on page 228.
show	**s**	Display the current client source IP validation configuration. See "ntls ipcheck show" on page 229.

ntls ipcheck disable

Disable client source IP address validation by NTLS upon an NTLA client connection. Use this command , for example, when you have network address translation (NAT) between your client(s) and the Luna SA appliance. The checking is enabled by default.

Syntax

ntls ipcheck disable

Example

```
lunash:>ntls ipcheck disable

NTLS client source IP validation disabled

Command Result : 0 (Success)
```

ntls ipcheck enable

Enable client source IP address validation by NTLS upon an NTLA client connection. The checking is enabled by default. The best security of your client-to-SA link is in force when ipcheck remains enabled. Keep it enabled if you have do not have network address translation (NAT) between your client(s) and the Luna SA appliance, or other situations where the ipcheck interferes with operation.

Syntax

ntls ipcheck enable

Example

```
lunash:>ntls ipcheck enable

NTLS client source IP validation enabled

Command Result : 0 (Success)
```

ntls ipcheck show

Display the current NTLS Client source IP validation configuration.

Syntax

ntls ipcheck show

Example

```
lunash:>ntls ipcheck show

NTLS client source IP validation : Enable

Command Result : 0 (Success)
```

ntls show

Display the NTLS binding network device or hostname/IP address.

Syntax

ntls show

Example

```
[myLuna] lunash:>ntls show

NTLS bound to network device: eth0  IP Address: "152.22.11.96" (eth0)

Command Result : 0 (Success)
```

ntls sslopsall

Perform all NTLS SSL operations in hardware. NTLS uses SSL to secure communication between the appliance and a client application. The **ntls sslopsall** command configures NTLS to perform all of the SSL operations on the HSM instead of in memory on the motherboard of the Luna appliance.

Syntax

ntls sslopsall

Example

```
lunash:>ntls sslopsall

Command Result : 0 (Success)
```

ntls sslopsrsa

Perform all NTLS SSL RSA operations in hardware. NTLS uses SSL to secure communication between the appliance and a client application. The **ntls sslopsrsa** command configures NTLS to perform the RSA operations of SSL on the HSM instead of in memory on the motherboard of the Luna appliance.

Syntax

ntls sslopsrsa

Example

```
lunash:>ntls sslopsrsa

Command Result : 0 (Success)
```

ntls tcp_keepalive

Access commands that allow you to view or configure the NTLS TCP keep alive settings.

Syntax

ntls tcp_keepalive

> **set**
> **show**

Parameter	Shortcut	Description
set	**-se**	Configure the NTLS TCP keep alive settings. See "ntls tcp_keepalive set" on page 234.
show	**-sh**	Display the current NTLS TCP keep alive configuration. See "ntls tcp_keepalive show" on page 235.

ntls tcp_keepalive set

Configure the NTLS TCP keep alive settings.

Syntax

ntls tcp_keepalive set -idle <seconds> **-interval** <seconds> **-probes** <number>

Parameter	Shortcut	Description
-idle	**-id**	Specifies the TCP keep alive idle timer, in seconds. This is the duration between two keep alive transmissions in idle condition. **Range**: 10 to 10,000 **Default**: 10
-interval	**-in**	Specifies the TCP keep alive interval time, in seconds. This is the duration between any two successive keep alive transmissions. **Range**: 10 to 360 **Default**: 10
-probes	**-p**	Specifies the number of retries to attempt if a transmission is not acknowledged. Default is 2. **Range**: 1 to 30 **Default**: 2

Example

```
lunash:>ntls tcp_keepalive set -idle 20 -interval 12 -probes 3

NOTICE: The NTLS service must be restarted for new settings to take effect.

Command Result : 0 (Success)
```

ntls tcp_keepalive show

Display the NTLS TCP keep alive configuration.

Syntax

ntls tcp_keepalive show

Example

```
lunash:>ntls tcp_show

NTLS TCP keepalive is configured as follows :

TCP_KEEPIDLE  : default (10)
TCP_KEEPINTVL : default (10)
TCP_KEEPCNT   : default (2)
```

ntls threads

Access commands that allow you to view or configure the NTLS worker threads settings.

Syntax

ntls threads

set
show

Parameter	Shortcut	Description
set	**se**	Configure the NTLS Datapath and CMD processor worker threads. See "ntls threads set" on page 237.
show	**sh**	Show the NTLS worker threads settings. See "ntls threads show" on page 238.

ntls threads set

Configure the NTLS Datapath and CMD processor worker threads. Data path threads control how many worker thread pairs are to be used to process inbound and outbound socket events. The default value of this configuration parameter is 5, which means there will be five inbound worker threads for reading data off the TLS/TCP socket and five outbound worker threads for writing data to the TLS/TCP socket. This implies that the data path can handle five different NTLS clients' data from five different sockets in parallel. In general, this configuration value should be increased if NTLS must service a high number of client NTLA connections.

The CMD Processor worker thread controls how many threads are used in the command processor to submit HSM requests to the K6 HSM key card inside the appliance. The default value of this configuration parameter (30 threads) is the ideal setting. Lowering this value will result in lower maximum throughput of some crypto operations, such as RSA Sign.

Above the "sweet spot" number of threads, increasing the threads does not increase throughput. The higher the number, the more task switching occurs within the process - this is the major trade-off that limits the number of threads that can provide optimum performance.

This command must be set individually and manually on all members of an HA group. Mixing settings across group members is untested and unsupported.

⚠ **CAUTION:** To achieve maximum performance with Luna SA 5.x and 6.x, client applications must spawn 30+ threads. The 10 threads indicated for legacy Luna SA 4.x is not sufficient to stress the current product.

Syntax

ntls threads set [**-datapath** <number>] **[-cmdprocessor** <number>]

Parameter	Shortcut	Description
-cmdprocessor	**-c**	Specifies the number of CMD processor threads. **Range**: 1 to 70
-datapath	**-d**	Specifies the number of data path threads. **Range**: 1 to 15

Example

```
lunash:>ntls threads set -datapath 10
NOTICE: The NTLS service must be restarted for new settings to take effect.
Command Result : 0 (Success)

lunash:>ntls threads set -cmdprocessor 60
NOTICE: The NTLS service must be restarted for new settings to take effect.
Command Result : 0 (Success)
```

ntls threads show

Display the configured number of NTLS worker threads that can run simultaneously.

Syntax

ntls threads show

Example

```
lunash:>ntls threads show

 Data path     : default (5) threads

 CMD processor : default (50) threads.

Command Result : 0 (Success)
```

ntls timer

Access commands that allow you to view or configure the NTLS receive timeout setting.

Syntax

ntls timer

set
show

Parameter	Shortcut	Description
set	**se**	Configure the NTLS receive timeout value. See "ntls timer set" on page 240.
show	**sh**	Display the NTLS receive timeout value. See "ntls timer show" on page 241.

ntls timer set

Set the number of seconds that NTLS will wait before kicking out an unauthorized connection to port 1792. Default 20 secs. Setting this parameter does not require an NTLS restart.

This command must be set individually and manually on all members of an HA group. Mixing settings across group members is untested and unsupported.

Syntax

ntls timer set -timeout <seconds>

Parameter	Shortcut	Description
-timeout	**-t**	Specifies the timeout, in seconds. **Range:** 10 to 300 **Default**: 20

Example

```
lunash:>ntls timer set 11

Command Result : 0 (Success)
```

ntls timer show

Display the configured NTLS timeout period.

Syntax

ntls timer show

Example

```
lunash:>ntls timer show

NTLS Receive timeout timer is set to default at 20 seconds

Command Result : 0 (Success)
```

package

Access commands that allow you to manage secure package updates. Use these commands after you have copied the package files to the Luna SA, using the **scp** utility.

Syntax

package

deletefile
erase
list
listfile
update
verify

Parameter	Shortcut	Description
deletefile	**d**	Delete a package file. See "package deletefile" on page 243.
erase	**e**	Delete a package . See "package erase" on page 244.
list	**l**	List the installed packages. See "package list" on page 245.
listfile	**listf**	List the uninstalled package files. See "package listfile" on page 246.
update	**u**	Update the package file. See "package update" on page 247.
verify	**v**	Verify the package file. See "package verify" on page 248.

package deletefile

Deletes a named package file from the Luna appliance.

Syntax

package deletefile <package_name>

Parameter	Shortcut	Description
<package_name>		Specifies the name of the package you want to delete.

Example

```
lunash:>package deletefile lunasa_update-5.1.0-8.spkg

Command Result : 0 (Success)
```

package erase

Erase the specified package. This command attempts to erase/uninstall the specified package from the Luna appliance. Package erase will not work if other packages are dependant upon the specified package. Only packages marked as “SOFTWARE” can be erased.

⚠ **CAUTION:** This command should never be used without the assistance or at the direction of SafeNet technical support staff.

Syntax

package erase <package_name>

Parameter	Shortcut	Description
<package_name>		Specifies the name of the package to erase. For a list of package names, use the **package list** command. (Do not specify version numbers of packages. For example, for package_abc.1.0.2-0, specify only package_abc).

Example

Please contact SafeNet for an example of this command.

package list

Display the list of all installed packages on the system. Packages are divided into system packages (cannot be erased) and software packages.

Syntax

package list

Example

```
lunash:> package list
RPM LIST (SYSTEM)
-------------------
 filesystem-2.4.0-2.el5.centos
termcap-5.5-1.20060701.1
kernel-headers-2.6.18-164.el5
centos-release-notes-5.4-4
glibc-common-2.5-42
    rootfiles-8.1-1.1.1
compat-libgcc-296-2.96-138
glibc-2.5-42
|
|
(long list - too long to include here)
RPM LIST (SOFTWARE)
-------------------
Command Result : 0 (Success)
```

package listfile

Displays a list of package files that have been transferred to the Luna SA and are available to install.

Syntax

package listfile

Example

```
lunash:> package listfile
Zero package files were found.
lunash:> package listfile
803066  Dec 09 2010 13:22 fwupK53-4.6.1-0.i386.spkg
9538  Mar 19 2012 09:10 lunasa_update-5.1.0-25PEDTimeout.spkg
```

package update

Update an existing secure package on the Luna appliance. All packages from SafeNet are signed and encrypted and come with an authcode that must be provided to decrypt and use the package. Use this command to update packages that can be seen when using the “package listfile” command. You can verify a package with the “package verify” command.

It is strongly recommended that your Luna appliance be connected to an Uninterruptable Power Supply (UPS) when you run this command. There is a small chance that a power failure during the update command could leave the Luna appliance in an unrecoverable condition.

If a version of this package is already installed, an error occurs, for example: Command failed: RPM update for original filename (fwupK6_real-6.0.9-RC1.i386.rpm)

Note: You must log into the HSM before you run this command.

Syntax

package update <filename> **-authcode** <authcode> [**-des3**]

Parameter	Shortcut	Description
-authcode	**-a**	Specifies the secure package authorization code provided by SafeNet with the secure package. The authorization code is checked during package installation to ensure that the package was encrypted and signed by SafeNet.
-des3	**-d**	Use DES3 Cipher for backward compatibility with older secure package updates.
<filename>		Specifies the name of the package to update. The new version of the package must have been transferred to the Luna appliance using **scp**.

Example

```
lunash:>hsm login
Please attend to the PED...
Command Result : 0 (Success)

lunash:>package update fwupK6_real-6.0.9-RC1.spkg -authcode pHLJtJ7/xJXS/FFK
Command succeeded:  decrypt package
Command succeeded:  verify package certificate
Command succeeded:  verify package signature
Preparing packages for installation...
fwupK6_real-6.0.9-RC1
Command Result : 0 (Success)
```

package verify

Verifies that the specified package is from SafeNet, and that the provided authcode is correct.

Syntax

package verify <package_name> **authcode** <authcode>

Parameter	Shortcut	Description
-authcode	**-a**	Specifies the secure package authorization code provided by SafeNet with the secure package
<package_name>		Specifies the name of the package to erase. For a list of packages waiting installation, use the **package listfile** command.

Example

```
lunash:>package verify lunasa_update-5.1.0-24.spkg -a qxTdRMNFFMJHYHsR

Command succeeded:  decrypt package
Command succeeded:  verify package certificate
Command succeeded:  verify package signature
Preparing packages for installation...

Command Result : 0 (Success)
```

partition

Access commands that allow you to manage partitions on the appliance.

> **Note:** Administration of partitions, using the 'partition' commands below, applies to application partitions that are owned by the HSM SO.
>
> Partitions that have their own Security Officer (PPSO) are administered from a Client computer using an appropriate application, with appropriate authentication.
> (You can supply your own application, or use the provided lunacm tool. See "Using LunaCM" on page 1.)

Syntax

partition

activate
backup
changepolicy
changepw
clear
create
createuser
deactivate
delete
list
resetpw
resize
restore
setlegacydomain
show
showcontent
showpolicies

Parameter	Shortcut	Description
activate	**a**	Activate a partition by caching its PED key data, allowing clients to authenticate with their partition password only. See "partition activate" on page 250.
backup	**b**	Backup the partition to a backup token. See "partition backup" on page 252.
changepolicy	**changepo**	Change the policies for a partition. See "partition changepolicy" on page 256.
changepw	**changepw**	Change a partition password. See "partition changepw" on page 257.
clear	**cl**	Delete all objects on a partition. See "partition clear" on page 259.

Parameter	Shortcut	Description
create	**create**	Create an HSM partition on the HSM. See "partition create" on page 260.
createuser	**createu**	Create a Crypto-User on a partition. See "partition createuser" on page 264
deactivate	**dea**	De-activate a partition by de-caching its PED key data, so that clients can no longer authenticate with their partition password only. See "partition deactivate" on page 267.
delete	**del**	Delete an HSM partition from the HSM. See "partition delete" on page 268.
list	**l**	Display a list of the accessible partitions. See "partition list" on page 269.
resetpw	**rese**	Reset a Partition Owner's password. See "partition resetpw" on page 270.
resize	**resi**	Resizes the storage space for a partition. See "partition resize" on page 272.
restore	**rest**	Restore the HSM partition contents from PCMCIA backup token. See "partition restore" on page 274.
setlegacydomain	**se**	Set the legacy cloning domain on a partition. See "partition setlegacydomain" on page 284.
show	**sh**	Display information for a partition. See "partition show" on page 285.
showcontents	**showc**	Display a list of the objects on a partition. See "partition showcontents" on page 287.
showpolicies	**showp**	Displays the policy configuration for a partition. See "partition showpolicies" on page 288.

partition activate

Caches a Partition's PED key data. Clients can then connect, authenticate with their Partition password, 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 appliance power off. If a Partition has not been activated, then each access attempt by a Client causes a login call which initiates a Luna PED operation (requiring the appropriate black PED Key). Unattended operation is possible while the Partition is activated.

Activation and auto-activation policies

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".

If you wish to automatically activate a Partition, then Partition policy number 23 "Allow auto-activation" can 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". Autoactivation caches the activation authentication data in battery-backed memory so that activation can persist/recover following a shutdown/restart or a power outage up to 2 hours duration. If Partition Policy 23 is set, then partition activation includes autoactivation. If Partition Policy 23 is not set, then partition activation persists only while the appliance is powered on, and requires your intervention to reinstate activation following a shutdown or power outage.

Syntax

partition activate -partition <name> [**-password** <password>] [**-cu**]

Parameter	Shortcut	Description
-partition	-par	Specifies the name of the HSM partition to activate. Obtain the HSM partition name by using the **partition list** command.
-password	-pas	Specifies the password needed to access the HSM partition. This is the partition string provided by the Luna PED when you created the partition - associated with the partition Owner black PED Key. For password-authenticated HSMs, it is the entire authentication for the named partition. If you omit the password in the command, you are prompted for it.
-cu	-c	Perform the task as the Crypto-User. This option is required if you have invoked the Crypto Officer / Crypto User roles and are performing this action as the Crypto User.

Example

```
lunash:> partition activate -partition b1

Please enter the password for the partition:
> *******
Luna PED operation required to activate partition on HSM - use User or Partition Owner (black)
PED key.
'partition activate' successful

Command Result : 0 (Success)
```

partition backup

Backup the HSM partition contents to a backup HSM. This command copies the contents of a HSM Partition to a special SafeNet backup token. The backup token is initialized during this process. The user is prompted to verify if this destructive command should continue (in case the token has any data on it).

The backup token is initialized to the same access control level as the HSM Partition being backed up.

This command requires the HSM's domain (string or PED Key) and the HSM Partition's Owner password (or PED Key and Partition password). If you chose MofN (values for N and for M greater than 1) at partition creation time, then quantity M of the black key are needed.

Because this is a destructive command (it initializes the backup token) , the user is given the option to proceed/quit before continuing. The Luna appliance admin may wish to use the **token show** command to see the label of a token before issuing this destructive command.

Password-authenticated HSMs

If the passwords and domain aren't provided via the command line, the user is interactively prompted for them. User input is echoed as asterisks. The user is asked to confirm new token Admin and user passwords (if needed).

PED-authenticated HSMs

Luna SA with Trusted Path Authentication backup tokens do not use text Partition Passwords in addition to PED Keys – they require only the PED Keys. Also, the passwords and blue/black PED Keys used for the backup token need not be the same as those used with the HSM.

Syntax

partition backup -partition <name> **-tokenPar** <name> **-serial** <serialnum> [**-password** <password>] [**-tokenSOPwd** <password>] [**-tokenPw** <password>] [**-domain** <domain>] [**-defaultdomain**] [**-add**] [**-replace**] **[-force**]

Parameter	Shortcut	Description
-add	-a	Add objects to the named backup HSM partition. Incremental backup (append). If any of the source objects already exist on the target partition, they are not duplicated, and they are not overwritten. The system flags an error and continues to the next object. This parameter is mandatory for pre-existing target partitions, if **-replace** is not specified. **Note:** This parameter is not needed if the target partition did not already exist and is being created by the partition backup command. If the target partition exists, then there is no default - you must specify whether to add/append to whatever exists on the partition, or overwrite it.
-defaultdomain	-de	Use the default domain string. Deprecated. This is retained only for benefit of customers who have previously used the default domain, and are constrained to continue using it, until they create new objects on an HSM with a proper domain. For security reasons, avoid this option.

Parameter	Shortcut	Description
-domain	-do	Specifies the text domain string that was used when creating the partition. This parameter is optional on password-authenticated HSMs. It is ignored on PED-authenticated HSMs. See the notes, below, for more information. **Note 1:** For Luna HSMs with Trusted Path Authentication, the red PED Key used for initializing the partition on the source HSM must be used for the backup HSM, as well. Ensure that a new domain is not created on the PED Key by answering NO to the Luna PED question “Do you wish to create a new domain?”. **Note 2:** When you call for a cloning operation (such as backup or restore), the source HSM transfers a single object, encrypted with the source domain. The target HSM then decrypts and verifies the received blob. If the verification is successful, the object is stored at its destination – the domains are a match. If the verification fails, then the blob is discarded and the target HSM reports the failure. Most likely the domain string or the domain PED Key, that you used when creating the target partition, did not match the domain of the source HSM partition. The source HSM moves to the next item in the object list and attempts to clone again, until the end of the list is reached. This means that if you issue a backup command for a source partition containing several objects, but have a mismatch of domains between your source HSM partition and the backup HSM partition, then you will see a separate error message for every object on the source partition as it individually fails verification at the target HSM. **Note 3:** If you do not specify a domain in the command line when creating a partition (partition create command),then you are prompted for it. The character string that you type at the prompt becomes the domain for the partition. When you run the partition backup command, you are again prompted for a domain for the target partition on the backup HSM. You can specify a string at the command line, or omit the parameter at the command line and specify a string when prompted. The domain that you apply to a backup HSM must match the domain on your source HSM partition.
-force	-f	Force the action without prompting.
-partition	-par	The name of the HSM partition from which all data/key objects are backed up. Obtain the HSM partition name by using the **partition list** command.
-password	-pas	The applicaton partition Crypto Officer's text password to be used

Parameter	Shortcut	Description
		for login. If you do not supply this value on the command line, you are prompted for it. This parameter is mandatory for password-authenticated HSMs. It is ignored for PED-authenticated HSMs.
-replace	-r	Clone objects to the target partition, overwriting whatever might already exist there. This parameter is mandatory for pre-existing target partitions, if **-add** is not specified. **Note:** This parameter is not needed if the target partition did not already exist and is being created by the partition backup command. If the target partition exists, then there is no default - you must specify whether to add/append to whatever exists on the partition, or overwrite it.
-serial	-s	Specifies the backup token serial number.
-tokenPar	-tokenpa	This is the name of the partition on the backup HSM, to which the backup objects are to be cloned. If a partition exists on the backup HSM with the name that you provide, here, that partition is selected. If no partition exists with the supplied label, then one is created. **Note:** Do not begin your partition label with a numeral. This can later be misinterpreted by some commands as a slot number, rather than a text label, resulting in failure of the command.
-tokenPw	-tokenpw	The token user password . This is the equivalent of Crypto Officer password for the backup partition on the Backup HSM. This parameter is mandatory for password-authenticated HSMs. It is ignored for PED-authenticated HSMs.
-tokenSOPwd	-tokenS	Token Admin (or Security Officer) password. This is the password to be used as login credential for the Backup HSM's security officer. The token SO password need not be the same password or PED Key as used for the source HSM Admin.

Example

```
lunash:> partition backup -partition j1 -password userpin

CAUTION:  Are you sure you wish to initialize the backup
HSM named:
backuphsm
Type 'proceed' to continue, or 'quit' to quit now.
> proceed

Luna PED operation required to initialize backup token - use blue PED Key.
Luna PED operation required to login to backup token - use blue PED Key.
Luna PED operation required to generate cloning domain on backup token - use red PED Key.
Luna PED operation required to generate partition backup space - use black PED Key.
Luna PED operation required to login to partition backup space - use black PED Key.
Luna PED operation required to login to partition - use black PED Key.
Key handle 10 cloned from source to target.
Key handle 11 cloned from source to target.
'partition backup' successful.
```

partition changepolicy

Change HSM Admin-modifiable elements from the HSM partition policy. This command toggles or alters a policy of the specified HSM partition. Only certain portions of the policy set are HSM Admin-modifiable. These policies and their current values can be determined using the **partition showpolicies** command. After a successful policy change, the command displays the new policy value.

This command must be executed by the Luna appliance “admin” logged in to the HSM as HSM Admin. If the HSM Admin is not authenticated, a “user not logged in” error message is returned.

This command can set a policy on or off, or set it to a certain value if it is a numerical policy. Policies can be set only to more restrictive values than the associated capability. You cannot relax a policy to a less-restrictive setting than the associated capability value. See the Capabilities and Policies section of this Reference Help, for a list of all partition capabilities/policies and their meanings.

Syntax

partition changePolicy -partition <name> **-policy** <policycode> **-value** <numvalue>

Parameter	Shortcut	Description
-partition	-pa	Specifies the name of the HSM Partition on which to alter policies. HSM Partition names are obtained with the **partition -list** command.
-policy	-po	Specifies the policy code of the policy to alter. Policy descriptions and codes are obtained with the **partition showpolicies** command.
-value	-v	Specifies the value that should be assigned to the specified policy. When specifying values for a on/off type policy, use '1' for on and '0' for off.

Example

```
lunash:> partition changePolicy -partition c1 -policy 22 -value 0

'partition changePolicy' successful.

Policy “Allow activation” is now set to: 0
```

partition changepw

Change the password for the named HSM Partition. This command sets a partition password or PED Key. For PED-authenticated HSMs, this command invokes the Luna PED to change the value on the black PED Key and on the named partition, as well as allowing you to change the partition password (the challenge secret) supplied by the Luna PED, and used by client applications. For password-authenticated HSMs, this command changes the partition password.

> **Note:** The option to "generate a new random challenge" is present for the Partition SO, only. Crypto Officer and Crypto User are allowed to change their challenge secrets to a string input via keyboard. If a new, random or default challenge is desired (generated by Luna PED), it is triggered by the SO using the "partition resetPw command.

Syntax

partition changePw -partition <partition_name> [**-cu**] [**-newpw** <partition_password>] [**-oldpw** <partition_password>]

Parameter	**Description**
-cu	Use this option if you have invoked the Crypto Officer / Crypto User role distinctions, and wish to change passwords as Crypto User.
-newpw	Specifies the new partition password.
-oldpw	Specifies the existing partition password, to be replaced by the new password.
-partiton	Specifies the partition name. HSM Partition names are obtained with the **partition -list** command.

Example

Example if you provide -oldpw and -newpw at the command line:

```
lunash:> partition changePw -partition mypar1 -oldpw XxPJNH4bY439FNPE -newpw MyPa$$w0rd

Luna PED operation required to activate partition on HSM - use User or Partition Owner (black)
PED Key.
'partition -changePw' successful.

Command Result : 0 (Success)
```

Example for Partition SO, if you do not provide -oldpw and -newpw at the command line:

```
lunash:> partition changePw -partition mypar1

Which part of the partition password do you wish to change?
1. change partition owner (black) PED key data
2. generate new random password for partition owner
3. specify a new password for the partition owner
4. both options 1 and 2
0. abort command
```

```
Please select one of the above options: 3

> ****************
Please enter the password for the partition:
>********

Please enter a new password for the partition:
>********

Luna PED operation required to activate partition on HSM - use User or Partition Owner (black)
PED Key


'partition -changePw' successful.

Command Result : 0 (Success)
```

Example for Partition Crypto Officer or Crypto User, if you do not provide -oldpw and -newpw at the command line:

```
lunash:> partition changePw -partition mypar1

Which part of the partition password do you wish to change?
1. change partition owner (black) PED key data
2. specify a new password for the partition owner
0. abort command
Please select one of the above options: 3

> ****************
Please enter the password for the partition:
>********

Please enter a new password for the partition:
>********

Luna PED operation required to activate partition on HSM - use User or Partition Owner (black)
PED Key


'partition -changePw' successful.

Command Result : 0 (Success)
```

partition clear

Delete all objects on a partition. Because this is a destructive command, the user is prompted to proceed/quit before the erasure occurs.

For password-authenticated HSMs, if the password isn't entered on the command line, the user will be prompted for it interactively. User input will be echoed as asterisks.

For PED-authenticated HSMs, PED action is required, and the Partition Owner PED Key (black) is requested. Any password provided at the command line is ignored. However, if a PED PIN was specified when the HSM partition was created, that PED PIN must be entered at the PED keypad.

Syntax

partition clear -partition <partitionname> **-password** <password> [**-force**]

Parameter	Shortcut	Description
-force	-f	Force the action without prompting.
-partition	-par	Specifies the name of the partition from which all objects are to be erased. To obtain a list of partitions, use the **partition list** command.
-password	-pas	The password to be used as login credential by the partition's user. This parameter is required on password-authenticated HSMs.

Example

```
lunash:> partition -clear -partition b2

Please enter the password for the partition:
> *******

CAUTION:  Are you sure you wish to clear the partition named:
b2
This will ERASE all the objects on the partition.
Type 'proceed' to clear the partition, or 'quit' to quit now.
> proceed

'partition -clear' successful.
```

partition create

Create an HSM partition on the HSM. This command creates and initializes a new HSM Partition on the HSM. To use the HSM partition create command you must be logged in to the HSM as HSM Admin (a.k.a. the SO).

By default, no clients are granted access to a new HSM Partition. The Luna appliance “admin” can run the **client assignPartition** command to give a registered client access to created HSM Partitions.

For password-authenticated HSMs, if the password is not provided via the command line, the user is interactively prompted for it. Input is echoed as asterisks, and user is asked for password confirmation.This creates the Crypto Officer role.

For PED-authenticated HSMs, PED action is required, and a partition Crypto Officer PED Key (black) is imprinted. Any password provided at the command line is ignored.

⚠ **CAUTION:** When labeling HSMs or partitions, never use a numeral as the first, or only, character in the name/label. Token backup commands allow slot-number or label as identifier, which can lead to confusion if the label is a string version of a slot number. For example, if the token is initialized with the label "1" then the user cannot use the label to identify the target for purposes of backup, because VTL parses "1" as signifying the numeric ID of the first slot rather than as a text label for the target in whatever slot it really occupies (the target is unlikely to be in the first slot), so backup fails.

Note: If you create a partition with name "somename" and do not specify a label, the label by default is "somename". If later you attempt to create another partition, and specify a label of "somename" the operation fails with LUNA_RET_ATTRIBUTE_VALUE_INVALID because the first partition has that label (even though you never explicitly set it to that string.

Partition and PKI token naming

When creating partitions on the HSM, a check is performed to ensure that the new partition's name is unique (on that HSM). However, this check does not extend to any token HSMs that might be inserted in connected card-reader slots. Therefore, it is possible to create a partition on the main, on-board HSM that has the same name as a PKI token in one of the reader slots. Avoid this by running the command **token pki listdeployed**, and checking the output, before invoking the **partition create** command.

Cloning is a repeating atomic action

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

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

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

Domain matching and the default domain

If you do not specify a domain in the command line when creating a partition (**partition create** command),then you are prompted for it.

If you type a character string at the prompt, that string becomes the domain for the partition.

When you run the partition backup command, you are again prompted for a domain for the target partition on the backup HSM. You can specify a string at the command line, or omit the parameter at the command line and specify a string when prompted. Otherwise press [Enter] with no string at the prompt to apply the default domain. The domain that you apply to a backup HSM must match the domain on your source HSM partition.

Syntax

partition create -partition <name> [**-haspso**] [**-label** <label>] [**-password** <password>] [**-domain** <domain>] [**-defaultdomain**] [**-defaultchallenge**] [**-size** <size>] [**-allfreestorage**] [**-force**]

> **Note:** A partition **name** or a partition **label** can include any of the following characters :
>
> !#$%'()*+,-./0123456789:=@ABCDEFGHIJKLMNOPQRSTUVWXYZ[]^_
> abcdefghijklmnopqrstuvwxyz{}~
> No spaces, unless you wish to surround the name or label in double quotation marks every time it is used.
> No question marks, no double quotation marks within the string.
> Minimum name or label length is 1 character. Maximum is 32 characters.
>
> Valid characters that can be used in a **password** or in a cloning **domain**, when entered via Luna Shell (*lunash*[1]), are:
>
> !#$%'*+,-./0123456789:=?@ABCDEFGHIJKLMNOPQRSTUVWXYZ[]^_
> abcdefghijklmnopqrstuvwxyz{}~
> (the first character in that list is the space character)
> Invalid or problematic characters, not to be used in passwords or cloning domains are
> "&';<>\`|()
>
> Valid characters that can be used in a **password** or in a cloning **domain**, when entered via *lunacm*, are:
>
> !"#$%&\'()*+,-./0123456789:;<=>?@ABCDEFGHIJKLMNOPQRSTUVWXYZ[\\]^_
> `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] Luna Shell on the Luna SA 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 Luna

> Shell 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.

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

Parameter	Shortcut	Description
-allfreestorage	-a	Create the partition using all the remaining, unused storage space on the HSM. After creating a partition with this option, you cannot create another without first deleting or resizing partitions to regain some space.
-defaultdomain	-defaultd	This "partition create" command, and the "setLegacyDomain" command both have the "-defaultdomain" option, which allows the use of the same default domain that would have been applied if you had just pressed [Enter] when prompted for a cloning domain with earlier Luna HSM versions. The current and future HSM versions do not allow you to omit providing a domain, unless you include this "-defaultdomain" option, which is an insecure choice and generally not recommended. The "-defaultdomain" option applies to Password-authenticated HSMs only. For PED-authenticated HSMs the PED always prompts for a physical PED Key and either reuses the value on the key that you insert, or generates a new value and imprints it on the PED Key.
-defaultchallenge	-defaultc	Specifies that the default Partition Challenge Secret 'PASSWORD' be used when the partition is created. This is useful when deploying many partitions automatically, for fully-automated testing, and when using Crypto Command Center (CCC) to create an HA group, which requires all member partitions to share the same password. The challenge password 'PASSWORD' is reserved, so it is not possible to change an existing challenge password to 'PASSWORD'.
-domain	-do	Specifies the cloning domain to be used when this partition needs to clone objects to/from another HSM, such as during backup/restore, or if the partition is included as a member of an HA group. For PED authenticated Luna SA, the domain is either generated on the HSM and imprinted on a red PED Key, or is accepted from an existing domain PED Key and imprinted on the HSM (for this partition).
-force	-f	Force the partition creation with no prompting - you are still prompted by Luna PED, if yours is a PED authenticated HSM.
-haspso	-h	Create the partition with its own security officer. See "About Configuring an Application Partition with Its Own SO " on page 1 in

Parameter	Shortcut	Description
		the *Configuration Guide*.
-label	-l	Specifies a label for the partition. This option does not apply to partitions with SO. If you include this option with the -haspso, it will be ignored. A partition label is applied later by the Partition SO, using the client-side lunacm tool.
-partition	-par	Specifies the name to assign to the HSM Partition. The name must be unique among all HSM Partitions on the HSM.
-password	-pas	Specifies the password to be used as login credential by the password-authenticated HSM partition's Crypto Officer or client application. If you omit the password from the command, for a password-authenticated Luna SA, you are prompted for it. For PED authenticated Luna SA, the password is not needed as input - one is generated and presented to you by the PED - and the black PED Key becomes the administrative authentication (for activation, etc.)
-size	-s	Specifies the size, in bytes, to allocate to the partition, from the remaining storage available on the HSM. If you specify a size, the HSM attempts to use it after calculating overhead requirements. If you do not specify a size, the HSM creates the partition with the default size, as determined by your purchased options for number of partitions and total storage on the HSM.

Example

```
lunash:> partition -create -par alreadyused

Error:  'partition -create' failed. (1006)
Error:  The name you provided for the new partition is not unique. Partitions must have unique
names.
Use 'partition -list' for a list of existing partition names.

lunash:> partition -create -par b1

Please enter password
Please enter domain
Please enter size
'partition -create' successful.
```

partition createuser

The Crypto Officer creates a Crypto User on a partition.
For Luna HSM with firmware 6.22.0 and newer, this command applies to either PED-authenticated or Password-authenticated HSMs.
The Crypto Officer's password is included as authentication before specifying the password that is assigned to the new Crypto User.

For older Luna HSM firmware versions, this command applied only to PED-authenticated HSMs, and had only the "-partition" option.

Syntax

partition createuser -partition <partition_name> [**-coPassword** <password>] [**-cuPassword** <password>] [**-defaultChallenge**]

Parameter	Shortcut	Description
-partition	**-p** **<name>**	The name of the HSM partition on which to create the Crypto User. Obtain the HSM partition name by using the **partition list** command.
-coPassword	**-co** **<password>**	The password of the Crypto Officer, when creating a Crypto User on a password-authenticated HSM.
-cuPassword	**-cu** **<password**	The Crypto User password, being assigned when creating a Crypto User on a password-authenticated HSM.
-defaultChallenge	**-d** **.**	For PED-authenticated HSM, sets the default challenge string "PASSWORD", instead of getting a random, 16-character string from Luna PED.

Example creating Crypto User on password-authenticated HSM partition

```
lunash:> partition createuser -partition b1 -coPassword somePWstring -cuPassword someother-
PWstring

'partition createuser' successful.
```

Example creating Crypto User on PED-authenticated HSM partition

Note: For PED-authenticated HSM, the **partition createuser** dialog directs you to the PED for two separate PED Key operations.

The first time, you provide the black PED Key for authentication by the Crypto Officer that was created when the application partition was first initialized.

The second time, if you have the newer label sheets that include gray stickers, you provide a PED Key labeled with a gray sticker; otherwise, just use a black-labeled PED Key, but be sure to identify that key as Crypto User, to prevent confusing it with the black Crypto Officer key.

```
[MyLunaSA2] lunash:>partition show

   Partition Name:                            P1SA2
   Partition SN:                              356654569703
   Partition Label:                           P1SA2
   Crypto Officer   PIN To Be Changed:        no
   Crypto Officer   Challenge To Be Changed:  no
   Crypto Officer   Locked Out:               no
   Crypto Officer   Login Attempts Left:      10
   Crypto Officer   is activated:             no
   Crypto User      is not initialized.
   Legacy Domain Has Been Set:                no
   Partition Storage Information (Bytes):     Total=2087864, Used=0, Free=2087864
   Partition Object Count:                    0


Command Result : 0 (Success)
[MyLunaSA2] lunash:>partition createuser -partition P1SA2 -d


  Please enter Crypto Officer password for the partition:
  > *******

Warning:  This partition will be created with default challenge password.

Luna PED operation required to activate partition on HSM - use Partition Owner (black) PED key.

Luna PED operation required to create user on partition - use Crypto User (black) PED key.

'partition createuser' successful.


Command Result : 0 (Success)
[MyLunaSA2] lunash:>partition show

   Partition Name:                            P1SA2
   Partition SN:                              356654569703
   Partition Label:                           P1SA2
   Crypto Officer   PIN To Be Changed:        no
   Crypto Officer   Challenge To Be Changed:  no
   Crypto Officer   Locked Out:               no
   Crypto Officer   Login Attempts Left:      10
   Crypto Officer   is activated:             no
   Crypto User      PIN To Be Changed:        no
   Crypto User      Challenge To Be Changed:  yes
   Crypto User      Locked Out:               no
   Crypto User      Login Attempts Left:      10
   Crypto User      is activated:             no
   Legacy Domain Has Been Set:                no
   Partition Storage Information (Bytes):     Total=2087864, Used=0, Free=2087864
   Partition Object Count:                    0
```

```
Command Result : 0 (Success)
[MyLunaSA2] lunash:>
```

partition deactivate

De-cache a partition's PED key data. clients cannot authenticate to the partition with just their partition password. While the partition is deactivated, each client attempt initiates a login call, which invokes Luna PED operation with the appropriate black PED Key.

Syntax

partition deactivate -partition <partitionname>

Parameter	Shortcut	Description
-partition	**-p**	The name of the HSM partition to delete. Obtain the HSM partition name by using the **partition list** command.

Example

```
lunash:> partition deactivate -partition b1

'partition deactivate' successful.
```

partition delete

Delete an HSM Partition from the HSM. This command deletes a HSM Partition on the HSM and frees the license used by the HSM Partition. To use the partition delete command you must be logged in to the HSM as HSM Admin.

Syntax

partition delete -partition <partition_name> [**-force**]

Parameter	Shortcut	Description
-force	**-f**	Force the action without prompting.
-partition	**-p**	The name of the HSM partition to deactivate. Obtain the HSM partition name by using the **partition list** command.

Example

```
lunash:> partition delete -partition b1

CAUTION:  Are you sure you wish to delete the partition named:
b1
Type 'proceed' to delete the partition, or 'quit'
to quit now.
> quit
'partition delete' aborted.

lunash:> partition delete -partition b1
CAUTION:  Are you sure you wish to delete the partition named:
b1
Type 'proceed' to delete the partition, or 'quit'
to quit now.
> proceed
'partition delete' successful.
```

partition list

Display a list of the accessible partitions on the HSM, including the number of objects on the partition, the partition size, and the used and free space.

Note: The HSM firmware needs approximately 2K bytes of memory to manage each partition and data objects in it. To avoid you having to calculate the exact memory space available for data storage -- with you deducting the memory used by internal data structures --the "partition list" command adjusts the memory size attributes for you. Thus, the total available memory reported by "partition list" will be different than that reported by "token backup show" and "token backup partition list."

Syntax

partition list

Example

```
lunash:> partition list
Storage (bytes)
Partition        Name     Objects Total    Used     Free
700022006        mypar2   0       102701      0     102701
700022008        mypar1   3       102701   1800     100901
Command Result : 0 (Success)
```

partition resetpw

Resets a Partition Owner's password, or PED key data.

The HSM Admin must be logged in to execute this command. This command is available only if the destructive HSM policy “SO can reset partition PIN” is ON.

This command detects firmware level and determines whether an action is allowed.

For password-authenticated HSMs, if the new password is not provided via the command line, the user is interactively prompted for it. Input is echoed as asterisks, and the user is asked for password confirmation.

For PED-authenticated HSMs, PED action is required, and a Partition Owner PED Key (black) is imprinted. Any password provided at the command line is ignored.

Syntax

partition resetPw -partition <partitionname> [-cu] [-password <password>] [-newpw <password>]

Parameter	Shortcut	Description
-cu	**-c**	Perform task as Crypto-User
-newpw	**-n**	The new password to be used as the HSM Partition Owner's login credential to the named HSM Partition. Requires the SO to be logged in. This parameter is mandatory for password-authenticated HSMs. It is ignored on PED-authenticated HSMs.If you omit the password from the command line, you will be prompted for it (password-authenticated HSMs).
-password	**-pas**	Partition Password
-partition	**-par**	Specifies the name of the HSM Partition ID for which to reset the Owner's PIN. Obtain the HSM partition name by using the **partition list** command.

Example

```
lunash:> partition resetpw -partition mypar

Which part of the partition password do you wish to change?


  1.  change Partition Owner (black) PED key data

  2.  generate new random password for partition owner

  3.  use default password for partition owner

  4.  both options 1 and 2

  5.  change crypto-user (black) PED key data

  6.  generate new random password for crypto-user
  7.  use default password for crypto-user

  0.  abort command

Please select one of the above options: 1

Luna PED operation required to reset partition PED key data - use User or Partition Owner
(black) PED key.

'partition resetPw' successful.

Command Result : (Success)
```

partition resize

Resizes the storage space of the named partition.

Syntax

partition resize -partition <name> [**-size** <size>] [**-allfreestorage**][**-force**]

Parameter	Shortcut	Description
-allfreestorage	**-a**	Resize this partition using all the remaining, unused storage space on the HSM. After creating or resizing a partition with this option, you cannot create another without first deleting or resizing partitions to regain some space.
-force	**-f**	Force the action without prompting.
-partition	**-par**	Specifies the name of the partition.
-size	**-s**	Specifies the size, in bytes, to allocate to the partition, from the remaining storage available on the HSM. If you specify a size (rather than the other option, -allfreestorage), the HSM attempts to use it after calculating overhead requirements that consider your purchased options for number of partitions and total storage remaining on the HSM.

Example

```
lunash:>partition show
Partition SN:   700022008
Partition Name:         mypartition
Activated:      yes
Auto Activation:        yes
Partition Owner Locked Out:     no
Partition Owner PIN To Be Changed:      no
Partition Owner Login Attempts Left:    10 before Owner is Locked Out
Crypto-User Locked Out:         no
Crypto-User Challenge To Be Changed:    no
Crypto-User Login Attempts Left:        10 before Crypto User is Locked Out!
Legacy Domain Has Been Set:     no
Partition Storage Information (Bytes):          Total=102701, Used=0, Free=102701
Partition Object Count:         2
Command Result : 0 (Success)

lunash:> partition resize -partition mypartition -allfreestorage

WARNING ! ! !
All all remaining free storage space will be allocated to this partition.
No more partitions can be created once this command is complete.
If you are sure you wish to continue, then type 'proceed'; otherwise type 'quit'
> proceed
Proceeding...
'partition resize' successful.

Command Result : 0 (Success)
```

```
[sa5] lunash:>partition show
Partition SN:   700022008
Partition Name:         mypartition
Activated:      yes
Auto Activation:        yes
Partition Owner Locked Out:     no
Partition Owner PIN To Be Changed:      no
Partition Owner Login Attempts Left:    10 before Owner is Locked Out
Crypto-User Locked Out:         no
Crypto-User Challenge To Be Changed:    no
Crypto-User Login Attempts Left:        10 before Crypto User is Locked Out!
Legacy Domain Has Been Set:     no
Partition Storage Information (Bytes):          Total=2094996, Used=0, Free=2094996
Partition Object Count:         2

Command Result : 0 (Success)

lunash:> partition resize -partition mypartition -size 102701

'partition resize' successful.

Command Result : 0 (Success)

lunash:>partition show
Partition SN:   700022008
Partition Name:         mypartition
Activated:      yes
Auto Activation:        yes
Partition Owner Locked Out:     no
Partition Owner PIN To Be Changed:      no
Partition Owner Login Attempts Left:    10 before Owner is Locked Out
Crypto-User Locked Out:         no
Crypto-User Challenge To Be Changed:    no
Crypto-User Login Attempts Left:        10 before Crypto User is Locked Out!
Legacy Domain Has Been Set:     no
Partition Storage Information (Bytes):          Total=102701, Used=0, Free=102701
Partition Object Count:         2
Command Result : 0 (Success)
```

partition restore

Restores the contents of an HSM partition from a backup token. This command securely moves contents from a backup token to an HSM partition on the HSM. The Luna SA administrator executing this command has the option of replacing the objects existing on the HSM partition or adding to them. Note that if objects are added to the HSM partition it is possible that the same object may exist twice on the HSM partition with two different object handles.

Because replacing data in a partition is destructive, if this option is selected the user is prompted to proceed/quit.

If the passwords are not provided via the command line, the user is prompted for them interactively. User input is echoed as asterisks.

Syntax

partition restore [**-partition name -password** <password>] [**-tokenpw** <password>] [**-add**] [**-replace** [**-force**]]

Parameter	Shortcut	Description
-add	**-a**	Use this switch (no argument) to specify that the data objects on the backup token shall be added to those already existing on the specified HSM Partition. Note that even objects on the backup token that are identical to objects in the HSM Partition will be added to the HSM Partition when specifying this switch; thus it is possible that the HSM Partition may have two identical objects on it as a result of this command. You must specify either **-add** or **-replace**.
-force	**-f**	Force the action without prompting.
-partition	**-par**	Specifies the name of the HSM partition from which all data/key objects are to be restored. Obtain the HSM partition name by using the **partition -list** command.
-password	**-pas**	Specifies the HSM Partition Owner's (or Crypto Officer's) text password. This parameter is mandatoryfor password-authenticated HSMs. It is ignored on PED-authenticated HSMs.
-replace	**-r**	Use this switch (no argument) to erase any data/key objects existing on the specified HSM Partition before loading the keys from the backup token. You must specify either **-add** or **-replace**.
-serial	**-s**	Specifies the token serial number.
-tokenpar	**-tokenpa**	Specifies the token partition name.
-tokenpw	**-tokenpw**	The password for the user on the backup token. If this is a Secure Authentication & Access Control token, then Luna PED is required and any value provided here is ignored. If you do not enter this parameter you will be prompted for it. This parameter is mandatoryfor password-authenticated HSMs. It is ignored on PED-authenticated HSMs.

Example

The following example is for a PED-authenticated HSM

```
lunash:> partition restore -partition j1 -password userpin -replace
CAUTION:  Are you sure you wish to erase all objects in the
partition named:
j1
Type 'proceed' to continue, or 'quit' to quit now.
> proceed
Luna PED operation required to login to partition backup space - use black PED Key.
Luna PED operation required to login to partition - use black PED Key.
Key handle 8 cloned from source to target.
Key handle 9 cloned from source to target.
'partition restore' successful.
```

partition sff

Access commands to perform backup and restore operations to-and-from a Small Form-Factor Backup device.

Syntax

partition sff

backup
clear
list
restore
showContents

Parameter	Shortcut	Description
backup	**b**	SFF Backup a Partition or Objects. See "partition sff backup " on page 276.
clear	**c**	Clear SFF backup token contents. See "partition sff clear " on page 278.
list	**l**	Get SFF backup token information. See "partition sff list " on page 279.
restore	**r**	Restore Partition or Objects. See "partition sff restore " on page 280.
showContents	**s**	Get SFF backup token objects information. See "partition sff showContents " on page 282.

partition sff backup

Perform backup of a Partition, or selected partition objects, onto a Small Form-Factor Backup token.

Syntax

partition sff backup [**-partition** <name> **-label** <label> [**-password** <password>] [**-objects** <name>] [**-force**]

Parameter	Parameter	Description
-partition	**-par** <name>	Partition Name
-password	**-pas** <password>	Partition Password
-label	**-pas** <label>	Partition Label
-objects	**-pas** <name>	Objects List
-force	**-f** .	Force the action

Example 1 - Backup partition contents

```
lunash:>partition sff backup -partition P1 -label SFFToken1

   WARNING: This operation will backup partition objects to SFF backup token !!!

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

   > proceed
   Proceeding...


  Please enter the password for the HSM user partition:
  > *******

Luna PED operation required to activate partition on HSM - use Partition Owner (black) PED key.


Operation in progress, please wait.

        (1/4):  Backing up object with handle 43... Success!
        (2/4):  Backing up object with handle 41... Success!
        (3/4):  Backing up object with handle 42... Success!
        (4/4):  Backing up object with handle 22... Success!

        Backup Complete.

        4 objects have been backed up to token with label SFFToken1
        on the backup device

'partition sff backup' successful.


Command Result : 0 (Success)
```

Example 2 - Backup specific objects

```
lunash:>partition sff backup -partition P1 -label SFFToken1 -objects 22,41

   WARNING: This operation will backup partition objects to SFF backup token !!!

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

   > proceed
   Proceeding...


  Please enter the password for the HSM user partition:
  > *******

Luna PED operation required to activate partition on HSM - use Partition Owner (black) PED key.


Operation in progress, please wait.

        (1/2):  Backing up object with handle 22... Success!
        (2/2):  Backing up object with handle 41... Success!

        Backup Complete.

        2 objects have been backed up to token with label SFFToken1
        on the backup device

'partition sff backup' successful.


Command Result : 0 (Success)
```

partition sff clear

Clears Small Form-Factor Backup token contents.

Syntax

partition sff clear [**-partition** <name> **-label** <label> [**-password** <password>] [**-objects** <name>] [**-force**]

Parameter	Parameter	Description
-partition	**-par** <name>	Target partition name
-password	**-pas** <password>	Partition Password
-force	**-f** .	Force the action

Example

```
lunash:>partition sff clear -partition P1

Please enter the password for the HSM user partition:
  > *******

Luna PED operation required to activate partition on HSM - use Partition Owner (black) PED key.


'partition sff clear' successful.

Command Result : 0 (Success)

.
```

partition sff list

Gets Small Form-Factor Backup token information.

Syntax

partition sff list [**-partition** <name> **-label** <label> [**-password** <password>] [**-objects** <name>] [**-force**]

Parameter	Parameter	Description
-partition	**-par** <name>	Target partition name
-password	**-pas** <password>	Partition Password
-force	**-f** .	Force the action

Example

```
lunash:>partition sff list -partition P1

  Please enter the password for the HSM user partition:
  > *******

Luna PED operation required to activate partition on HSM - use Partition Owner (black) PED key.


        Partition:      SFFToken1
        Object Type:    Partition
        Object UID:     54030000bc00000779980800


'partition sff list' successful.

Command Result : 0 (Success)
```

partition sff restore

Restore partition objects from a Small Form-Factor Backup token.

Syntax

partition sff restore [**-partition** <name> [**-password** <password>] [**-objects** <name>] [**-force**]

Parameter	Parameter	Description
-partition	**-par** <name>	Target partition name
-password	**-pas** <password>	Partition Password
-objects	**-pas** <name>	Objects List
-force	**-f** .	Force the action

Example 1 - Restore entire content of SFF backup token

```
lunash:>partition sff restore -partition P1

   WARNING: This operation will restore objects from the SFF backup token !!!

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

   > proceed
   Proceeding...


  Please enter the password for the HSM user partition:
  > *******

Luna PED operation required to activate partition on HSM - use Partition Owner (black) PED key.


        Restoring objects...

        (1/4) Restoring object 00-3a050000bc00000779980800-053a4591b-
c955e4e4767ecc220462c1505d982861bb48765d8632798cd7e3ec2...Success - Handle 22
        (2/4) Restoring object 00-39050000bc00000779980800-
ab8f192c2b3d6b14bbed16f4a8ec841c285041c7d657c4a35e6f865898e591d2...Success - Handle 41
        (3/4) Restoring object 00-b90000071f00000079980800-fc980e771f1ed79785cb-
bc484fdf7d00e468b1587af83145f38d0560fa181d58...Success - Handle 42
        (4/4) Restoring object 00-b90000071e00000079980800-26b55de31c7d54b2010b-
f2b236abfc11796ab2991ad41018bd61ead9e219e659...Success - Handle 45

'partition sff restore' successful.


Command Result : 0 (Success)
```

Example 2 - Restore specific objects from SFF backup token

```
lunash:>partition sff restore -partition P1 -objects 1,4

   WARNING: This operation will restore objects from the SFF backup token !!!

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

   > proceed
   Proceeding...


  Please enter the password for the HSM user partition:
  > *******

Luna PED operation required to activate partition on HSM - use Partition Owner (black) PED key.


        Restoring objects...

        (1/2) Restoring object 00-3a050000bc00000779980800-053a4591b-
c955e4e4767ecc220462c1505d982861bb48765d8632798cd7e3ec2...Success - Handle 22
        (2/2) Restoring object 00-b90000071e00000079980800-26b55de31c7d54b2010b-
f2b236abfc11796ab2991ad41018bd61ead9e219e659...Success - Handle 41

'partition sff restore' successful.


Command Result : 0 (Success)
```

partition sff showContents

Gets Small Form-Factor Backup token objects information.

Syntax

partition sff showContents [**-partition** <name> [**-password** <password>] [**-quick**]

Parameter	Parameter	Description
-partition	**-par** <name>	Target partition name
-password	**-pas** <password>	Partition Password
-quick	**-q** .	Show the contents in abbreviated format

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 sff showContents,**, free space must be available within the target partition, equivalent to the size of the largest object on the SFF token.

Example

```
lunash:>partition sff showContents -partition P1

  Please enter the password for the HSM user partition:
  > *******

Luna PED operation required to activate partition on HSM - use Partition Owner (black) PED key.


        Listing SFF Backup contents...

        Found 4 backup objects:

        Partition:      SFFToken1
        Object Type:    Partition
        Object UID:     54030000bc00000779980800

        Label:          Generated DES3 Key
        Index:          1
        Object Type:    Public Key
        Object UID:     3a050000bc00000779980800
        Fingerprint:    053a4591bc955e4e4767ecc220462c1505d982861bb48765d8632798cd7e3ec2

        Label:          Generated AES Key
        Index:          2
        Object Type:    Public Key
        Object UID:     39050000bc00000779980800
        Fingerprint:    ab8f192c2b3d6b14bbed16f4a8ec841c285041c7d657c4a35e6f865898e591d2

        Label:          Generated RSA Private Key
        Index:          3
        Object Type:   Symmetric Key
        Object UID:    b90000071f00000079980800
        Fingerprint:   fc980e771f1ed79785cbbc484fdf7d00e468b1587af83145f38d0560fa181d58

        Label:         Generated RSA Public Key
        Index:         4
        Object Type:   Private Key
        Object UID:    b90000071e00000079980800
        Fingerprint:   26b55de31c7d54b2010bf2b236abfc11796ab2991ad41018bd61ead9e219e659


'partition sff showContents' successful.

Command Result : 0 (Success)
```

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 whose contents are to be migrated to the Luna SA 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 token HSM whose contents are to be migrated to the Luna SA 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.

As well, 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 -partition <name> [**-password** <password>] [**-domain** <domain>]

Parameter	Shortcut	Description
-domain	**-d**	Specifies the legacy cloning domain name. This parameter is required on password-authenticated HSMs. It is ignored on PED-authenticated HSMs.
-partition	**-par**	Specifies the partition name.
-password	**-pas**	Specifies the partition password. This parameter is required on password-authenticated HSMs. It is ignored on PED-authenticated HSMs.

Example

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

The PED prompts for the legacy red domain PED Key (notice mention of "raw data" in the PED mes-
sage).
Command result: Success!
```

partition show

Display a detailed list of accessible partitions with relevant information. This command outputs information about one or all partitions on the Luna appliance's key card (the HSM). It is not necessary to be logged in as HSM Admin to execute this command.

For each partition that is present, the following information is displayed:

- partition serial number
- partition name
- primary authentication status (activated or not)
- partition auto-authenticate status
- user lock-out statue
- HSM serial number
- HSM label
- HSM firmware version

Syntax

partition show [<partition_name>]

Parameter	Shortcut	Description
<partition_name>		Specifies the name of the partition for which to display information. By default information about all partitions is shown. Obtain the partition name by using the partition list command.

Example

```
lunash:> partition show -partition mypar
Partition SN:

65010001
Partition Name:

mypar1
Activated:

yes
Auto Activation:

yes
Partition Owner Locked Out:

no
Partition Owner PIN To Be Changed:

no
Partition Owner Login Attempts Left:

10 before Owner is Locked Out
Crypto-User Locked Out:
```

```
no
Crypto-User Challenge To Be Changed:

no
Crypto-User Login Attempts Left:

10 before Crypto User is Locked Out!
Legacy Domain Has Been Set:

no
Partition Storage Information (Bytes):

Total=102701, Used=1800, Free=100901
Partition Object Count:

3
Command Result : 0 (Success)
```

partition showcontents

Display a list of all objects on a partition. The partition name, serial number and total object count is displayed. For each object that is found, the label and object type are displayed.

For Luna SA with Password Authentication, if the HSM Partition Owner password isn't entered on the command line, the user is prompted for it interactively. User input is echoed as asterisks.

For Luna SA with PED [Trusted Path] Authentication, PED action is required, and the Partition Owner PED Key (black) is requested. Any password provided at the command line is ignored. However, if a PED PIN was specified when the HSM Partition was created, that PED PIN must be entered at the PED keypad.

Syntax

partition showcontents -partition <partition_name> [-cu] **-password** <password>

Parameter	Shortcut	Description
-cu	**-c**	Perform task as Crypto-User. This option is required if you are using the Crypto-Officer/Crypto-User distinction.
-partition	**-par**	Specifies the name of the HSM Partition for which contents are to be displayed. Obtain the HSM Partition name by using the partition -list command.
-password	**-pas**	The HSM Partition Owner password or partition challenge password.

Example

```
lunash:> partition showContents -partition c1

Please enter the password for the partition:
> *******
Partition Name: c1
Partition SN: 150520009
Storage (Bytes): Total=102701, Used=1800, Free=100901
Number objects: 3

Object Label: Generated DES Key
Object Type: Symmetric Key

Object Label: Generated RSA Public Key
Object Type: Public Key

Object Label: Generated RSA Private Key
Object Type: Private Key

Command Result : 0 (Success)
```

partition showpolicies

Display the policy vectors of the specified HSM partition. This command displays the specified HSM Partition's policies and capabilities. The output is arranged into three sections

1. Capabilities
2. Write-restricted policies
3. HSM Admin-modifiable policies.

Each policy's current setting is displayed. For modifiable policies, the policy code is displayed for use when changing policies.

Syntax

partition showpolicies -partition <partition_name> [**-configonly**]

Parameter	Shortcut	Description
-configonly	**-c**	List only the HSM Admin-modifiable HSM partition policies.
-partition	**-p**	The name of the partition for which policies will be displayed. To obtain a list of partitions, use the **partition list** command.

Example

```
lunash:> partition showPolicies -partition mypartition

Partition Name: mypartition
Partition Num: 65038002

The following capabilities describe this HSM Partition and can
never be changed.

Description                           Value
===========                           =====
Enable private key cloning            Allowed

Enable private key wrapping           Disallowed

Enable private key unwrapping         Allowed

Enable private key masking            Disallowed

Enable secret key cloning             Allowed

Enable secret key wrapping            Allowed

Enable secret key unwrapping          Allowed

Enable secret key masking             Disallowed

Enable multipurpose keys              Allowed

Enable changing key attributes        Allowed

Enable PED use without challenge      Allowed
```

```
Allow failed challenge responses           Allowed

Enable operation without RSA blinding      Allowed

Enable signing with non-local keys         Allowed

Enable raw RSA operations                  Allowed

Max failed user logins allowed             10

Enable high availability recovery          Allowed

Enable activation                          Allowed

Enable auto-activation                     Allowed

Minimum pin length (inverted: 255 - min)   248

Maximum pin length                         255

Enable Key Management Functions            Allowed

Enable RSA Signing without confirmation    Allowed

Enable Remote Authentication               Allowed

Enable private key unmasking               Allowed

Enable secret key unmasking                Allowed

The following policies are set due to current configuration
of this partition and may not be altered directly by the user.

Description                               Value
===========                               =====
Challenge for authentication not needed   False

The following policies describe the current configuration of this
partition and may be changed by the HSM Security Officer.

Description                               Value      Code
===========                               =====      ====
Allow private key cloning                 On         0

Allow private key unwrapping              On         2

Allow secret key cloning                  On         4

Allow secret key wrapping                 On         5

Allow secret key unwrapping               On         6

Allow multipurpose keys                   On         10

Allow changing key attributes             On         11

Ignore failed challenge responses         On         15

Operate without RSA blinding              On         16
```

```
Allow signing with non-local keys          On          17

Allow raw RSA operations                   On          18

Max failed user logins allowed             10          20

Allow high availability recovery           On          21

Allow activation                           Off         22

Allow auto-activation                      Off         23

Minimum pin length (inverted: 255 - min)   248         25

Maximum pin length                         255         26

Allow Key Management Functions             On          28

Perform RSA signing without confirmation   On          29

Allow Remote Authentication                On          30

Allow private key unmasking                On          31

Allow secret key unmasking                 On          32

Command Result : 0 (Success)
```

service

Access commands that allow you to view or manage services.

Syntax

service

> **list**
> **restart**
> **start**
> **status**
> **stop**

Parameter	Shortcut	Description
list	**l**	Display a list of the services. See "service list" on page 292.
restart	**r**	Restart a service. See "service restart" on page 293.
start	**star**	Start a service. See "service start" on page 295.
status	**stat**	Display the status for a service. See "service status" on page 296.
stop	**sto**	Stop a service. See "service stop" on page 297.

service list

Lists the services that the user can start, stop, restart, or for which the user can request status information.

Syntax

service list

Example

```
lunash:>service list

The following are valid service names:

      cbs     - HSM callback service
      htl     - Host trust link service
      lsta    - Luna SNMP trap agent service
      network - Network service (Needed for ntls, ssh and scp)
      ntls    - Network trust link service
      ntp     - Network time protocol service
      snmp    - SNMP agent service
      ssh     - Secure shell service (Needed for ssh and scp)
      stc     - Secure trusted channel service
      syslog  - Syslog service
      sysstat - System status monitoring (controls LCD)

Command Result : 0 (Success)
```

service restart

Restart a service on the Luna appliance. Services require restarting if their configurations have changed. For example, after changing any network settings using the **network** commands, you should restart the network service to ensure the new settings take affect. Also, after regenerating the server certificate with the sysconf regencert command, you must restart the NTLS service so that the new certificate is used for the NTLA. For a list of services that can be restarted, use the **service list** command.

Restarting a service isn't always the same as doing a service stop followed by a service start. If you restart the network service while connected to the Luna appliance via the network (ssh), you will not lose your connection (assuming no changes were made that would cause a connection loss). However, if you were to stop the network service, you would immediately lose your connection, and you would need to log in via the local console to start the service again. The same applies for the sshd service.

> **Note:** It can sometimes take slightly more than a minute for NTLS to fully restart, depending on where the system was in its normal cycle of operation when you initiated the restart. This is relatively rare, with the usual NTLS restart time being on the order of ten seconds. We mention it here in case you notice an entry like **vtsd: Error: Server Listening Port could not Bind** in the logs. One or more occurrences can be normal behavior unless there is no recovery and no successful restart.

Syntax

service restart <service_name> [**-force**]

Parameter	Shortcut	Description
<service_name>		Specifies the service to restart. **Valid values:** network, ssh, ntls, syslog, ntp, snmp, sysstat
-force	**-f**	Force the action without prompting.

Example

```
lunash:>service restart syslog

Shutting down kernel logger:                               [  OK  ]
Shutting down system logger:                               [  OK  ]
Starting system logger:                                    [  OK  ]
Starting kernel logger:                                    [  OK  ]

Command Result : 0 (Success)

lunash:>service restart ntls

Checking for connected clients before stopping NTLS service:
WARNING !! There are 1 client(s) connected to this Luna SA
appliance.  It is recommended that you disconnect all clients
before stopping or restarting the NTLS service.
If you are sure that you wish to proceed, then type 'proceed', otherwise type 'quit'
> proceed
Proceeding...
Stopping ntls:                                             [  OK  ]
```

```
Starting ntls:                                             [  OK  ]
Command Result : 0 (Success)

lunash:>service restart ssh

Stopping sshd:                                             [  OK  ]
Starting sshd:                                             [  OK  ]
Command Result : 0 (Success)

[myLuna] lunash:>service restart network

Shutting down interface eth0:                              [  OK  ]
Shutting down interface eth1:                              [  OK  ]
Shutting down loopback interface:                          [  OK  ]
Bringing up loopback interface:                            [  OK  ]
Bringing up interface eth0:                                [  OK  ]
Bringing up interface eth1:                                [  OK  ]

Command Result : 0 (Success)

lunash:>service restart ntp

Shutting down ntp:                                         [  OK  ]
Starting ntp:                                              [  OK  ]
Command Result : 0 (Success)

lunash:>service restart snmp
Stopping snmpd:                                            [  OK  ]
Starting snmpd:                                            [  OK  ]
Command Result : 0 (Success)
```

service start

Start a named service on the Luna appliance. Services usually need to be started only if they were stopped with a service stop command, or if the service stopped unexpectedly.

Use the **service list** command to display a list of services that you can stop.

Syntax

service start <service_name>

Parameter	Shortcut	Description
<service_name>		Specifies the service to start. **Valid values:** network, ssh, ntls, syslog, ntp, snmp, sysstat

Example

```
lunash:>service start syslog

Starting system logger:                                     [  OK  ]
Starting kernel logger:                                     [  OK  ]

Command Result : 0 (Success)
```

service status

Display the current status (running/stopped) for the specified service. You may wish to run this command to ensure that specific services are running properly. For example, if troubleshooting a problem with the NTLA, it is wise to ensure that the NTLS service is properly started. If it is not, the server may not be able to resolve itself by the hostname in the server certificate.

Syntax

service status <service_name>

Parameter	Shortcut	Description
<service_name>		Specifies the service for which you want to display the status. **Valid values:** network, ssh, ntls, syslog, ntp, snmp, sysstat

Example

```
lunash:>service status ntp

ntp is not running

Command Result : 0 (Success)
```

service stop

Stop a service on the Luna appliance. Customer support might ask you to stop a particular service. Or, you may wish to control which functions are available on the Luna appliance. For example, if you are performing maintenance and prefer that nobody be able to use the NTLA to connect to the Luna SA, you can stop the NTLS service. A user performing maintenance via the serial port can stop the ssh service to prevent anyone from accessing the Luna appliance.

Use the **service list** command to display a list of services that you can stop.

Syntax

service stop <serviceName>

Parameter	Shortcut	Description
<service_name>		Specifies the service to stop. **Valid values:** network, ssh, ntls, syslog, ntp, snmp, sysstat
-force	**-f**	Force the action without prompting.

Example

```
lunash:> service stop ntls

Checking for connected clients before stopping NTLS service:
There are no connected clients. Proceeding...
Stopping ntls:OK

Command Result : 0 (Success)
```

status

Access commands that allow you to view the current system status.

Syntax

status

> **cpu**
> **date**
> **disk**
> **interface**
> **mac**
> **mem**
> **netstat**
> **ps**
> **sensors**
> **sysstat**
> **time**
> **zone**

Parameter	Shortcut	Description
cpu	**c**	Display the current CPU load. See "status cpu" on page 299.
date	**da**	Display the current date and time. See "status date" on page 300
disk	**di**	Display the current disk usage. See "status disk" on page 301.
interface	**i**	Display the current network interface information. See "status interface" on page 302.
mac	**ma**	Display the current MAC address configuration. See "status mac" on page 303.
mem	**me**	Display the current memory usage. See "status mem" on page 304.
netstat	**n**	Display the current network connections. See "status netstat" on page 305.
ps	**ps**	Display the current status of processes. See "status ps" on page 306
sensors	**se**	Display the sensors output. See "status sensors" on page 308.
sysstat	**sy**	Display system status monitor information. See "status sysstat" on page 310.
time	**t**	Display the current time. See "status time" on page 313.
zone	**z**	Display the current time zone. See "status zone" on page 314.

status cpu

Display the current CPU load. The CPU load data is presented as a series of five entries, as follows:

1. The average CPU load for the previous minute. This value is 0.14 in the example below.
2. The average CPU load for the previous five minutes. This value is 0.10 in the example below.
3. The average CPU load for the previous ten minutes. This value is 0.08 in the example below.
4. The number of currently running processes and the total number of processes. The example below shows 1 of 68 processes running.
5. The last process ID used. This value is 11162 in the example below.

Syntax

status cpu

Example

```
lunash:>status cpu

CPU Load Averages:
0.14 0.10 0.08 1/68 11162
System uptime:
At Fri Jan 10 08:05:23 EST 2014, I am up 45 min

Command Result : 0 (Success)
```

status date

Display the current date and time.

Syntax

status date

Example

```
lunash:>status date

Thu Oct 30 16:28:05 EST 2011

Command Result : 0 (Success)
```

status disk

Display the current disk usage information from the SMART monitoring service.

Syntax

status disk

Example

```
lunash:>status disk
===================== Hard Disk utilization =====================
Filesystem      1K-blocks       Used    Available       Use%    Mounted on
/dev/sda5       988212          124028  813984          14%     /
/dev/sda7       1976492         35784   1840304         2%      /tmp
/dev/sda9       3945128         96496   3648224         3%      /var
/dev/sda10      1976492         35764   1840324         2%      /var/tmp
/dev/sda11      1976492         40712   1835376         3%      /var/log
/dev/sda12      29538432        176576  27861388        1%      /home
/dev/sda8       39381744        594544  36786708        2%      /usr
/dev/sda6       101086  14220   81647   15%     /boot
===================== Hard Disk SMART Report =====================

=== START OF INFORMATION SECTION ===
Device Model: WDC WD1600BEVT-00A23T0
Serial Number: WD-WX91A10N4146
Firmware Version: 04.04V06

=== START OF READ SMART DATA SECTION ===
SMART overall-health self-assessment test result: PASSED
SMART Attributes Data Structure revision number: 16
Vendor Specific SMART Attributes with Thresholds:

ID#     ATTRIBUTE_NAME          FLAG    VALUE   WORST   THRESH  TYPE      UPDATED  WHEN_FAILED  RAW_
VALUE
1       Raw_Read_Error_Rate     124028  200     200     051     Pre-fail  Always        -       0
3       Spin_Up_Time            35784   201     200     021     Pre-fail  Always        -       2933
4       Start_Stop_Count        96496   100     100     000     Old_Age   Always        -       24
5       Reallocated_Sector_Ct   35764   200     200     140     Pre-fail  Always        -       0
7       Seek_Error_Rate         40712   200     200     000     Old_Age   Always        -       0
9       Power_On_Hours          176576  100     100     000     Old_Age   Always        -       101
10      Spin_Retry_Count        594544  100     253     000     Old_Age   Always        -       0
11      Calibration_Retry_Count 0x0012  100     253     000     Old_Age   Always        -       0
12      Power_Cycle_Count       0x0032  100     100     000     Old_Age   Always        -       24
192     Power-Off_Retract_Count 0x0032  200     200     000     Old_Age   Always        -       4
193     Load_Cycle_Count        0x0032  200     200     000     Old_Age   Always        -       385693
194     Temperature_Celsius     0x0022  117     093     000     Old_Age   Always        -       30
196     Reallocated_Event_Count 0x0032  200     200     000     Old_Age   Always        -       0
197     Current_Pending_Sector  0x0012  200     200     000     Old_Age   Always        -       0
198     Offline_Uncorrectable   0x0010  100     253     000     Old_Age   Offline       -       0
199     UDMA_CRC_Error_count    0x0032  200     200     000     Old_age   Always        -       0
200     Multi_Zone_Error_Rate   0x00008 100     253     000     Old_Age   Ofline        -       0

SMART Error Log Version: 1

No Errors Logged

Command Result : 0 (Success)
```

status interface

Display network interface information.

Syntax

status interface

Example

```
lunash:>status interface
eth0      Link encap:Ethernet  HWaddr 00:03:47:E7:56:1A
       inet addr:172.19.11.75  Bcast:172.19.255.255  Mask:255.255.0.0
       UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
       RX packets:9015 errors:0 dropped:0 overruns:0 frame:0
       TX packets:5683 errors:0 dropped:0 overruns:0 carrier:0
       collisions:0 txqueuelen:100
       RX bytes:1040267 (1015.8 Kb)  TX bytes:514608 (502.5 Kb)
       Interrupt:11 Base address:0x7000
eth1      Link encap:Ethernet  HWaddr 00:02:B3:AB:C5:4D
       inet addr:192.168.2.21  Bcast:192.168.2.255  Mask:255.255.255.0
       UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
       RX packets:4539 errors:0 dropped:0 overruns:0 frame:0
       TX packets:595 errors:0 dropped:0 overruns:0 carrier:0
       collisions:539 txqueuelen:100
       RX bytes:2038531 (1.9 Mb)  TX bytes:39281 (38.3 Kb)
       Interrupt:11 Base address:0x9000
lo        Link encap:Local Loopback
       inet addr:127.0.0.1  Mask:255.0.0.0
       UP LOOPBACK RUNNING  MTU:16436  Metric:1
       RX packets:34 errors:0 dropped:0 overruns:0 frame:0
       TX packets:34 errors:0 dropped:0 overruns:0 carrier:0
       collisions:0 txqueuelen:0
       RX bytes:2832 (2.7 Kb)  TX bytes:2832 (2.7 Kb)
Command Result : 0 (Success)
```

status mac

Display the network interface MAC addresses.

Syntax

status mac

Example

```
lunash:>status mac

eth0 00:03:47:EF:67:FE
eth1 00:02:B3:AB:B5:D4

Command Result : 0 (Success)
```

status mem

Display the current memory usage.

Syntax

status mem

Example

```
lunash:>status mem

        total           used    free     shared   buffers       cached
Mem:    2067000         88764   1978236  0        21472         45608
-/+ buffers/cache:      21684   2045316
Swap:   2008084         0       2008084

Command Result : 0 (Success)
```

status netstat

Display the current network connections.

Syntax

status netstat

Example

```
lunash:>status netstat
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN
tcp        0    232 172.19.11.75:22         172.21.100.69:1114      ESTABLISHED
Active UNIX domain sockets (servers and established)
Proto RefCnt Flags       Type       State         I-Node Path
unix  7      [ ]         DGRAM                    746    /dev/log
unix  2      [ ACC ]     STREAM     LISTENING     847    /var/run/acpid.socket
unix  2      [ ]         DGRAM                    23121689
unix  2      [ ]         DGRAM                    6561
unix  2      [ ]         DGRAM                    973
unix  2      [ ]         DGRAM                    882
unix  2      [ ]         DGRAM                    755
unix  2      [ ]         STREAM     CONNECTED     425
Command Result : 0 (Success)
```

status ps

Display the status of the appliance processes.

Syntax

status ps

Example

```
lunash:>status ps
USER            PID     % CPU   %MEM    VSZ     RSS     TTY     STAT     START   TIME   COMMAND
root    1       0.0     0.0     2068    672     ?       Ss      07:19    0:00    init [3]
root    2       0.0     0.0     0       0       ?       S<s     07:19    0:00    [migration/0]
root    3       0.0     0.0     0       0       ?       SN      07:19    0:00    [ksoftirqd/0]
root    4       0.0     0.0     0       0       ?       S<      07:19    0:00    [watchdog/0]
root    5       0.0     0.0     0       0       ?       S<      07:19    0:00    [migration/1]
root    6       0.0     0.0     0       0       ?       SN      07:19    0:00    [ksoftirqd/1]
root    7       0.0     0.0     0       0       ?       S<      07:19    0:00    [watchdog/1]
root    8       0.0     0.0     0       0       ?       S<      07:19    0:00    [events/0]
root    9       0.0     0.0     0       0       ?       S<      07:19    0:00    [events/1]
root    10      0.0     0.0     0       0       ?       S<      07:19    0:00    [khelper]
root    11      0.0     0.0     0       0       ?       S<      07:19    0:00    [kthread]
root    15      0.0     0.0     0       0       ?       S<      07:19    0:00    [kblockd/0]
root    16      0.0     0.0     0       0       ?       S<      07:19    0:00    [kblockd/1]
root    17      0.0     0.0     0       0       ?       S<      07:19    0:00    [kacpid]
root    163     0.0     0.0     0       0       ?       S<      07:19    0:00    [cqueue/0]
root    164     0.0     0.0     0       0       ?       S<      07:19    0:00    [cqueue/1]
root    167     0.0     0.0     0       0       ?       S<      07:19    0:00    [khubd]
root    169     0.0     0.0     0       0       ?       S<      07:19    0:00    [kseriod]
root    238     0.0     0.0     0       0       ?       S       07:19    0:00    [pdflush]
root    239     0.0     0.0     0       0       ?       S       07:19    0:00    [pdflush]
root    240     0.0     0.0     0       0       ?       S<      07:19    0:00    [kswapd0]
root    241     0.0     0.0     0       0       ?       S<      07:19    0:00    [aio/0]
root    242     0.0     0.0     0       0       ?       S<      07:19    0:00    [aio/1]
root    406     0.0     0.0     0       0       ?       S<      07:19    0:00    [kpsmoused]
root    437     0.0     0.0     0       0       ?       S<      07:19    0:00    [ata/0]
root    438     0.0     0.0     0       0       ?       S<      07:19    0:00    [ata/1]
root    439     0.0     0.0     0       0       ?       S<      07:19    0:00    [ata_aux]
root    443     0.0     0.0     0       0       ?       S<      07:19    0:00    [scsi_eh_0]
root    444     0.0     0.0     0       0       ?       S<      07:19    0:00    [scsi_eh_1]
root    445     0.0     0.0     0       0       ?       S<      07:19    0:00    [scsi_eh_2]
root    446     0.0     0.0     0       0       ?       S<      07:19    0:00    [scsi_eh_3]
root    447     0.0     0.0     0       0       ?       S<      07:19    0:00    [scsi_eh_4]
root    448     0.0     0.0     0       0       ?       S<      07:19    0:00    [scsi_eh_5]
root    449     0.0     0.0     0       0       ?       S<      07:19    0:00    [kjournald]
root    475     0.0     0.0     0       0       ?       S<      07:19    0:00    [kauditd]
root    508     0.0     0.0     2240    640     ?       S<s     07:20    0:00    /sbin/udevd -d
root    1318    0.0     0.0     0       0       ?       S<      07:20    0:00    [kstriped]
root    1332    0.0     0.0     0       0       ?       S<      07:20    0:00    [kmpathd/0]
root    1333    0.0     0.0     0       0       ?       S<      07:20    0:00    [kmpathd/1]
root    1334    0.0     0.0     0       0       ?       S<      07:20    0:00    [kmpath_handlerd]
root    1372    0.0     0.0     0       0       ?       S<      07:20    0:00    [kjournald]
root    1374    0.0     0.0     0       0       ?       S<      07:20    0:00    [kjournald]
root    1376    0.0     0.0     0       0       ?       S<      07:20    0:00    [kjournald]
root    1378    0.0     0.0     0       0       ?       S<      07:20    0:00    [kjournald]
root    1380    0.0     0.0     0       0       ?       S<      07:20    0:00    [kjournald]
root    1382    0.0     0.0     0       0       ?       S<      07:20    0:00    [kjournald]
root    1384    0.0     0.0     0       0       ?       S<      07:20    0:00    [kjournald]
root    1941    0.0     0.0     2464    360     ?       Ss      07:20   0:00      irqbalance
root    1955    0.0     0.0     1672    532     ?       Ss      07:20   0:00     /usr/sbin/acpid
root    1985    0.0     0.0     4092    980     ?       Ss      07:20   0:00     /usr/sbin/sshd
root    2001    0.0     0.0     5296    1128    ?       Ss      07:20   0:00     crond
root    2221    0.0     0.1     1676    624     ?       Ss      07:20   0:00     /usr/lunasa/oamp/oamp
root    2240    0.0     0.2     0       0       ?       SN      07:20   0:00     [kipmi0]
root    2263    0.0     0.0     3952    664     ?       S       07:20   0:00     /usr/sbin/ipmievd open
root    2282    0.0     0.0     1516    1516    ?       S<L     07:20   0:00     /usr/lunasa//watchdog/wdt_
root    2302    0.0     0.0     0       0       ?       S<s     07:20   0:00     [kondemand/0]
root    2303    0.0     0.0     0       0       ?       S<s     07:20   0:00     [kondemand/1]
root    2326    0.0     0.0     3512    584     ?       S       07:20   0:00     /usr/sbin/smartd -q never
root    2349    0.0     0.0     2824    1084    ?       S       07:20   0:00     /usr/lunasa/sysstat/syssta
root    2351    0.0     0.0     1784    628     ?       Ss      07:20   0:00     /sbin/mgetty /dev/ttyS0 -
root    3797    0.0     0.1     7300    2176    ?       Ss      07:20   0:00     sshd: admin@pts/0
root    5252    0.0     0.0     1952    844      pts/0          Ss+     07:21    0:00    -lush
root    10589   0.0     0.0     2408    960      pts/0  S+      08:10   0:00     /bin/sh S
root    10590   0.0     0.0     2180    816      pts/0  R+      08:10   0:00     ps auxw
root    11885   0.0     0.0     13424   916     ?       Sl      07:42   0:00     rsyslogd -m 0
root    11889   0.0     0.0     1676    300     ?       Ss      07:42   0:00     rklogd -x
root    16685   0.0     0.1     16488   2512    ?       S       07:36   0:00     /usr/local/sbin/snmpd

Command Result : 0 (Success)
```

status sensors

Displays the fan speed, temperature and voltage of the motherboard and power supply units.

Depending upon when you purchased your Luna SA appliance, the baseboard management controller firmware may be at a revision that reports more data on the power supply units than earlier BMC versions. The first example below shows the output from an earlier version of the BMC firmware. The second example shows the output from a more recent version. In this second example, the right PSU (facing the front of Luna SA) has no A/C power connected to it (it is in an audible alarm state).

Syntax

status sensors [**-log**]

Parameter	Shortcut	Description
-log	-l	Show sensors event logs.

Example

```
lunash:>status sensors

This command displays the fan speed, temperature and voltage of the motherboard and power supply
units.
Sensor           | Reading    | Unit       |status | Thresholds
---------------------------------------------------------------------------------------------
Fan1A          . | 4300.000   | RPM        | ok    | 1000.000  | 2000.000  | na        | na
Fan1B          . | 6300.000   | RPM        | ok    | 1000.000  | 2000.000  | na        | na
Fan2A          . | 4300.000   | RPM        | ok    | 1000.000  | 2000.000  | na        | na
Fan2B          . | 6000.000   | RPM        | ok    | 1000.000  | 2000.000  | na        | na
Fan3A          . | 4500.000   | RPM        | ok    | 1000.000  | 2000.000  | na        | na
Fan3B          . | 5900.000   | RPM        | ok    | 1000.000  | 2000.000  | na        | na
CPU            . | 13.000     | degrees C  | ok    | na        | na        | 72.000    | 89.000
VRD            . | 33.000     | degrees C  | ok    | na        | na        | 90.000    | 100.000
PCH            . | 57.000     | degrees C  | ok    | na        | na        | 90.000    | 100.000
Inlet          . | 22.000     | degrees C  | ok    | na        | na        | 39.000    | 45.000
CHA DIMM 0     . | na         | degrees C  | na    | na        | na        | 87.000    | 97.000
CHA DIMM 1     . | na         | degrees C  | na    | na        | na        | 87.000    | 97.000
CHA DIMM 2     . | na         | degrees C  | na    | na        | na        | 87.000    | 97.000
CHB DIMM 0     . | na         | degrees C  | na    | na        | na        | 87.000    | 97.000
CHB DIMM 1     . | na         | degrees C  | na    | na        | na        | 87.000    | 97.000
CHB DIMM 2     . | na         | degrees C  | na    | na        | na        | 87.000    | 97.000
RAM TMax       . | 0.000      | degrees C  | ok    | na        | na        | 87.000    | 97.000
CPU_VCORE      . | 0.928      | Volts      | ok    | na        | 0.632     | 1.440     | na
VBAT           . | 3.164      | Volts      | ok    | na        | 2.796     | na        | na
3VSB           . | 3.364      | Volts      | ok    | na        | 3.092     | 3.492     | na
3VMain         . | 3.364      | Volts      | ok    | na        | 3.092     | 3.492     | na
+5V            . | 5.126      | Volts      | ok    | na        | 4.692     | 5.304     | na
+12V           . | 11.856     | Volts      | ok    | na        | 11.284    | 12.740    | na
PSU1_Present   . | 0x0        | discrete   | 0x0200| na        | na        | na        | na
PSU2_Present   . | 0x0        | discrete   | 0x0200| na        | na        | na        | na
PSU1_+12V_value. | 12.024     | Volts      | ok    | 11.232    | na        | na        | 13.392
PSU1 Temp_value. | 41.000     | degrees C  | ok    | na        | na        | na        | 115.000
PSU1 FAN_value . | 8000.000   | RPM        | ok    | 300.000   | na        | na        | na
PSU2_+12V_value. | 12.024     | Volts      | ok    | 11.232    | na        | na        | 13.392
PSU2 Temp_value. | 39.000     | degrees C  | ok    | na        | na        | na        | 115.000
PSU2 FAN_value . | 7300.000   | RPM        | ok    | 300.000   | na        | na        | na
```

```
CPU_Thermtrip  . | 0x0        | discrete   | OK     | na         | na         | na         | na

Notes:
NR: Not Reading (Error)
CR: Critical
0.00 RPM means fan unplugged, failed, or sensors not readable
DIMM: Dual In-Line Memory Module
PSU1: Power Supply Unit 1
PSU2: Power Supply Unit 2
Fan1, Fan2 and Fan3 are pluggable modules on the front of the appliance.
Each fan unit contains two fans: A and B.

----------- Power Supplies Status --------------
CPU_Thermtrip  . | OK
----------- Front Cooling Fans Status --------------
Fan1A          . | OK  | 4300 RPM
Fan1B          . | OK  | 6300 RPM
Fan2A          . | OK  | 4300 RPM
Fan2B          . | OK  | 6000 RPM
Fan3A          . | OK  | 4500 RPM
Fan3B          . | OK  | 5900 RPM
PSU1 FAN_value . | OK  | 8000 RPM
PSU2 FAN_value . | OK  | 7300 RPM

-------------- chassis status  -----------------
System Power         : on
Power Overload       : false
Power Interlock      : inactive
Main Power Fault     : false
Power Control Fault  : false
Power Restore Policy : always-on
Last Power Event     : ac-failed
Chassis Intrusion    : inactive
Front-Panel Lockout  : inactive
Drive Fault          : false
Cooling/Fan Fault    : false
Front Panel Control  : none
Command Result : 0 (Success)
```

status sysstat

Access commands that allow you to display system status monitor service information and status code descriptions.

Syntax

status sysstat

code
show

Parameter	Shortcut	Description
code	**c**	Display descriptive text for a status code. See "status sysstat code" on page 311.
show	**s**	Display system status monitor service information. See "status sysstat show" on page 312.

status sysstat code

Code lookup for the system status monitor service. Provide the integer code from the system status monitor and descriptive text will be provided to describe the error.

Syntax

status sysstat code all | <system-status-code>

Parameter	Shortcut	Description
all	**a**	Display descriptions for all system status codes.
<system-status-code>		Specifies the system status code for which you want to display information.

Example

```
lunash:>status sysstat code 25
Code
================
25

System State
================
OOS

Code Description
================
The NTLS is not bound to an Ethernet device. Please run the "ntls show", "ntls bind" and "syslog
tail" commands for more information.

Command Result : 0 (Success)
```

status sysstat show

Display system status monitor service information.

Syntax

status sysstat show

Example

```
lunash:>status sysstat show
Volatile State:
sysstatd (pid 2432) is running...
Service Status: sysstatd (pid 2432) is running...

Non-volatile State:
Disabled

System Status Monitor - Current Status
======================================
Hostname: snake21
Interface eth0: 172.20.11.21
Interface eth1: 192.168.254.1
Software Version: SA:5.x.0-25
System Status: ISO
System Status Code: 60
Status Check Time: 20:47 on 27/10/2012

System State Description
ISO (In Service Okay): The appliance is online and the necessary subsystems are operational.
IST (In Service with Trouble): The appliance is online and the necessary subsystems are oper-
ational with some troubles.
OFL (Off Line): The appliance is not currently connected to the ethernet network and cannot
provide service.
OOS (Out Of Service): The appliance is online but the necessary subsystems are NOT operational.

Command Result : 0 (Success)
```

status time

Display the current time, using the 24 hour clock.

Syntax

status time

Example

```
lunash:> status time

09:41:23

Command Result : 0 (Success)
```

status zone

Displays the current time zone. This command is equivalent to the **sysconf timezone show** command.

Syntax

status zone

Example

```
lunash:> status zone

EST

Command Result : 0 (Success)
```

stc

Access the STC-level commands. Use these commands to configure and manage secure trusted channel (STC) partition-client network links.

You must be logged in as the HSM SO to use the **stc** commands.

Syntax

stc

> **activationtimeout set**
> **activationtimeout show**
> **cipher disable**
> **cipher enable**
> **cipher show**
> **client deregister**
> **client list**
> **client register**
> **hmac disable**
> **hmac enable**
> **hmac show**
> **partition export**
> **partition show**
> **rekeythreshold set**
> **rekeythreshold show**
> **replaywindow set**
> **replaywindow show**
> **status**

Parameter	Shortcut	Description
activationtimeout set	**a se**	Set the activation timeout for an STC link. See "stc activationtimeout set" on page 317.
activationtimeout show	**a sh**	Display the STC link activation timeout for the specified partition. See "stc activationtimeout show" on page 318
cipher disable	**ci d**	Disable the use of a symmetric encryption cipher algorithm for data encryption on an STC link. See "stc cipher disable" on page 319.
cipher enable	**ci e**	Enable the use of a symmetric encryption cipher algorithm used for data encryption on an STC link. See "stc cipher enable" on page 321.
cipher show	**ci s**	List the symmetric encryption cipher algorithms you can use for STC data encryption on the specified partition. See "stc cipher show" on page 323.
client deregister	**cl d**	Deregister a client's STC public key from the specified partition. See "stc client deregister" on page 324.
client list	**cl l**	List the clients registered to the specified partition. See "stc client list" on page 325.

Parameter	Shortcut	Description
client register	**cl r**	Register a client's STC public key to the specified partition. See "stc client register" on page 326
hmac disable	**h d**	Disable the use of an HMAC message digest algorithm for identity verification on an STC link. See "stc hmac disable" on page 327.
hmac enable	**h e**	Enable the use of an HMAC message digest algorithm for integrity verification on an STC link. See "stc hmac enable" on page 328
hmac show	**h s**	List the HMAC message digest algorithms you can use for STC message integrity verification on the specified partition. See "stc hmac show" on page 329
partition export	**p e**	Export the specified partition's public key to a file. "stc partition export" on page 330.
partition show	**p s**	Display the public key and serial number for the current partition. See "stc partition show" on page 331.
rekeythreshold set	**rek se**	Set the key life for the symmetric key used to encrypt data on the STC link for the specified partition. See "stc rekeythreshold set" on page 332.
rekeythreshold show	**rek sh**	Display the key life for the symmetric key used to encrypt data on the STC link for the specified partition. See "stc rekeythreshold show" on page 333.
replaywindow set	**rep se**	Set the size of the packet replay window. See "stc replaywindow set" on page 334
replaywindow show	**rep sh**	Display the current setting for the size of the packet replay window. See "stc replaywindow show" on page 335.

stc activationtimeout set

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.

You must be logged in as the HSM SO to use this command.

Syntax

stc activationtimeout set -partition <partition_name> **-time** <timeout>

Parameter	Shortcut	Description
-partition <partition_name>	**-p** <partition_name>	Specifies the name of the partition for which you want to set the STC link activation timeout.
-time <timeout>	**-t** <timeout>	Specifies the activation timeout, in seconds. **Range:**1-240 **Default:**

Example

```
lunash:> stc a se -par mapleleafs -t 30

Successfully changed the activation timeout for partition mapleleafs to 30 seconds.
```

stc activationtimeout show

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.

You must be logged in as the HSM SO to use this command.

Syntax

stc activationtimeout show -partition <partition>

Parameter	Shortcut	Description
-partition <partition_ name>	**-p** <partition_ name>	Specifies the name of the partition for which you want to display the STC link activation timeout.

Example

```
lunash:> stc a sh -par mapleleafs

The channel activation timeout for partition mapleleafs is 30 seconds.
```

stc cipher disable

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 "stc cipher show" on page 323 to show which ciphers are currently enabled/disabled.

Disabling all of the ciphers turns off symmetric encryption on the link.

You must be logged in as the HSM SO to use this command.

Note: Performance is reduced for larger ciphers.

Syntax

stc cipher disable -partition <partition_name> **-all -id** <cipher_id>

Parameter	Shortcut	Description
-partition <partition_name>	**-p** <partition_name>	Specifies the name of the partition that will perform STC data encryption using the specified cipher.
-all	**-a**	Allow the specified cipher.
-id <cipher_id>	**-id** <cipher_id>	Specifies the numerical identifier of the cipher you want to use, as listed using the command "stc cipher show" on page 323.

Example

```
lunash:>stc cipher show -p mapleleafs

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

STC Encryption: On

Cipher ID    Cipher Name                                 Enabled
_________________________________________________________________
1            AES 128 Bit with Cipher Block Chaining   Yes
2            AES 192 Bit with Cipher Block Chaining   Yes
3            AES 256 Bit with Cipher Block Chaining   Yes

Command Result : 0 (Success)

lunash:> stc cipher disable -par mapleleafs -id 3

AES 256 Bit with Cipher Block Chaining is now disabled.

Command Result : 0 (Success)

lunash:>stc cipher show -p mapleleafs

This table lists the ciphers supported for STC links to the partition. 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   No

Command Result : 0 (Success)
```

stc cipher enable

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 "stc cipher show" on page 323 to show which ciphers are currently enabled/disabled.

You must be logged in as the HSM SO to use this command.

Note: Performance is reduced for larger ciphers.

Syntax

stc cipher enable -partition <partition_name> **-all -id** <cipher_id>

Parameter	Shortcut	Description
-partition <partition_name>	**-p** <partition_name>	Specifies the name of the partition for which you want to enable the specified cipher.
-all	**-a**	Enable all ciphers.
-id <cipher_id>	**-id** <cipher_id>	Specifies the numerical identifier of the cipher you want to use, as listed using the command "stc cipher show" on page 323.

Example

```
lunash:>stc cipher show -p mapleleafs

This table lists the ciphers supported for STC links to the partition. 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      No

Command Result : 0 (Success)

lunash:> stc cipher enable -par mapleleafs -id 3

AES 256 Bit with Cipher Block Chaining is now enabled.

lunash:>stc cipher show -p mapleleafs

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

STC Encryption: On
```

```
Cipher ID    Cipher Name                              Enabled
_________________________________________________________________
1            AES 128 Bit with Cipher Block Chaining   Yes
2            AES 192 Bit with Cipher Block Chaining   Yes
3            AES 256 Bit with Cipher Block Chaining   Yes

Command Result : 0 (Success)
```

stc cipher show

List the symmetric encryption cipher algorithms you can use for data encryption on an STC link. If all ciphers are disabled, symmetric encryption is not used on the link.

You must be logged in as the HSM SO to use this command.

Syntax

stc cipher show -partition <partition_name>

Example

Parameter	Shortcut	Description
-partition <partition_name>	**-p** <partition_name>	Specifies the partition for which you want to display the available ciphers.

```
lunash:>stc cipher show -p mapleleafs

This table lists the ciphers supported for STC links to the partition. 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      No

Command Result : 0 (Success)
```

stc client deregister

Deregister a client's STC public key from the specified partition. You must be the owner of the partition to use this command.

You must be logged in as the HSM SO to use this command.

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

Syntax

stc client deregister -partition <partition_name> **-label** <client_label>

Parameter	Shortcut	Description
-partition <partition_name>	**-p** <partition_name>	Specifies the name of the partition containing the public key you want to deregister.
-label <client_label>	**-l** <client_label>	A string used to identify the client being deregistered.

Example

```
lunacm:> stc client deregister -par mapleleafs -label dkeon

Successfully deregistered the client public key of dkeon in partition mapleleafs
```

stc client list

List the clients registered to the specified partition. You must be logged in as the HSM SO and own the partition to use this command.

Syntax

stc client list -partition <partition_name>

Parameter	Shortcut	Description
-partition <partition_name>	**-p** <partition_name>	Specifies the name of the partition.

Example

```
lunash:> stc client list -par mapleleafs

Client Name   Client Identity Public Key SHA1 Hash
rellis        2fd4e1c67a2d28fced849ee1bb76e7391b93eb1
nullman       de9f2c7fd25e1b3afad3e85a0bd17d9b100db4b3
phenderson    da39a3ee5e6b4b0d3255bfef95601890afd80709
```

stc client register

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

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

Syntax

stc client register -partition <partition_name> **-label** <client_label> **-file** <client_public_key>

Parameter	Shortcut	Description
-partition <partition_name>	**-p** <partition_name>	Specifies the name of the partition.
-label <client_name>	**-l** <client_label>	A string used to identify the client being registered.
-file <client_public_key>	**-f** <client_public_key>	The client public key file as displayed using the command "my file list" on page 178.

Example

```
lunash:> stc client register -par mapleleafs -l bsalming -f 45021294.pem

Successfully registered the client public key of bsalming in partition mapleleafs
```

stc hmac disable

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 "stc hmac show" on page 329 to show which HMAC message digest algorithms are currently enabled/disabled.

Note: All STC links use message integrity verification, so at least one HMAC algorithm must be enabled.

You must be logged in as the HSM SO to use this command.

Syntax

stc hmac disable -partition <partition_name> **-id** <hmac_id>

Parameter	Shortcut	Description
-partition <partition_name>	**-p** <partition_name>	Specifies the partition for which you want to enable an HMAC algorithm.
-id <hmac_id>	**-id** <hmac_id>	Specifies the numerical identifier of the HMAC algorithm you want to disable, as listed using the command "stc hmac show" on page 329.

Example

```
lunash:> stc hmac show -par mapleleafs

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

Command Result : 0 (Success)

lunash:> stc hmac disable -par mapleleafs -id 0

HMAC with SHA 256 Bit is now disabled for partition mapleleafs.

Command Result : 0 (Success)

lunash:> stc hmac show -par mapleleafs

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

Command Result : 0 (Success)
```

stc hmac enable

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 "stc hmac show" on page 329 to show which HMAC message digest algorithms are currently enabled/disabled.

Note: All STC links use message integrity verification, so at least one HMAC algorithm must be enabled.

You must be logged in as the HSM SO to use this command.

Syntax

stc hmac enable -partition <partition_name> **-id** <hmac_id>

Parameter	Shortcut	Description
-partition <partition_name>	**-p** <partition_name>	Specifies the partition for which you want to enable the HMAC algorithm.
-id <hmac_id>	**-id** <hmac_id>	Specifies the numerical identifier of the HMAC algorithm you want to enable, as listed using the command "stc hmac show" on page 329.

Example

```
lunash:> stc hmac show -par mapleleafs

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

Command Result : 0 (Success)

lunash:> stc hmac enable -par mapleleafs -id 0

Command Result : 0 (Success)

HMAC with SHA 256 Bit is now enabled for partition mapleleafs.

lunash:> stc hmac show -par mapleleafs

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

Command Result : 0 (Success)
```

stc hmac show

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

You must be logged in as the HSM SO to use this command.

Syntax

stc hmac show -partition <partition_name>

Example

Parameter	Shortcut	Description
-partition <partition_name>	**-p** <partition_name>	Specifies the partition for which you want to display the available HMAC algorithms.

```
lunash:> stc hmac show -par mapleleafs

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

stc partition export

Export the specified partition's public key to a file. You must be logged in to the partition as the SO to perform this command.

Note: If the HSM is zeroized while STC is enabled, the STC link between LunaSH 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 **stc partition export** 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 LunaSH 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

stc partition export -partition <partition_name>

Parameter	Shortcut	Description
-partition<partition_name>	**-p** <partition_name>	Specifies the name of the partition whose public key you want to export.

Example

```
lunash:> stc partition export -par mapleleafs

Successfully exported partition identity for partition mapleleafs to file: 359693009023.pid
```

stc partition show

Display the public key and serial number for the current partition. You must be logged into the partition as the SO to perform this command.

Syntax

stc partition show -partition <partition_name>

Parameter	Shortcut	Description
-partition<partition_ name>	**-p** <partition_ name>	Specifies the name of the partition whose public key and serial number you want to display

Example

```
lunash:> stc partition show -par mapleleafs

Partition Serial Number:                 359693009023
Partition Identity Public Key SHA1 Hash: ee27ac0376af538a6f15523002c43c7b6febdf34
```

stc rekeythreshold set

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).

You must be logged in as the HSM SO to use this command.

Syntax

stc rekeythreshold set -partition <partition> **-value** <key_life>

Parameter	Shortcut	Description
-partition <partition_ name>	**-p** <partition_ name>	Specifies the name of the partition for which you want to specify the STC rekey threshold.
-value <key_life>	**-v** <key_life>	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

```
lunash:> stc rekeythreshold set -par mapleleafs -v 200

Successfully changed the rekey threshold for partition mapleleafs to 200 million messages.
```

stc rekeythreshold show

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

You must be logged in as the HSM SO to use this command.

Syntax

stc rekeythreshold show -partition <partition_name>

Parameter	Shortcut	Description
-partition <partition_name>	**-p** <partition_name>	Specifies the name of the partition for which you want to display the STC rekey threshold.

Example

```
lunash:> stc rekeythreshold show -par mapleleafs

Current rekey threshold for partition mapleleafs is 400 million messages.
```

stc replaywindow set

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.

You must be logged in as the HSM SO to use this command.

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

stc replaywindow set -partition <partition_name> **-size** <number_of_packets>

Parameter	Shortcut	Description
-partition <partition_name>	**-p** <partition_name>	Specifies the name of the partition.
-size <number_of_packets>	**-s** <number_of_packets>	Specifies the number of packets (commands) in the replay window. **Range:**100-1000 **Default:**120

Example

```
lunash:> stc replaywindow set -par mapleleafs -size 500

Successfully changed the size of the replay window for partition mapleleafs to 500 commands.
```

stc replaywindow show

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.

You must be logged in as the HSM SO to use this command.

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

stc replaywindow show -partition <partition_name>

Parameter	Shortcut	Description
-partition <partition_name>	**-p** <partition_name>	Specifies the name of the partition for which you want to display the STC replay window.

Example

```
lunash:> stc replaywindow show -par mapleleafs

The current replay window size for partition mapleleafs is 500 commands.
```

sysconf

Access commands that allow you to configure the appliance.

Syntax

sysconf

appliance
config
drift
fingerprint
hwregencert
ntp
regencert
securekeys
snmp
ssh
time
timezone

Parameter	Shortcut	Description
appliance	**a**	Access commands that allow you to manage the appliance. See "sysconf appliance" on page 338.
config	**c**	Access the system configuration commands. See "sysconf config" on page 358.
drift	**d**	Access commands that allow you to view and configure the drift. See "sysconf drift" on page 369.
fingerprint	**f**	Display the certificate fingerprints. See "sysconf fingerprint" on page 376.
hwregencert	**h**	Generate or re-generate the Luna appliance server hardware certificate . See "sysconf hwregencert" on page 385
ntp	**n**	Access commands that allow you to view or configure the network time protocol (NTP). See "sysconf ntp" on page 388.
regenCert	**re**	Generate or re-generate the Luna appliance server hardware certificate. See "sysconf regencert" on page 417.
securekeys	**se**	Move the Luna keys used to secure the NTLS link from the Luna appliance's file system into the HSM. See "sysconf securekeys" on page 418.
snmp	**sn**	Access commands that allow you to view or configure the Simple Network Management Protocol (SNMP) settings for Luna appliance. See "sysconf snmp" on page 419.
ssh	**ss**	Access commands that allow you to view or configure the SSH

Parameter	Shortcut	Description
		options on the appliance. See "sysconf ssh" on page 441.
time	**t**	Set or display the time and date. See "sysconf time" on page 453.
timezone	**timez**	Set or display the time zone. See "sysconf timezone" on page 454.

sysconf appliance

Access the **sysconf appliance** commands to manage the appliance.

Syntax

sysconf appliance

```
    cpugovernor
    hardreboot
    poweroff
    reboot
    rebootonpanic
    watchdog
```

Parameter	Shortcut	Description
cpugovernor	**c**	System CPU on-demand governor. See "sysconf appliance cpugovernor" on page 339.
hardreboot	**h**	Reboot the appliance, bypassing graceful closing of services. See "sysconf appliance hardreboot" on page 343.
poweroff	**p**	Power off the appliance. See "sysconf appliance poweroff" on page 344.
reboot	**r**	Reboot the appliance. See "sysconf appliance reboot" on page 345.
rebootonpanic	**rebooto**	System reboot on panic. See "sysconf appliance rebootonpanic " on page 346.
watchdog	**w**	System watchdog. See "sysconf appliance watchdog" on page 350.

sysconf appliance cpugovernor

Access the sysconf appliance governor commands to enable or disable the CPU governor and view the current CPU governor status.

Syntax

The following subcommands are available:

Parameter	Shortcut	Description
disable	**d**	Disable the CPU governor. See "sysconf appliance cpugovernor disable" on page 340.
enable	**e**	Enable the CPU governor. See "sysconf appliance cpugovernor enable" on page 341.
show	**s**	Display CPU governor information. See "sysconf appliance cpugovernor show" on page 342.

sysconf appliance cpugovernor disable

Disable the system CPU on-demand governor. The system contains a CPU governor that lowers the clock frequency to save power in times of low demand. Once in a lower-demand state, as the demand on the processor increases, the governor returns the CPU clock frequency to its former setting. This command disables that function.

Syntax

sysconf appliance cpuGovernor disable

Example

```
lunash:>sysconf appliance cpuGovernor disable

Command Result : 0    (Success)
```

sysconf appliance cpugovernor enable

Enable the system CPU on-demand governor. The system contains a CPU governor that lowers the clock frequency to save power in times of low demand. Once in a lower-demand state, as the demand on the processor increases, the governor returns the CPU clock frequency to its former setting. This command enables that function.

Syntax

sysconf appliance cpugovernor enable

Example

```
lunash:>sysconf appliance cpuGovernor enable

Command Result : 0   (Success)
```

sysconf appliance cpugovernor show

Display the system CPU governor configuration status

Syntax

sysconf appliance cpugovernor show

Example

```
lunash:>sysconf appliance cpugovernor show

System CPU ondemand governor is enabled.

Command Result : 0   (Success)
```

sysconf appliance hardreboot

Perform a hard restart (reboot) of the Luna appliance.

When you do not have convenient physical access to your Luna appliances, this command replaces the "sysconf appliance reboot" command (see "sysconf appliance reboot" on page 345) which performs an orderly soft reboot sequence by ordering a large number of services/daemons to conclude their operations, and logs that process. That is the preferred method of rebooting a Luna SA appliance, if you have physical access and can retry in case any of the processes hangs and prevents the soft reboot sequence from proceeding.

Use the **sysconf appliance hardreboot** command when the appliance is not accessible for physical intervention (such as in a secluded, lights-off facility), if needed. This command bypasses many running processes at shutdown, allowing the reboot to occur without hanging.

Syntax

sysconf appliance hardreboot [**-force**]

Parameter	Shortcut	Description
-force	**-f**	Force the action without prompting.

Example

```
lunash:>sysconf appliance hardReboot
 WARNING !! This command will reboot the appliance without gracefully shutting down.
            All clients will be disconnected.
If you are sure that you wish to proceed, then type 'proceed',
otherwise type 'quit'
   > proceed

login as: admin
admin@192.20.11.22's password:
Last login: Fri Nov 22 10:20:25 2013 from 172.20.10.106

Luna SA 5.4.0-5 Command Line Shell - Copyright (c) 2001-2013 SafeNet, Inc. All rights reserved.

[local_host] lunash:>
[local_host] lunash:>
>
```

sysconf appliance poweroff

Power off the Luna SA appliance.

Appliance reboot and power-off automatically take a snapshot of the system's known state so that a customer can later send that to SafeNet for further investigation. This is useful if the system is not behaving and needs reboot or power-off.

Syntax

sysconf appliance poweroff [**-force**]

Parameter	Shortcut	Description
-force	**-f**	Force the action without prompting.

Example

```
lunash:>sysconf appliance poweroff
     WARNING !! This command will power off the appliance.
All clients will be disconnected and the appliance will require a manual power on for further
access.
If you are sure that you wish to proceed, then type 'proceed', otherwise type 'quit'> proceed
Proceeding...
'hsm supportInfo' successful.
Use 'scp' from a client machine to get file named:
supportInfo.txt
Broadcast message from root (pts/0) (Wed Aug 18 20:05:22 2010):
The system is going down for system halt NOW!
Power off commencing
```

sysconf appliance reboot

Performs a warm restart (reboot) of the Luna appliance, shutting down all running processes in a controlled manner.

Appliance reboot and power-off automatically take a snapshot of the system's known state so that a customer can later send that to SafeNet for further investigation. This is useful if the system is not behaving and needs reboot or power-off.

To deal with the possibility that a controlled shutdown might not be possible, see "sysconf appliance rebootonpanic enable" on page 348.

Syntax

sysconf appliance reboot [**-force**]

Parameter	Shortcut	Description
-force	**-f**	Force the action without prompting.

Example

```
lunash:>sysconf appliance reboot
WARNING !! This command will reboot the appliance.
           All clients will be disconnected.
If you are sure that you wish to proceed, then type 'proceed',
otherwise type 'quit'
   > proceed
 Proceeding...
'hsm supportInfo' successful.
   Use 'scp' from a client machine to get file named:
 supportInfo.txt
     Broadcast message from root (pts/0) (Wed Aug 18 20:05:22 2010):
   The system is going down for reboot NOW!
Reboot commencing
Command Result : 0 (Success)
[myluna] lunash:>
```

sysconf appliance rebootonpanic

Access commands that allow you to enable or disable reboot on panic and show reboot on panic information.

Syntax

sysconf appliance rebootonpanic

disable
enable
show

The following subcommands are available:

Parameter	Shortcut	Description
disable	**d**	Disable system reboot on panic. See "sysconf appliance rebootonpanic disable" on page 347.
enable	**e**	Enable system reboot on panic. See "sysconf appliance rebootonpanic enable" on page 348.
show	**s**	Show system reboot on panic information. See "sysconf appliance rebootonpanic show " on page 349.

sysconf appliance rebootonpanic disable

Disable system automatic reboot on kernel panic.

Syntax

sysconf appliance rebootonpanic disable

Example

```
lunash:>sysconf appliance rebootOnPanic disable

Command Result : 0   (Success)
```

sysconf appliance rebootonpanic enable

Enable automatic reboot in case of problem.

In normal situations, the command "sysconf appliance reboot" on page 345 causes the appliance to shut down in a controlled manner.

This command (sysconf appliance rebootonpanic enable) configures the Luna appliance to automatically reboot in the event that the appliance fails to complete a normal shutdown. In conjunction with the AutoActivation setting, this option can allow Luna HSM cryptographic service to resume after a problem, without need for human intervention.

Syntax

sysconf appliance rebootonpanic enable

Example

```
lunash:>sysconf appliance rebootOnPanic enable

Command Result : 0    (Success)
```

sysconf appliance rebootonpanic show

Display the reboot-on-panic configuration status.

Syntax

sysconf appliance rebootonpanic show

Example

```
 lunash:>sysconf appliance rebootonpanic show

System auto reboot on panic is enabled.

Command Result : 0   (Success)
```

sysconf appliance watchdog

Access commands that allow you to enable or disable the system watchdog and show system watchdog information.

Syntax

sysconf appliance watchdog

```
    disable
    enable
    show
```

The following subcommands are available:

Parameter	Shortcut	Description
disable	**d**	Disable the system watchdog. See "sysconf appliance watchdog disable" on page 351.
enable	**e**	Enable the system watchdog. See "sysconf appliance watchdog enable " on page 352.
show	**s**	Show system watchdog information. See "sysconf appliance watchdog show" on page 353.

sysconf appliance watchdog disable

Disable the system watchdog. The system contains a standard hardware watchdog circuit that constantly monitors the CPU. If the CPU fails to show signs of life, the watchdog can independently trigger a system reboot. This command disables that function.

When the watchdog is enabled (sysconf appliance watchdog enable), look for the following syslog message:

kernel: iTCO_wdt: initialized. heartbeat=30 sec (nowayout=0)

When it is disabled (sysconf appliance watchdog disable), look for this log entry

kernel: iTCO_wdt: Watchdog Module Unloaded.

The absence of these messages on a sysconf appliance watchdog enable and sysconf appliance watchdog disable suggests that the watchdog timer device driver did not load successfully at power up.

Syntax

sysconf appliance watchdog disable

Example

```
lunash:>sysconf appliance watchdog disable

Command Result : 0    (Success)
```

sysconf appliance watchdog enable

Enable the system watchdog. The system contains a standard hardware watchdog circuit that constantly monitors the CPU. If the CPU fails to show signs of life, the watchdog can independently trigger a system reboot. This command enables that function.

When the watchdog is enabled (sysconf appliance watchdog enable), look for the following syslog message:

kernel: iTCO_wdt: initialized. heartbeat=30 sec (nowayout=0)

When it is disabled (sysconf appliance watchdog disable), look for this log entry

kernel: iTCO_wdt: Watchdog Module Unloaded.

The absence of these messages on a sysconf appliance watchdog enable and sysconf appliance watchdog disable suggests that the watchdog timer device driver did not load successfully at power up.

Syntax

sysconf appliance watchdog enable

Example

```
lunash:>sysconf appliance watchdog enable

Command Result : 0    (Success)
```

sysconf appliance watchdog show

Show the system watchdog configuration status.

Syntax

sysconf appliance watchdog show

Example

```
lunash:>sysconf appliance watchdog show

System watchdog is enabled.

Command Result : 0   (Success)
```

sysconf banner

Access the sysconf banner commands to set and clear an extended text banner, displayed to appliance administrative users when they log into a Luna Shell session.

Syntax

sysconf banner

add
clear

Parameter	Shortcut	Description
add	**a**	Add extended banner text from a file. See "sysconf banner add" on page 355 .
clear	**c**	Clear the extended banner text. See "sysconf banner clear" on page 357.

sysconf banner add

Add a custom text banner that is displayed when administrative users connect and log into the appliance. The text is initially obtained from a file. The file must already have been uploaded to the appliance's admin user, via scp/pscp.

Only the "admin" user can perform this operation. The command is not available to "operator".

A single extended banner is set for all users who log in; it is not possible to set different banners for different users or classes of users.

Use the command **user file list** to view available files and verify the name of the desired banner file.

The banner file size is limited to 8KB.

The banner filename is limited to characters a-z, A-Z, 0-9, '.', '-' or '_'.

For the banner text within the file, only standard ASCII characters are accepted (characters between 0 and 127 in http://www.asciitable.com/).

You must be logged into the HSM before issuing the command **sysconf banner add -file** <filename>

Syntax

sysconf banner add -file <filename>

Parameter	Shortcut	Description
-file	**-f** <filename>	Banner text file name.

Example

```
[myluna] lunash:>my file list

      248 Nov  4 12:10 banner2.txt
      213 Nov  4 12:00 banner1.txt
   323902 Nov  4 11:31 supportInfo.txt
    10505 Nov  4 11:29 update5_4_0_4.log
   127067 Oct 15 15:55 fwupdateInfo.txt

Command Result : 0 (Success)
[myluna] lunash:>sysconf banner add -file banner2.txt

Please login as HSM Admin first!

Command Result : 65535 (Luna Shell execution)
[myluna] lunash:>hsm login


Luna PED operation required to login as HSM Administrator - use Security Officer (blue) PED key.

'hsm login' successful.


Command Result : 0 (Success)
[myluna] lunash:>
[myluna] lunash:>sysconf banner add -file banner2.txt
```

```
Command Result : 0 (Success)
[myluna] lunash:> exit


login as: admin
admin@192.20.9.22's password:
Last login: Mon Nov  4 13:17:21 2013 from 192.20.11.20

Luna SA 5.4.0-1 Command Line Shell - Copyright (c) 2001-2013 SafeNet, Inc.
All rights reserved.

      * * * * W A R N I N G ! * * * *

Your use of this resource is monitored and
recorded for security and for quality-control
purposes.


      * * * * * * * * * * * * * * * *



[local_host] lunash:>
```

sysconf banner clear

Remove a custom text banner that is displayed when administrative users connect and log into the appliance. The extended text was previously added from a file with the command **sysconf banner add -file** <filename>. If you wish to change an existing extended banner, simply re-issue the "add" command, naming a file with the new text. This command (**sysconf banner clear**) simply clears any extended banner text completely, with no replacement.

Only the "admin" user can perform this operation. The command is not available to "operator".

You must be logged into the HSM before issuing the command **sysconf banner clear**

Syntax

sysconf banner clear [-force]

Parameter	Shortcut	Description
-force	**-f** .	Force the action (useful for scripting).

Example

```
login as: admin
admin@192.20.9.22's password:
Last login: Mon Nov  4 15:20:14 2013 from 192.20.10.109
Luna SA 5.4.0-1 Command Line Shell - Copyright (c) 2001-2013 SafeNet, Inc. All rights reserved.

* * * * W A R N I N G ! * * * *
Your use of this resource is monitored and
recorded for security and for quality-control
purposes.
Have a nice day.
* * * * * * * * * * * * * * * *

[myluna] lunash:>
[myluna] lunash:>sysconf banner clear

WARNING !!  This command will clear the extended banner text.
If you are sure that you wish to proceed, then enter 'proceed', otherwise this command will
abort.

> proceed
Proceeding...

Command Result : 0 (Success)

[myluna] lunash:>



login as: operator
operator@192.20.9.22's password:
Last login: Mon Nov  4 15:18:15 2013 from 192.20.10.109
Luna SA 5.4.0-1 Command Line Shell - Copyright (c) 2001-2013 SafeNet, Inc. All rights reserved.


[myluna] lunash:>
```

sysconf config

Access the system configuration commands. This command manages the various configuration files that are created and modified when you set up various system elements such as NTLS, SSH, NTP, SNMP, etc.

Syntax

sysconf config

backup
clear
delete
export
factoryreset
import
list
restore
show

Parameter	Shortcut	Description
backup	**b**	Backs up configuration data. See "sysconf config backup" on page 359.
clear	**c**	Deletes all the configuration backup files except the initial factory configuration file. See "sysconf config clear" on page 360.
delete	**d**	Deletes a configuration backup file. See "sysconf config delete" on page 361.
export	**e**	Exports a configuration backup file. See "sysconf config export" on page 362.
factoryreset	**f**	Factory reset. See "sysconf config factoryreset" on page 364.
import	**i**	Imports a configuration backup file. See "sysconf config import" on page 363.
list	**l**	List configuration backup files. See "sysconf config list" on page 366.
restore	**r**	Restores configuration backup. See "sysconf config restore" on page 367.
show	**s**	Show the current configuration. See "sysconf config show" on page 368.

sysconf config backup

Backs up configuration data. This command creates a backup of the configuration of the following modules and services:

- user accounts and files
- network settings
- syslog settings
- NTP settings
- SNMP settings
- SSH settings
- NTLS settings
- keys and certificates.

It does not include the HSM and partition configurations. You can save the backup file to the internal HSM, or an external backup token using the **sysconf config export** command.

Syntax

sysconf config backup -description <comment>

Parameter	Shortcut	Description
-description	**-d**	Comment describing this backup. The description must enclosed in double quotes if it contains spaces.

Example

```
lunash:>sysconf config backup -description mybackup2
Created configuration backup file: smyluna_Config_20120221_1725.tar.gz.

Command Result : 0 (Success)
```

sysconf config clear

Delete all the configuration backup files in the file system, in the internal HSM, or in an external backup token. This command does not delete the initial factory configuration file in the file system.

If the -deviceType parameter is not specified, the files in the file system are deleted.

-serialNumber is required if -deviceType is "token" and optional if -deviceType is "hsm".

-serialNumber is not required and is ignored if -deviceType is not specified.

SO login is required before running this command if -deviceType is "hsm" or "token".

Syntax

sysconf config clear [**-force**]

Parameter	Shortcut	Description
-deviceatypescription	**-d**<devicetype>	Comment describing this backup
-force	**-f**	Force the action without prompting.
-serialNumber	**- s** <serialnum>	Token Serial Number

Example

```
lunash:>sysconf config clear

WARNING !!  This command deletes all the configuration backup files except the initial factory
configuration file.

If you are sure that you wish to proceed, then type 'proceed', otherwise type 'quit'.
> proceed

Proceeding...

Command Result : 0 (Success)
```

sysconf config delete

Delete a configuration backup file.

Syntax

sysconf config delete -file <filename> [**-deviceType** <devicetype>] [**-serialnumber** <serialnum>] [**-force**]

Parameter	Shortcut	Description
-devicetype	**-d** <devicetype>	Device Type (hsm, token)
-file	**-fi** <filename>	File Name to delete
-force	**-fo**	Force Action (no prompting for confirmation)
-serialnumber	**-s** <serialnum>	Token Serial Number

Example

```
lunash:>sysconf config delete -file myluna_Config20101021_2015.tar.gz

WARNING !!  This command deletes the configuration backup file: myluna_Config_20101021_
2015.tar.gz.

If you are sure that you wish to proceed, then type 'proceed', otherwise type 'quit'.
> proceed

Proceeding...

Command Result : 0 (Success)
```

sysconf config export

Exports a configuration backup file from the file system to the internal HSM, or to an external backup token. This command overwrites the existing configuration file with the same name.

-serialNumber is required if -deviceType is "token" and optional if -deviceType is "hsm".

SO login is required before running this command if -deviceType is "hsm" or "token".

Syntax

sysconf config export -file <filename> [**-devicetype** <devicetype>] [**-serialnumber** <serialnum>] [**-force**]

DESCRIPTION

Parameter	Shortcut	Description
-devicetype	**-d** <devicetype>	Device Type (hsm, token)
-file	**-fi** <filename>	File Name to delete
-force	**-fo**	Force Action (no prompting for confirmation)
-serialnumber	**-s** <serialnum>	Token Serial Number

Example

```
[myluna] lunash:>sysconf config export -file myluna_Config20101021_2015.tar.gz
-devicetype hsm
WARNING !!  This command exports the configuration backup file: factoryInit_local_host_Con-
fig.tar.gz to the hsm.
It will overwrite the existing configuration file with the same name on the hsm.
If you are sure that you wish to proceed, then type 'proceed', otherwise type 'quit'..
> proceed

Proceeding...

Command Result : 0 (Success)
```

sysconf config import

Import a configuration backup file from the internal HSM or from an external backup HSM and saves it as a file. This command overwrites the existing configuration file with the same name.

This command does NOT restore the configuration from the imported file. You can use the "sysconf config restore" command after running this command to restore the configurations.

-serialNumber is required if -deviceType is "token" and optional if -deviceType is "hsm".

SO login is required before running this command if -deviceType is "hsm" or "token".

Syntax

sysconf config import -file <filename> [**-devicetype** <devicetype>] [**-serialnumber** <serialnum>] [**-force**]

Parameter	Shortcut	Description
-devicetype	**-d** <devicetype>	Device Type (hsm, token)
-file	**-fi** <filename>	File Name to delete
-force	**-fo**	Force the action without prompting.
-serialnumber	**-s** <serialnum>	Token Serial Number

Example

```
lunash:>sysconf config import -file myluna_Config20101021_2015.tar.gz
-devicetype hsm
WARNING !!  This command imports the configuration backup file: factoryInit_local_host_Con-
fig.tar.gz from the hsm.

It will overwrite the existing configuration file with the same name.

If you are sure that you wish to proceed, then type 'proceed', otherwise type 'quit'.
> proceed

Proceeding...

Command Result : 0 (Success)
```

sysconf config factoryreset

Reset the appliance to the settings created at the factory. This is the same action as running the "sysconf config restore" command on the 'factoryInit_local_host..." file. You can specify any individual service's configuration, or just reset all of them to the initial factory settings with the '-all' option. This reset is for the configurations of the indicated services and does not affect the HSM.

This command affects appliance settings external to the HSM. To reset the HSM, use **hsm factoryReset** (which can be run from a local serial console only).

Note: To reset the configuration for the NTLS service, you must first stop this service (**service stop ntls**).

Syntax

sysconf config factoryReset -service <service> [**-force**]

Parameter	Shortcut	Description
-force	**-fo**	Force the action without prompting.
-service	**-s**	Specifies the service name. **Valid values:** network,ssh,NTLS,syslog,ntp,snmp,users,system,all

Example

```
lunash:>sysconf config factoryReset -service all
This command restores the initial factory configuration of service: all.
The HSM and Partition configurations are NOT included.

This command restores the previous configurations from the backup file:
factoryInit_local_host_Config.tar.gz

WARNING !!  This command restores the configuration backup file:
factoryInit_local_host_Config.tar.gz.

It first creates a backup of the current configuration before restoring:
factoryInit_local_host_Config.tar.gz.

If you are sure that you wish to proceed, then type 'proceed', otherwise type 'quit'.
> proceed
Proceeding...

This command creates a backup of the configuration of the following modules
and services: users' accounts and files, network, syslog, NTP, SNMP, SSH
and NTLS settings, keys and certificates. It does not include the HSM and
Partition configurations.

Created configuration backup file: myluna_Config_20101021_1112.tar.gz
You can save it to the HSM or an external backup token using the
"sysconf config export" command.
```

```
Restore the ntls configuration: Failed: file not found.
Restore the network configuration: Succeeded.
Restore the syslog configuration: Succeeded.
Restore the ntp configuration: Succeeded.
Restore the snmp configuration: Succeeded.
Restore the ssh configuration: Succeeded.
Restore the users configuration: Failed: file not found.
Restore the system configuration: Failed: file not found.
You must either reboot the appliance or restart the service(s) for the changes to take effect.
Please check the new configurations BEFORE rebooting or restarting the services.
You can restore the previous configurations if the new settings are not acceptable.
Command Result : 0 (Success)
```

Note: The items that failed above simply failed to reset because they were already at factory default settings and had never been configured, so that no file of configuration settings for the particular service was ever created, and there was nothing for the "sysconf config factoryReset" command to do in those cases.

sysconf config list

Show the list of configuration backup files.

Syntax

sysconf config list

Example

lunash:>sysconf config list

```
Size     Filename                                         Description
30411    myluna_Config_20090930_0934.tar.gz               Automatic Backup Before Restore
30397    myluna2_Config_20090930_0925.tar.gz              MyBackup
18400    factoryInit_local_host_Config_20011231_1901.tar.gz    Initial Factory Settings
25179    myluna2_Config_20100907_2122.tar.gz              Joe Backup 1
```

sysconf config restore

Restore configuration of the selected services from a backup file. The service(s) must be stopped before restoring their configuration. This command does not restore the HSM and Partition configurations.

You must reboot the appliance for the changes to take effect.

Please check the new configurations BEFORE rebooting or restarting the services.

It automatically creates a backup file of the current configurations before restoring a previous configuration. You can restore the previous configurations if the new settings are not acceptable.

Syntax

sysconf config restore -file <filename> **-service** <service> [**-force**]

Parameter	Shortcut	Description
-file	**-fi**	File name
-force	**-fo**	Force the action without prompting.
-service	**-s**	The service name. **Valid values:** network,ssh,NTLS,syslog,ntp,snmp,users,system,all

Example

```
[myluna] lunash:>sysconf config restore -file SA76_test_Config_20111104_1018.tar.gz -service
users
WARNING !!  This command restores the configuration backup file: SA76_test_Config_20111104_
1018.tar.gz.
It first creates a backup of the current configuration before restoring: SA76_test_Config_
20111104_1018.tar.gz.
If you are sure that you wish to proceed, then type 'proceed', otherwise type 'quit'.
> proceed
Proceeding...
Created configuration backup file: SA76_test_Config_20111104_1020.tar.gz
Restore the users configuration: Succeeded.
You must either reboot the appliance or restart the service(s) for the changes to take effect.
Please check the new configurations BEFORE rebooting or restarting the services.
You can restore the previous configurations if the new settings are not acceptable.
Command Result : 0 (Success)
```

sysconf config show

Shows the system information of a configuration backup file.

Syntax

sysconf config show -file <filename>

Show system config file information

Parameter	Shortcut	Description
-file	**-fi**	File name

Example

```
lunash:>sysconf config show -file myluna_Config_20090930_0925.tar.gz

System information when this backup was created:

hostname: myluna
eth0 IP Address: 172.20.11.21
eth1 IP Address: 192.168.254.1
Software Version: Luna SA 5.1.0-25 [Build Time: 20120224 16:07]
HSM Firmware Version: 6.0.8
HSM Serial Number: 696910
uptime:  09:25:07 up 3 days,  9:50,  2 users,  load average: 0.09, 0.12, 0.09
Current time: Fri Feb 24 09:25:07 IST 2012
Description: MyBackup

Command Result : 0 (Success)
```

sysconf drift

Access the sysconf drift commands to view and configure drift.

Syntax

sysconf drift

init
reset
set
startmeasure
status
stopmeasure

Parameter	Shortcut	Description
init	**i**	Activate automatic drift adjustments. See "sysconf drift init" on page 370.
reset	**r**	Reset all drift tracking data. See "sysconf drift reset" on page 371.
set	**se**	Manually set internal drift data. See "sysconf drift set" on page 372.
startmeasure	**star**	Set the time and start measuring. See "sysconf drift startmeasure" on page 373.
status	**stat**	Display the current drift data. See "sysconf drift status" on page 374.
stopmeasure	**sto**	Stop measuring and record the drift. See "sysconf drift stopmeasure" on page 375.

sysconf drift init

Sets the time, and activates the automatic periodic drift adjustments. This is done after you have completed a period of drift measurement with the **sysconf drift startmeasure** and **sysconf drift stopmeasure** commands, with at least an uninterrupted three day measurement period between the start and stop, to calculate the baseline of drift.

Syntax

sysconf drift init -currentprecisetime <currentprecisetime>

Parameter	Shortcut	Description
-currentprecisetime	**-c**	Current best precise time in hh:mm:ss format.

Example

```
lunash:>sysconf drift init -c 18:29:01

Measuring drift correction data on this appliance.

Setting the time to 18:29:01 and initializing drift correction of 5 seconds per day on this
   appliance.  The time will be adjusted daily to compensate for this drift.

Use the command 'sysconf drift reset' to disable drift correction.

Date and time set to:  Thu April  7 18:29:01 EDT 2011

Command Result : 0 (Success)
```

The following is the response if you did not run **sysconf drift startmeasure** and allow measurement for sufficient time before initializing drift correction.

```
lunash:>sysconf drift init -currentprecisetime 13:51:01

Measuring drift correction data on this appliance.


Error: unable to initialize drift correction.  The internal data containing
   drift values can not be found.

Ensure that the proper data acquisition steps were followed.

Command Result : 0 (Success)
```

sysconf drift reset

Reset drift and internal drift tracking data.

Syntax

sysconf drift reset [**-force**]

Parameter	Shortcut	Description
-force	**-f**	Force the action without prompting

Example

```
lunash:>sysconf drift reset

If you are sure that you wish to clear all data relating to drift
correction, then type 'proceed', otherwise type 'quit'
> proceed

Proceeding...

Command Result : 0 (Success)
```

sysconf drift set

Manually set the internal drift measurement data.

Syntax

sysconf drift set

Example

```
lunash:>sysconf drift set

Enter the value to be used for drift (in seconds per day): 3

This value will overwrite the previous value of the drift that may have
been measured.  If you are sure that you wish to overwrite it, then type
'proceed', otherwise type 'quit'
> proceed

Proceeding...

NOTE: The new value will not take effect until 'sysconf drift init' is run.
Command Result : 0 (Success)
```

sysconf drift startmeasure

Sets the time, and starts measuring drift.

Syntax

sysconf drift startmeasure -currentprecisetime <currentprecisetime>

Parameter	Shortcut	Description
-currentprecisetime	**-c**	Current best precise time in hh:mm:ss format.

Example

```
[myLuna] lunash:>sysconf drift startmeasure -c 13:53:01

Setting the time to 13:53:01 and recording data for drift correction mechanism.
Current date and time set to:  Tue April  5 13:53:01 EDT 2011

Command Result : 0 (Success)
```

sysconf drift status

Display the status of the current drift data.

Syntax

sysconf drift status

Example

```
lunash:>sysconf drift status
   Drift measurement started on:  Fri Apr  8 14:47:00 EDT 2011
   Measurement has yet to be stopped.
   Current drift correction is:   4 seconds per day
   (Note that drift correction may be manually set.)

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

The following is the result if **sysconf drift startmeasure** was not run before this command.

```
lunash:>sysconf drift status

Internal configuration data indicates that drift measurement was never started.
No drift correction is in effect.

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

sysconf drift stopmeasure

Stops measuring and records the drift.

Syntax

sysconf drift stopmeasure -currentprecisetime <currentprecisetime>

Parameter	Shortcut	Description
-currentprecisetime	**-c**	Current best precise time in hh:mm:ss format.

Example

```
lunash:>sysconf drift drift stopmeasure -currentprecisetime 18:40:37

   Measuring drift correction data on this appliance.
   Storing measured drift of 12 seconds/day in internal configuration files.
   Use the command 'sysconf drift init' to initialize drift correction.

Command Result : 0 (Success)
```

sysconf fingerprint

This command displays the system's certificate fingerprints for use when ensuring that ssh connections are being made to the correct host, or that the correct server certificate was brought to a client.

Specify if you wish to see the ssh certificate fingerprint or the NTLS certificate fingerprint. The NTLS certificate is created using the sha256WithRSAEncryption algorithm.

Syntax

sysconf fingerprint {**ssh** | **ntls**}

Parameter	Shortcut	Description
ssh	**s**	Display the fingerprint of the SSH certificate. (Compare this with the value presented by the SSH client upon first SSH to the Luna appliance admin interface.) See "sysconf fingerprint ssh" on page 378.
ntls	**n**	Display the fingerprint of the NTLS certificate. (On the client side, you can compare this with the value returned from vtl fingerprint -f server.pem) See "sysconf fingerprint ntls" on page 377.

sysconf fingerprint ntls

This command displays the system's certificate fingerprints for use when ensuring that the correct server certificate was brought to a client.

Syntax

sysconf fingerprint ntls

Parameter	Shortcut	Description
ntls	**n**	Display the fingerprint of the NTLS certificate. (On the client side, you can compare this with the value returned from vtl fingerprint -f server.pem)

Example

```
[mylunasa6] lunash:>sysconf fingerprint ntls

NTLS server certificate fingerprint: DC:0E:23:36:7E:E4:76:39:09:85:13:4C:76:FE:87:EC:86:DD:89:3D

Command Result : 0 (Success)
```

sysconf fingerprint ssh

This command displays the system's certificate fingerprint for use when ensuring that ssh connections are being made to the correct host.

Syntax

sysconf fingerprint ssh

Parameter	Shortcut	Description
ssh	**s**	Display the fingerprint of the SSH certificate. (Compare this with the value presented by the SSH client upon first SSH to the Luna appliance admin interface.)

Example

```
[mylunasa6] lunash:>sysconf fingerprint ssh

SSH Server Public Keys

Type   Bits Fingerprint
-----------------------------------------------------------
RSA    2048 26:29:d8:bf:23:cd:22:82:28:38:1c:01:d3:12:5c:d2
DSA    1024 d7:67:26:db:f3:f8:46:2c:5b:db:dd:6a:7c:c0:5a:29
ECDSA   256 13:9b:0c:01:22:5c:86:b5:99:66:b6:6f:10:49:58:4d

Command Result : 0 (Success)
```

sysconf forcesologin

Access commands that allow you to enable or disable SO login enforcement, or display the current SO login enforcement setting.

When SO login enforcement is enabled, access to some lunash commands is restricted to the HSM SO. See "sysconf forcesologin enable" on page 382 for a list of the affected commands.

Syntax

sysconf forcesologin

disable
enable
show

Parameter	Shortcut	Description
disable	d	Disable SO login enforcement. See "sysconf forcesologin disable" on page 381 (*).
enable	e	Enable SO login enforcement. See "sysconf forcesologin enable" on page 382 (**).
show	s	Display the current SO login enforcement setting. See "sysconf forcesologin show" on page 384.

(* On successful `hsm factoryReset` or `sysconf config factoryReset` (option "all") the Luna SA HSM Administrator Login Enforcement feature is reset to "disabled".)

(** If the HSM is not initialized, then the Luna SA HSM SO Login Enforcement feature cannot be enabled or disabled.)

Most Luna SA lunash commands, except time- and partition-specific ones do not require HSM Security Officer (also known as HSM Administrator) to be logged in. The Luna SA HSM SO Login Enforcement option functions as follows:

- Only the SO can enable Luna SA HSM SO Login Enforcement.
- When enabled, the feature verifies that HSM SO is logged in before authorizing the operations described below.
- Only HSM Administrator can disable Luna SA HSM SO Login Enforcement.

Affected commands

The affected commands include all commands that can have an effect on the HSM, its partitions, or application access to the partitions. (Items that are solely appliance-level features generally are not affected.)

client

- client assignPartition
- client revokePartition
- client register
- client delete
- client hostip map
- client hostip unmap

ntls

- ntls bind
- ntls activateKeys
- ntls deactivateKeys
- ntls sslOpsAll
- ntls sslOpsRSA
- ntls information reset
- ntls certificate monitor enable
- ntls certificate monitor disable
- ntls certificate monitor trap trigger
- ntls tcp_keepalive set
- ntls timer set
- ntls threads set
- ntls ipcheck enable
- ntls ipcheck disable

htl

- htl clearOtt
- htl generateOtt
- htl set gracePeriod
- htl set ottExpiry
- htl set defaultOttExpiry

sysconf

- sysconf regenCert
- sysconf hwRegenCert
- sysconf secureKeys

sysconf forcesologin disable

Disable SO login enforcement.

Note: You must be logged in as the HSM SO to execute this command.

Note: The HSM must be initialized before you can execute this command. See "hsm init" on page 92 for more information.

Note: The SO login enforcement setting persists backup and restore operations.

Syntax

sysconf forcesologin disable

Example

```
lunash:> sysconf forcesologin disable

Command Result : 0 (Success)

lunash:> sysconf forcesologin show

HSM Administrator Login Enforcement is NOT enabled.

Command Result : 0 (Success)
```

sysconf forcesologin enable

Enable SO login enforcement. You must be logged in as the HSM SO to execute this command.

SO login enforcement is reset to disabled if the HSM is factory reset using the **hsm factoryReset** or **sysconf config factoryReset** commands. The SO login enforcement setting persists backup and restore operations.

> **Note:** The HSM must be initialized before you can execute this command. See "hsm init" on page 92 for more information.

Affected Commands

When SO login enforcement is enabled, the following commands can be executed by the HSM Administrator only:

Client commands

- "client assignpartition" on page 52
- "client delete" on page 53
- "client hostip map" on page 56
- "client hostip unmap" on page 58
- "client register" on page 60
- "client revokepartition" on page 62

NTLS commands

- "ntls activatekeys" on page 211
- "ntls bind" on page 212
- "ntls certificate monitor disable" on page 216
- "ntls certificate monitor enable" on page 217
- "ntls certificate monitor trap trigger" on page 219
- "ntls deactivatekeys" on page 222
- "ntls information reset" on page 224
- "ntls ipcheck disable " on page 227
- "ntls ipcheck enable" on page 228
- "ntls sslopsall " on page 231
- "ntls sslopsrsa" on page 232
- "ntls tcp_keepalive set" on page 234
- "ntls threads set" on page 237
- "ntls timer set" on page 240

HTL commands

- "htl clearott command" on page 166
- "htl generateott" on page 167

- "htl set defaulttottexpiry" on page 169
- "htl set graceperiod" on page 170
- "htl set ottexpiry" on page 171

Sysconf commands

- "sysconf hwregencert" on page 385
- "sysconf regencert" on page 417
- "sysconf securekeys" on page 418

Syntax

sysconf forcesologin enable

Example

```
lunash:> sysconf forcesologin enable

Command Result : 0 (Success)

lunash:> sysconf forcesologin show

HSM Administrator Login Enforcement is enabled.

Command Result : 0 (Success)
```

sysconf forcesologin show

Display the current SO login enforcement setting.

Syntax

sysconf forcesologin show

Example

```
lunash:> sysconf forcesologin show

HSM Administrator Login Enforcement is enabled.

Command Result : 0 (Success)
```

sysconf hwregencert

This command generates or re-generates the Luna appliance server certificate used for the NTLA in hardware.

If you are using a system with DNS, you should not specify an IP address. If you are using a system that does not use DNS, you should specify the IP address of eth0 so that the certificate will be properly generated.

It is very important that the certificates are properly generated or the NTLA will not work.

This command stores the resulting private and public keys in the HSM, and the certificate generated from them on the file system (hard disk) inside the Luna appliance.
If you prefer the additional speed of keys that are stored in the file system, use the command 'sysconf regenCert' instead.

Trade-off

If you use 'sysconf hwRegenCert', the private key exists only on the HSM. Therefore the parts of the NTLS-setup handshake that need the private key take slightly longer to complete. For applications that set up an NTLS link for an extended period and perform multiple crypto operations, the additional overhead is negligible.

For applications that set up the link, perform one operation, tear down the link, then set up another for the next operation, the overhead of storing the private key on the HSM could become noticeable.

Additional Commands Required

To use keys in hardware, the following sequence is necessary:

- at the Luna SA, run **sysconf hwRegenCert**
- run **ntls bind**, as required; this also restarts NTLS
- run **ntls activateKeys**, to ensure that the keys in the special partition remain available
- transfer the new server certificate to clients
- at the client, register the new server certificate

As well, if the Luna appliance is rebooted/restarted for any reason (secure package update, power failure...) with the NTLS keys in the HSM, you must perform **ntls activateKeys** and **service restart ntls**.

This command generates a new key-pair. If you wish to use existing keys, that you have already created in the file system (not yet stored on the HSM), then you can move your existing keys into the HSM with **sysconf secureKeys**

You must be logged in to use this command.

The keys in hardware feature requires a special container "Cryptoki User" to keep the RSA key pair for NTLS. Even though it shows in the partition list, this container is not meant to be managed by customers directly. Once it is created, you should never need to touch this partition at all.

Syntax

sysconf hwRegenCert [<eth0_ip_address>]

Parameter	Shortcut	Description
<eth0_ip_address>		Provide the IP address of eth0 if the rest of your setup was done without DNS.
-days		Specifies the certificate validity period, in days.

Parameter	Shortcut	Description
		Range: 1 to 3653
-force		Force the action without prompting.
-startdate		Specifies the certificate validity start date, in numeric year, month, day format with four-digit year (yyyymmdd).

Example

```
[mylunaSA]lunash:>par create -par "Cryptoki User"


On completion, you will have this number of partitions: 1

-label:  Not provided; using name for label.


          Note: This partition is only to be used for NTLS Keys in Hardware.

          Type 'proceed' to create the initialized partition, or
          'quit' to quit now.
          > proceed
Please ensure that you copy the password from the Luna PED and
that you keep it in a safe place.

Luna PED operation required to create a partition - use User or Partition Owner (black) PED key.

Luna PED operation required to generate cloning domain on the partition - use Domain (red) PED
key.

'partition create' successful.


Command Result : 0 (Success)
[mylunaSA] lunash:>sysconf hwRegenCert


WARNING !!  This command will overwrite the current server certificate and private key.
            All clients will have to add this server again with this new certificate.
If you are sure that you wish to proceed, then type 'proceed', otherwise type 'quit'

> proceed
Proceeding...

NTLS certificate generated. Migrate NTLS private key into HSM hardware..

Enter User Password:

Proceeding to create/migrate keys to "Cryptoki User" with handle 9
Please attend to the PED to activate partition on HSM - use User or Partition Owner (black) PED
key.


Success:  NTLS keys are in hardware.
```

```
'sysconf hwRegenCert' successful. NTLS and/or STC must be (re)started before clients can con-
nect.

Please use the 'ntls show' command to ensure that NTLS is bound to an appropriate network device
or IP

address/hostname for the network device(s) NTLS should be active on. Use 'ntls bind' to change
this binding if

necessary.


Command Result : 0 (Success)
[mylunaSA] lunash:>ntls activateKeys

Enter User Password:
Please attend to the PED to activate partition on HSM - use User or Partition Owner (black) PED
key.
Stopping ntls:OK
Starting ntls:OK
Stopping htl:OK
Starting htl:OK

Command Result : 0 (Success)
[mylunaSA] lunash:>
```

sysconf ntp

Access the commands used to view and set the network time protocol (NTP) configuration.

Syntax

sysconf ntp

> **addserver**
> **autokeyauth**
> **deleteserver**
> **disable**
> **enable**
> **listservers**
> **log**
> **ntpdate**
> **show**
> **status**
> **symmetricauth**

Parameter	Shortcut	Description
addserver	**ad**	Add NTP Server. See "sysconf ntp addserver" on page 389.
autokeyauth	**au**	NTP Autokey Authentication. See "sysconf ntp autokeyauth" on page 390.
deleteserver	**de**	Delete NTP Server. See "sysconf ntp deleteserver " on page 397.
disable	**di**	Disable NTP Service. See "sysconf ntp disable" on page 398.
enable	**e**	Enable NTP Service. See "sysconf ntp enable" on page 399.
listservers	**li**	List Configured NTP Servers. See "sysconf ntp listservers" on page 400.
log	**lo**	NTP Log Command. See "sysconf ntp log tail" on page 402.
ntpdate	**n**	Set date and time using NTP. See "sysconf ntp ntpdate" on page 403.
show	**sh**	Show NTP Configuration. See "sysconf ntp show" on page 404.
status	**st**	Get NTP Service Status. See "sysconf ntp status" on page 405
symmetricauth	**sy**	NTP Symmetric Key Authentication. See "sysconf ntp symmetricauth" on page 406.

sysconf ntp addserver

Add an NTP server.

Syntax

sysconf ntp addserver <hostname_or_ipaddress> [**-autokey**]|[**-key** <keyid>] [**-burst**] [**-iburst**] [**-prefer**] [**-version** <version>]

Parameter	Shortcut	Description
<hostname_or_ipaddress>		Specifies the hostname or IP address of the NTP Server.
-autokey	**au**	Send and receive packets authenticated by the Autokey scheme (not used with key <keyid>).
-burst	**de**	Send multiple packets when the server is reachable.
-iburst	**di**	Send out bursts of 8 packets when the server is unreachable.
-key		Specifies the NTP Authentication Keyid (not used with Autokey) **Range:** 1 to 65535
-prefer	**e**	Set this server as the preferred server.
-version	**li**	Specifies the NTP version **Valid values**: 3 or 4

Example

```
lunash:> sysconf ntp addserver time.nrc.ca
NTP server 'server time.nrc.ca' added.
WARNING !! Server 'time.nrc.ca' added without authentication.
NTP is enabled
Shutting down ntpd:                                [  OK  ]
Starting ntpd:                                     [  OK  ]
Please wait to see the result ......
NTP is running
===========================================================
NTP Associations Status:
ind assid status  conf reach auth condition  last_event cnt
===========================================================
1 56579  8011   yes    no  none    reject    mobilize  1
2 56580  8011   yes    no  none    reject    mobilize  1
===========================================================
Please look at the ntp log to see any potential problem.
Command Result : 0 (Success)
```

sysconf ntp autokeyauth

Access commands that allow you to configure Autokey NTP server authenticaton.

When you add a trusted NTP server, Luna SA and the server negotiate, exchange certificates, and so on. You can optionally choose to use AutoKey to authenticate your connection. Additionally, if using AutoKey, you can optionally choose to use one of the supported identity schemes, IFF (Identify Friend or Foe), GQ (Guillou-Quisguater), or MV (Mu-Varadharajan), or by default none of those schemes, and just exchange private certificates.

Syntax

sysconf ntp autokeyauth

```
    clear
    generate
    install
    list
    update
```

Parameter	Shortcut	Description
clear	**c**	Delete all keys and certificates. See "sysconf ntp autokeyauth clear" on page 391.
generate	**g**	Generate client keys and certificates (required to use AutoKey). See "sysconf ntp autokeyauth generate" on page 392.
install	**i**	Install Autokey Identity Scheme IFF|GQ|MV (optional). See "sysconf ntp autokeyauth install" on page 394.
list	**l**	Show Autokey keys and certificates. "sysconf ntp autokeyauth list" on page 395.
update	**u**	Update client certificates (a certificate usually has a ttl of one year, after which you must update to renew). "sysconf ntp autokeyAuth update" on page 396.

sysconf ntp autokeyauth clear

Delete all Autokey authentication keys and certificates.

Syntax

sysconf ntp autokeyAuth clear [**-force**}

Parameter	Shortcut	Description
-force	**-f**	Force the action without prompting.

Example

```
lunash:>sysconf ntp autokeyAuth clear -force

Force option used. Proceed prompt bypassed.
All key and certificates files were deleted.
You must restart NTP for the changes to take effect.
Check NTP status after restarting it to make sure that the client is able to start and sync with
the server.

Command Result : 0 (Success)
```

sysconf ntp autokeyauth generate

Generate new keys and certificates for NTP public key authentication

Syntax

sysconf ntp autokeyAuth generate [**-certalg** <certalg>] [**-modulus** <modulus>] [**-signalg** <signalg>] [**-password** <ntpkey>]

Parameter	Shortcut	Description
-certalg	**-c**	NTP Certificate Algorithm. **Valid values:** RSA-MD5, RSA-SHA, RSA-SHA1, RSA-RIPEMD160, DSA-SHA, DSA-SHA1 **Default:** RSA-SHA1
-modulus	**-m**	NTP Modulus Size **Range:** 512 to 2048 **Default:** 2048
-password	**-p**	NTP Symmetric Key Value
-signalg	**-s**	NTP Sign Algorithm **Valid values:** RSA, DSA **Default:** RSA

Note: If you set the signing algorithm to DSA (**-signalg sha**), specify DSA-SHA1, not DSA-SHA, for the certificate algorithm (**-certalg dsa-sha1**). Using DSA-SHA will cause a 'invalid digest type' error.

Example

```
lunash:>sysconf ntp autokeyAuth generate

Generate new keys and certificates using ntp-keygen

WARNING ! Generating keys without client Password.
Generating new keys and certificates using these arguments:  -S RSA -c RSA-SHA1  -m 2048

Using OpenSSL version 90802f
Using host sa5 group sa5
Generating RSA keys (2048 bits)...
RSA 0 13 46     1 2 6                           3 1 2

Generating new host file and link
ntpkey_host_sa5->ntpkey_RSAhost_sa5.3538763554
Generating RSA keys (2048 bits)...
RSA 0 0 698     1 2 12                          3 1 4

Generating new sign file and link
ntpkey_sign_sa5->ntpkey_RSAsign_sa5.3538763554
Generating new certificate sa5 RSA-SHA1
```

```
X509v3 Basic Constraints: critical,CA:TRUE
X509v3 Key Usage: digitalSignature,keyCertSign

Generating new cert file and link
ntpkey_cert_sa5->ntpkey_RSA-SHA1cert_sa5.3538763554
You must restart NTP for the changes to take effect.
Check NTP status after restarting it to make sure that the client is able to start and sync with
the server.

Command Result : 0 (Success)
```

sysconf ntp autokeyauth install

Install an Autokey Identity scheme.

Syntax

sysconf ntp autokeyauth install -idscheme <identityscheme> -keyfile <filename>

Parameter	Shortcut	Description
-idscheme	**-i**	Specifies the NTP AutoKey Identity Scheme to install. **Valid values:** IFF, GQ, or MV
-keyfile	**-k**	Specifies the keyfile name.

sysconf ntp autokeyauth list

List the NTP Autokey authentication keys.

Syntax

sysconf ntp autokeyauth list

Example

```
 lunash:>sysconf ntp autokeyauth  list

=========== Installed keys and certificates: ====================
ntpkey_RSA-SHA1cert_sa5.3538763554
ntpkey_RSAsign_sa5.3538763554
ntpkey_cert_sa5 -> ntpkey_RSA-SHA1cert_sa5.3538763554
ntpkey_sign_sa5 -> ntpkey_RSAsign_sa5.3538763554
ntpkey_RSAhost_sa5.3538763554
ntpkey_host_sa5 -> ntpkey_RSAhost_sa5.3538763554
=================== Certificate details: =======================
Certificate File: ntpkey_RSA-SHA1cert_sa5.3538763554
Certificate:
Data:
Version: 3 (0x2)
Serial Number: -756203742 (-0x2d12c0de)
Signature Algorithm: sha1WithRSAEncryption
Issuer: CN=sa5
Validity
Not Before: Feb 20 21:52:34 2012 GMT
Not After : Feb 19 21:52:34 2013 GMT
Subject: CN=sa5
X509v3 extensions:
X509v3 Basic Constraints: critical
CA:TRUE
X509v3 Key Usage:
Digital Signature, Certificate Sign
=================================================================

Command Result : 0 (Success)
```

sysconf ntp autokeyAuth update

Update the client certificates and keys.

Syntax

sysconf ntp autokeyAuth update

Example

```
lunash:>sysconf ntp autokeyAuth update

------- Updating client autokey certificate ----------
client password not configured.
Updating certificates without password.
Using OpenSSL version 90802f
Using host sa5 group sa5
Using host key ntpkey_RSAhost_sa5.3527441331
Using sign key ntpkey_RSAsign_sa5.3527441331
Generating new certificate sa5 RSA-SHA1
X509v3 Basic Constraints: critical,CA:TRUE
X509v3 Key Usage: digitalSignature,keyCertSign
Generating new cert file and link
ntpkey_cert_sa5->ntpkey_RSA-SHA1cert_sa5.3538440207
You must restart NTP for the changes to take effect.
Check NTP status after restarting it to make sure that the client is able to start and sync with
the server.

Command Result : 0 (Success)
```

sysconf ntp deleteserver

Delete an NTP server.

Syntax

sysconf ntp deleteserver <hostname_or_ipaddress>

Parameter	Shortcut	Description
<hostname_or_ipaddress>		Specifies the hostname or IP address of the NTP server to delete.

Example

```
lunash:> sysconf  ntp deleteserver time.nrc.ca

NTP server 'server time.nrc.ca' deleted.
NTP is enabled
Shutting down ntpd:                                 [  OK  ]
Starting ntpd:                                      [  OK  ]
Please wait to see the result ......
NTP is running
===========================================================
NTP Associations Status:
ind assid status  conf reach auth condition  last_event cnt
===========================================================
  1 56579   963a    yes   yes   none  sys.peer sys_peer    3

===========================================================
Please look at the ntp log to see any potential problem.

Command Result : 0 (Success)
```

sysconf ntp disable

Disable and stop the NTP service.

Syntax

sysconf ntp disable

Example

```
lunash:> sysconf ntp disable

NTP is disabled
Shutting down ntpd:  [  OK  ]
NTP is stopped

Command Result : 0 (Success)
```

sysconf ntp enable

Enable and start the NTP service.

Syntax

sysconf ntp enable

Example

```
lunash:> sysconf ntp enable

NTP is enabled
Shutting down ntpd:                                 [  OK  ]
Starting ntpd:                                      [  OK  ]
Please wait to see the result ......
NTP is running
===========================================================
NTP Associations Status:
ind assid status  conf reach auth condition  last_event cnt
===========================================================
  1 18515  8011    yes     no   none     reject     mobilize   1
  2 18516  8011   yes     no   none     reject     mobilize   1
===========================================================
Please look at the ntp log to see any potential problem.

Command Result : 0 (Success)
```

sysconf ntp listservers

List the configured NTP servers.

Syntax

sysconf ntp listservers

Example

```
lunash:> sysconf ntp listservers
=================================================================
NTP Servers:
server 127.127.1.0
server time.nrc.ca
=================================================================
Command Result : 0 (Success)
```

sysconf ntp log

Display the NTP logs.

Syntax

sysconf ntp log

Parameter	Shortcut	Description
tail		Display the log entries at the end of the log. See "sysconf ntp log tail" on page 402.

sysconf ntp log tail

Display the NTP logs.

Syntax

sysconf ntp log tail [**-entries** <logentries>]

Parameter	Shortcut	Description
tail		Display the log entries at the end of the log.
-entries	**-e**	Specifies the number of entries to display. **Range:** 0 to 2147483647

Example

```
lunash:> sysconf  ntp log tail -entries 12

===============================================================================
syslog tail -l ntp -e 12
13 Oct 00:08:54 ntpd[842]: 0.0.0.0 064d 0d kern PPS no signal
13 Oct 00:43:48 ntpd[842]: 0.0.0.0 065d 0d kern PPS no signal
13 Oct 01:28:25 ntpd[842]: 0.0.0.0 066d 0d kern PPS no signal
13 Oct 02:03:54 ntpd[842]: 0.0.0.0 067d 0d kern PPS no signal
13 Oct 02:39:02 ntpd[842]: 0.0.0.0 068d 0d kern PPS no signal
13 Oct 03:14:38 ntpd[842]: 0.0.0.0 069d 0d kern PPS no signal
13 Oct 03:49:00 ntpd[842]: 0.0.0.0 06ad 0d kern PPS no signal
13 Oct 04:41:50 ntpd[842]: 0.0.0.0 06bd 0d kern PPS no signal
13 Oct 05:33:49 ntpd[842]: 0.0.0.0 06cd 0d kern PPS no signal
13 Oct 06:27:09 ntpd[842]: 0.0.0.0 06dd 0d kern PPS no signal
13 Oct 07:02:59 ntpd[842]: 0.0.0.0 06ed 0d kern PPS no signal
13 Oct 07:37:55 ntpd[842]: 0.0.0.0 06fd 0d kern PPS no signal
===============================================================================

Command Result : 0 (Success)
```

sysconf ntp ntpdate

Set the date and time using NTP

Syntax

sysconf ntp ntpdate <hostname_or_ipaddress> [**-key** <keyid>] [**-version** <version>]

Parameter	Shortcut	Description
<hostname_or_ipaddress>		Specifies the hostname or IP address of the NTP server.
-key	**-k**	NTP Authentication Keyid **Range:** 1 to 65535
-version	**-v**	Specifies the NTP version **Valid values:** 3 or 4

Example

```
[myluna] lunash:> sysconf  ntp ntpdate 127.127.1.0
This command sets the date and time using ntp server "127.127.1.0" if NTP daemon is not running.
NTP daemon is running. You can stop ntpd using the "service stop ntp" command before running
this command.
Command Result : 0 (Success)
[myLuna] lunash:>

[myLuna] lunash:>service stop ntp
Shutting down ntp:                                                              [  OK  ]
Command Result : 0 (Success)
[myluna] lunash:>

[myluna] lunash:> sysconf  ntp ntpdate 127.127.1.0
This command sets the date and time using ntp server "127.127.1.0" if NTP daemon is not running.
Current time before running ntpdate: Wed Oct 12 20:47:17 PDT 2011
Current time after running ntpdate: Wed Oct 12 20:47:33 PDT 2011
Command Result : 0 (Success)
[myLuna] lunash:>
[myLuna] lunash:>service start ntp
Starting ntp:                                                                    [  OK  ]
Command Result : 0 (Success)
```

sysconf ntp show

Display the NTP configuration.

Syntax

sysconf ntp show

Example

```
lunash:> sysconf ntp show

---------------- NTP Version ----------------------------------------
ntpq 4.2.6p2@1.2194-o Fri Oct  8 19:30:08 UTC 2010 (1)
==================== NTP Configuration ===============================
restrict default kod nomodify notrap nopeer noquery
restrict -6 default kod nomodify notrap nopeer noquery
restrict 127.0.0.1
restrict -6 ::1
fudge 127.127.1.0 stratum 10
--------------------- NTP Servers -------------------------------------
server 127.127.1.0
server time.nrc.ca
=======================================================================

Command Result : 0 (Success)
```

sysconf ntp status

Display the NTP service status.

A “+” in front of an NTP server name means that it’s a good candidate for synchronization. More than one NTP server could be a good candidate.

A “*” in front of an NTP server name means that the it’s the source of synchronization and the client has been synchronized to it. Only one NTP server at a time will be chosen as the source of synchronization.

Syntax

sysconf ntp status

Example

```
lunash:> sysconf ntp status

NTP is running
NTP is enabled
Peers:
==============================================================================
remote           refid         st t when poll reach   delay   offset  jitter
==============================================================================
*LOCAL(0)        .LOCL.          10 l   15     64       7        0.000     0.000   0.000
==============================================================================
Associations:
==============================================================================
ind assid status  conf reach auth condition  last_event cnt
===========================================================
 1  12393   963a   yes     yes   none   sys.peer     sys_peer    3
==============================================================================
NTP Time:
==============================================================================
ntp_gettime() returns code 0 (OK)
time d2407aa3.4e858000  Wed, Oct 12 2011 13:44:19.306, (.306725),
maximum error 8020716 us, estimated error 0 us
ntp_adjtime() returns code 0 (OK)
modes 0x0 (),
offset 0.000 us, frequency 0.000 ppm, interval 1 s,
maximum error 8020716 us, estimated error 0 us,
status 0x1 (PLL),
time constant 2, precision 1.000 us, tolerance 512 ppm,
==============================================================================

Command Result : 0 (Success)
```

sysconf ntp symmetricauth

Access commands that allow you to manage NTP symmetric keys.

Syntax

sysconf ntp symmetricauth

key
trustedkeys

Parameter	Shortcut	Description
key	**k**	Manage symmetric keys. See "sysconf ntp symmetricauth key" on page 407.
trustedkeys	**t**	Manage trusted symmetric keys. See "sysconf ntp symmetricauth trustedkeys" on page 412.

sysconf ntp symmetricauth key

Access commands that allow you to manage the NTP symmetric authentication keys.

Syntax

sysconf ntp symmetricauth key

add
clear
delete
list

Parameter	Shortcut	Description
add	**a**	Add a symmetric authentication key. See "sysconf ntp symmetricauth key add" on page 408.
clear	**c**	Delete all NTP symmetric authentication keys. See "sysconf ntp symmetricauth key clear" on page 409.
delete	**d**	Delete an NTP symmetric authentication key. See "sysconf ntp symmetricauth key delete" on page 410.
list	**l**	List all of the currently configured NTP symmetric keys. See "sysconf ntp symmetricauth key list" on page 411.

sysconf ntp symmetricauth key add

Add an NTP symmetric authentication key.

Syntax

sysconf ntp symmetricauth trustedkeys add -id <keyid> **-type** <keytype> **-value** <ntpkey>

Parameter	Shortcut	Description
-id	**-i**	Specifies the key ID. **Range:** 1 to 65535
-type	**-t**	Specifies the key type.
-value	**-v**	Specifies the key value.

sysconf ntp symmetricauth key clear

Delete all symmetric Authentication Keys.

Syntax

sysconf ntp symmetricAuth key clear [**-force**]

Parameter	Shortcut	Description
-force	**-f**	Force the action without prompting.

Example

```
[ott1-myluna1] lunash:>sysconf ntp symmetricauth trustedkeys clear

some-id deleted

some-other-id deleted

Command Result : 0 (Success)
```

sysconf ntp symmetricauth key delete

Delete a single-named authentication key from the appliance's list.

Syntax

sysconf ntp symmetricauth key delete -id <keyid> **-force**

Parameter	Shortcut	Description
-force	**-f**	Force the action without prompting.
-id	**-i**	Specifies the ID of the NTP authentication key to delete.

Example

```
lunash:>sysconf ntp symmetricauth key delete someid

someid deleted

Command Result : 0 (Success)
```

sysconf ntp symmetricauth key list

List the NTP symmetric authentication keys.

Syntax

sysconf ntp symmetricauth key list

Example

```
 lunash:>sysconf ntp symmetricauth key list

NTP Symmetric Authentication Keys:
=================================

keyId keyType KeyValue
=================================
2 M *****
=================================

Command Result : 0 (Success)
```

sysconf ntp symmetricauth trustedkeys

Access commands that allow you to manage symmetric NTP authentication trusted keys.

Syntax

sysconf ntp symmetricauth trustedkeys

add
clear
delete
list

Parameter	Shortcut	Description
add	**a**	Add a symmetric NTP authentication trusted key. See "sysconf ntp symmetricauth trustedkeys add" on page 413.
clear	**c**	Delete all symmetric NTP authentication trusted keys. See "sysconf ntp symmetricauth trustedkeys clear" on page 414.
delete	**d**	Delete an symmetric NTP authentication trusted key. See "sysconf ntp symmetricauth trustedkeys delete" on page 415.
list	**l**	List all of the currently configured symmetric trusted NTP keys. See "sysconf ntp symmetricauth trustedkeys list" on page 416.

sysconf ntp symmetricauth trustedkeys add

Add a trusted authentication key. The key should have already been added using the **sysconf ntp symmetricAuth key add** command.

Syntax

sysconf ntp symmetricauth trustedkeys add <keyid>

Parameter	Shortcut	Description
<keyid>		Specifies the ID of the key to add. **Range:** 1 to 65535

sysconf ntp symmetricauth trustedkeys clear

Delete all Trusted Authentication Keys.

Syntax

sysconf ntp symmetricauth trustedkeys clear [**-force**]

Parameter	Shortcut	Description
-force	**-f**	Force the action without prompting.

Example

```
lunash:>sysconf ntp symmetricauth trustedkeys clear

WARNING !!  This command deletes all NTP symmetric trusted keys.
If you are sure that you wish to proceed, then type 'proceed', otherwise type 'quit'.

> proceed
Proceeding...

Command Result : 0 (Success)
```

sysconf ntp symmetricauth trustedkeys delete

Delete a single named trusted authentication key from the appliance's list of trusted NTP servers.

Syntax

sysconf ntp symmetricauth trustedkeys delete <keyid> [**-force**]

Parameter	Shortcut	Description
<keyid>		Specifies the ID of the key you want to delete. **Range:** 1-65535
-force	**-f**	Force the action without prompting.

Example

```
lunash:>sysconf ntp symmetricauth trustedkeys delete someid

someid deleted

Command Result : 0 (Success)
```

sysconf ntp symmetricauth trustedkeys list

Lists the trusted authentication keys in the appliance's list of trusted NTP servers.

Syntax

sysconf ntp symmetricauth trustedkeys list

Example

```
lunash:>sysconf ntp symmetricauth trustedkeys list

current trustedkeys:

Command Result : 0 (Success)
```

sysconf regencert

Generate server certificate in software. This command generates or re-generates the Luna appliance server certificate used for the NTLA in the Luna appliance file system.

If you are using a system with DNS, you should not specify an IP address. If you are using a system that does not use DNS, you should specify the IP address of eth0 so that the certificate will be properly generated.

It is very important that the certificates are properly generated or the NTLA will not work.

This command stores the resulting private and public keys, and the certificate generated from them, on the file system (hard disk) inside the Luna appliance.
If you prefer the additional security of keys that are stored inside the HSM, use the command **sysconf hwregencert** instead.

Syntax

sysconf regenCert <eth0_ipaddress> [**-startdate** <startdate>] [**-days** <days>] [**-force**]

Parameter	Shortcut	Description
<eth0_ ipaddress>		Specifies the IP address of eth0. This parameter is required if the rest of your setup was done without DNS.
-days	**-d**	Specifies the number of days for which the new certificate will remain valid, starting on <startdate> **Default:** 10 years
-force	**-f**	Force the action without prompting.
-startdate	**-s**	Specifies the starting date upon which the certificate becomes valid - default is 24 hours ago, to obviate possible timezone mismatch issues if you need the certificate to be valid immediately anywhere in the world.

Example

```
lunash:> sysconf regenCert 192.168.1.254

WARNING !!  This command will overwrite the current server certificate and private key.
All clients will have to add this server again with this new certificate.
If you are sure that you wish to proceed, then type 'proceed', otherwise type 'quit'
> proceed
Proceeding...
'sysconf regenCert' successful. NTLS must be (re)started before clients can connect.
Please use the 'ntls show' command to ensure that NTLS is bound to an appropriate network device
or IP address/hostname
for the network device(s) NTLS should be active on. Use 'ntls bind' to change this binding if
necessary.

Command Result : 0 (Success)
```

sysconf securekeys

Move RSA keys to hardware. This command migrates the Luna keys used to secure the NTLS link from the Luna appliance's file system into the HSM.

If you use **sysconf regenCert**, the generated private key, public key and certificate reside, by default, in the Luna appliance's file system.

This command (**sysconf secureKeys**) moves your existing RSA keys into the HSM.

You must be logged in to use this command.

Once the keys reside in the HSM, any operation that needs the private key will require HSM access. For this reason, whenever the system is rebooted (maintenance, power outage, etc.) you must run **ntls activateKeys** to activate (authenticate to) the partition containing those keys.

If your application sets up an NTLS link and then runs multiple crypto operations over that link, you are unlikely to notice an operational difference. If your application sets up and tears down the link for each crypto operation, then the slight additional overhead might become apparent.

Syntax

sysconf securekeys [**-force**]

Parameter	Shortcut	Description
-force	**-f**	Force the action without prompting.

Example

```
lunash:> sysconf secureKeys
WARNING !!  This command migrates the SSL RSA keys to the internal hardware module.
If you are sure that you wish to proceed, then type 'proceed', otherwise type 'quit'
> proceed

Proceeding...

Enter User Password:
Proceeding to migrate keys to "Cryptoki User" with handle 13
Success: NTLS keys are in hardware.
Command Result : 0 (Success)
[myLuna] lunash:>ntls activateKeys
Enter User Password:
Stopping ntls:OK
Starting ntls:OK:

Command Result : 0 (Success)
```

sysconf snmp

Access commands that allow you to configure the Simple Network Management Protocol (SNMP) settings for Luna appliance, and enable or disable the service. At least one user must be configured before the SNMP agent can be accessed.

Syntax

sysconf snmp

disable
enable
notification
show
trap
user

Parameter	Shortcut	Description
disable	**d**	Disable the SNMP service. See "sysconf snmp disable" on page 420.
enable	**e**	Enable the SNMP service. See "sysconf snmp enable" on page 421.
notification	**n**	Access commands that allow you to view or configure the notifications that can be sent by the SNMP agent. See "sysconf snmp notification" on page 422.
show	**s**	Display SNMP service information. See "sysconf snmp show" on page 427.
trap	**t**	Access commands that allow you to view or configure the SNMP trap hosts. See "sysconf snmp trap" on page 428.
user	**u**	Access commands that allow you to view or configure the users that can access the SNMP agent. See "sysconf snmp user" on page 436.

sysconf snmp disable

Disable and stop the SNMP service.

Syntax

sysconf snmp disable

Example

```
lunash:>sysconf snmp disable
SNMP is disabled
Stopping snmpd:       [  OK  ]
SNMP is stopped
Command Result : 0 (Success)
```

sysconf snmp enable

Enable and start the SNMP service.

Syntax

sysconf snmp enable

Example

```
lunash:>sysconf snmp enable
SNMP is enabled
Starting snmpd:          [  OK  ]
SNMP is started
Command Result : 0 (Success)
```

sysconf snmp notification

Access command that allow you to view and configure the notifications that can be sent by the SNMP agent. At least one user must be configured before the SNMP agent can be accessed.

Syntax

sysconf snmp notification

add
clear
delete
list

Parameter	Shortcut	Description
add	**a**	Add a notification target . See "sysconf snmp notification add" on page 423.
clear	**c**	Delete all notification targets. See "sysconf snmp notification clear" on page 424.
delete	**d**	Delete a notification target. See "sysconf snmp notification delete" on page 425.
list	**l**	Display a list of the notification targets. See "sysconf snmp notification list" on page 426.

sysconf snmp notification add

Add a single notification destination to be notified via the SNMP service.

Syntax

sysconf snmp notification add -ipaddress <ipaddress> **-authpassword** <password> [**-authprotocol** <protocol>] [**-notifytype** {**trap** | **inform**}] **-privpassword** <password> **-secname** <userid> [**-udpport** <port>]

Parameter	Shortcut	Description
-authpassword	**-authpa**	Specifies the authentication password. The password may be 8-to-128 characters long.
-authprotocol	**-authpr**	Specifies the authentication protocol. **Valid values:** SHA **Default:** SHA
-ipaddress	**-i**	Specifies the IPv4 address of the destination (a machine running snmptrapd from Net-SNMP or some other SNMP management application, such as MG-Soft's MIB Browser or HP's Openview.)
-notifytype	**-n**	Specifies the notification type. **Valid values:** **trap:** one-way unconfirmed notification **inform:** confirmed notification with retries **Default:** trap
-privpassword	**-p**	Specifies the privacy password or encryption password. The password may be 8-to-128 characters long.
-secname	**-s**	Specifies the security name or user name for this user. The user name may be 1-to-31 characters. In the context of notifications this is the "Security Name" on whose behalf notifications are sent.
-udpport	**-u**	Specifies the UDP port on the notification target host to which notifications are sent. 162 is the SNMP default port for notifications. **Default:** 162

sysconf snmp notification clear

Deletes all users that are currently configured to use the SNMP command with this Luna appliance. If you do not use the -force option, a prompt requires you to type "proceed" if the operation is to go ahead - otherwise, it is aborted.

This command is most useful if you have a number of SNMPv3 notification targets defined and wish to delete all targets. This command is also useful for Luna Shell scripts that need to ensure that all SNMPv3 notification targets have been deleted and that there is thus a clean and empty SNMP notification target configuration.

Syntax

sysconf snmp notification clear [**-force**]

Parameter	Shortcut	Description
-force	**-f**	Force the action without prompting.

Example

```
lunash:>sysconf snmp notification clear

WARNING !!  This command deletes all notification target information from the SNMP Agent.
If you are sure that you wish to proceed, then type 'proceed', otherwise type 'quit'.

> proceed

Command Result : 0 (Success)
```

sysconf snmp notification delete

Delete all notification targets that are configured for IP address <ipaddress> and UDP Port <udpPort>. It is possible that there are 0, 1 or multiple such notification targets configured. (They could be using different values for <notifyType> and/or <secName> although this would not be common.) Note that if <udpPort> is not specified, then only notification targets configured for the default SNMP UDP port 162 will be deleted.

Syntax

sysconf snmp notification delete -ipaddress <ipaddress> [**-udpport** <port>]

Parameter	Shortcut	Description
-ipAddress	**-i**	Specifies the IP address of the notification target to delete.
-udpPort	**-u**	Specifies the UDP port of the notification target to delete. (0-65535) **Default:** 162

Example

```
lunash:>sysconf snmp notification delete -ipAddress 192.20.11.11

SNMP notification target information deleted

Command Result : 0 (Success)
```

sysconf snmp notification list

Lists the targets to which SNMPv3 notifications (traps or informs) will be sent.

Syntax

sysconf snmp notification list

Example

```
lunash:> sysconf snmp notification list

SNMP Notification Targets:
--------------------------
 172.21.100.82:162
 utsp SHA AES
```

In this example the output conveys the following information:

Field	Description
172.21.100.82	The IP address of the notification target host (A machine running snmptrapd from Net-SNMP or some other SNMP management application, such as MG-Soft's MIB Browser or HP's Openview.)
162	The UDP port on the notification target host to which notifications are sent. 162 is the SNMP default port for notifications.
utsp	The "Security Name" (or user name) on whose behalf notifications are sent.
SHA	The authentication protocol used for notifications.
AES	The privacy (or encryption) protocol used for notifications (always AES for Luna SA).

sysconf snmp show

Display SNMP service information.

Syntax

sysconf snmp show

Example

```
lunash:>sysconf snmp show

SNMP is not running
SNMP is disabled

Command Result : 0 (Success)
```

sysconf snmp trap

Access commands that allow you to view or configure SNMP trap hosts.

Syntax

sysconf snmp trap

clear
disable
enable
set
show
test

Parameter	Shortcut	Description
clear	**c**	Clear SNMP trap host information. See "sysconf snmp trap clear" on page 429.
disable	**d**	Disable and stop the Luna SNMP Trap Agent (lsta). See "sysconf snmp trap disable" on page 430.
enable	**e**	Enable and start the Luna SNMP Trap Agent (lsta). See "sysconf snmp trap enable" on page 431.
set	**se**	Set SNMP trap host information. See "sysconf snmp trap set" on page 432.
show	**sh**	Display SNMP trap host information. See "sysconf snmp trap show" on page 433.
test	**t**	Test SNMP trap notification. See "sysconf snmp trap test" on page 434.

sysconf snmp trap clear

Deletes all SNMP Trap Host Information.

Syntax

sysconf snmp trap clear [**-force**]

Parameter	Shortcut	Description
-force	**-f**	Force the action without prompting.

Example

```
lunash:> sysconf snmp trap clear

If you are sure that you wish to clear snmp trap information, then enter 'proceed', otherwise
type 'quit'.

> Proceed

Command Result : 0 (Success)
```

sysconf snmp trap disable

Disable and stop the Luna SNMP Trap Agent (lsta).

Syntax

sysconf snmp trap disable

Example

```
lunash:>sysconf snmp trap disable

SNMP trap agent is disabled
Shutting down lsta:                                        [  OK  ]
SNMP trap agent is stopped

Command Result : 0 (Success)
```

sysconf snmp trap enable

Enable and start the Luna SNMP Trap Agent (lsta).

Syntax

sysconf snmp trap enable

Example

```
lunash:>sysconf snmp trap enable

SNMP trap agent is enabled
Starting lsta:                                              [  OK  ]
SNMP trap agent is started

Command Result : 0 (Success)
```

sysconf snmp trap set

Set SNMP trap host information.

Syntax

sysconf snmp trap set -host <hostname_or_ipaddress> [**-secname** <secname>] [**-engineid** <engineID>] [**-authprotocol** <protocol>] [**-authpwd** <password>] [**-privprotocol** <protocol>] [**-privpwd** <password>]

Parameter	Shortcut	Description
-host	**-h**	Specifies the trap host name or IP address.
-secname	**-s**	Specifies the SNMP v3 security name.
-engineID	**-e**	Specifies the SNMP v3 Engine ID (Hex Number, No 0x or 0X)
-authprotocol	**-authpr**	Specifies the SNMP v3 Authenication Protocol (SHA)
-authpwd	**-authpw**	Specifies the SNMP v3 Authenication password
-privProtocol	**-privpr**	Specifies the SNMP v3 Privacy protocol (AES)
-privPwd	**-privpw**	Specifies the SNMP v3 Privacy Password

Example

```
lunash:>sysconf snmp trap set -host mysnmphost

SNMP trap is not configured. No trap will be sent.

Command Result : 0 (Success)
```

sysconf snmp trap show

Display SNMP trap host information.

Syntax

sysconf snmp trap show

Example

```
lunash:>sysconf snmp trap show

SNMP trap is not configured. No trap will be sent.

Command Result : 0 (Success)
```

sysconf snmp trap test

Test the SNMP trap notification.

This command allows an administrator to create test logs to initiate trap notifications. Refer to the *Syslog Monitoring Guide* for details of which log messages result in traps.

To initiate a trap notification use the command parameters to format and record a log message via syslog. To distinguish between messages in the logs that are generated by this command and those that represent legitimate events, all log messages generated using this command are prefixed with “***TEST :”, as shown in the following example:

```
2012 Feb 29 12:05:01 myLUT  daemon crit  smartd[19685]: ***TEST : Device: /dev/sda, Temperature
45 Celsius reached limit of 44 Celsius (Min/Max 31/49)
```

Note: The Luna administrative shell prohibits the ‘<’ and ‘>’ characters as parameters. However, some traps rely on the presence of these comparators in log messages. To enable test log messages of the form that need these comparators, use a “.lt” or “.gt” string in place of the ‘<’ or ‘>’ character in the formatted command.

Note: This command writes a record to the applicable system log file. The command has no dependency on the status of the Luna SNMP Trap Daemon. To test trap generation, ensure that you have enabled traps as described in the *Syslog and SNMP Monitoring Guide*.

Syntax

sysconf snmp trap test -logfacility <logfacility> **-loglevel** <loglevel> **-process** <process> **-message** <message> [**-pid**]

Parameter	Shortcut	Description
-logfacility	**-logf**	Specifies the log facility to use when generating the test message. **Valid values:** kern, user, daemon, auth, syslog, authpriv, cron, local0, local1, local2, local3, local4, local5, local6, local7
--loglevel	**-logl**	Specifies the severity level to assign to the test message. **Valid values:** emergency, alert, critical, crit, error, err, warning, warn, notice, info, debug
-process	**-pr**	Specifies the system process to use when generating the test message. **Valid values:** Any process defined for the system. For example, NTLS, impievd, smartd, sysstatd.
-message	**-m**	A string that specifies the body text for the test message. You must enclose the string in double quotes ("<string>") if it contains spaces.
-pid	**-pi**	Add a process identifier to the test message.

Example

```
lunash:> sysconf snmp trap test -logfacility daemon -loglevel crit -process smartd -message
"Device: /dev/sda, Temperature 45 Celsius reached limit of 44 Celsius (Min/Max 31/49)" -pid

Command Result : 0 (Success)
```

sysconf snmp user

Access commands that allow you to view and configure the users that can access the SNMP agent. At least one user must be configured before the SNMP agent can be accessed.

Syntax

sysconf snmp user

Parameter	Shortcut	Description
add	**a**	Add a user. See "sysconf snmp user add" on page 437.
clear	**c**	Delete all users. See "sysconf snmp user clear" on page 438.
delete	**d**	Delete a user. See "sysconf snmp user delete" on page 439.
list	**l**	List the currently configured users. See "sysconf snmp user list" on page 440.

sysconf snmp user add

Add a user who can use SNMP service. To enhance security, the authpassword and the privpassword should not be set to the same value. SNMP users created with this command are automatically configured for:

- read (GET/GET-NEXT/GET-BULK)
- write (SET) and
- notify (TRAP/INFORM) access to all MIB objects.

> **Note:** It is not possible to modify the parameters for a configured user. You must use **sysconf snmp user delete** followed by **sysconf snmp user add**.

Syntax

sysconf snmp user add -secname <secname> **-authpassword** <password> [**-authprotocol** <protocol>] **-privpassword** <password>

Parameter	Shortcut	Description
-secName	**-s**	Specifies the security name. The name may be 1-to-31 characters; this is effectively the SNMPv3 term for "User name"
-authPassword	**-authPa**	Specifies the authentication password. The password may be 8-to-128 characters long (for better security, it should be different than the **privpassword**).
-authprotocol	**-authPr**	Specifies the authentication protocol. **Valid values:** SHA **Default:** SHA
-privPassword	**-privPa**	Specifies the privacy password or encryption password. The password may be 8-to-128 characters (for better security, it should be different than **authPassword**).
-privProtocol	**-privPr**	Specifies the privacy protocol. **Valid values:** AES **Default:** AES

Example

To create an SNMP user with the name "admin", issue the following command:

```
lunash:> sysconf snmp user add -secName admin -authPassword 12345678 -privPassword 87654321
```

An SNMP agent on the Luna host "myLuna1" can then be accessed by means of the Net-SNMP "snmpwalk utility, using a command like:

```
snmpwalk -v 3 -u admin -l authPriv -a SHA -A 12345678 -x AES -X 87654321 myLuna1 .1
```

sysconf snmp user clear

Delete all users that are currently configured to use the SNMP command with this Luna appliance. If you do not use the -force option, a prompt requires you to type "proceed" if the operation is to go ahead - otherwise, it is aborted.

Syntax

sysconf snmp user clear [**-force**]

Parameter	Shortcut	Description
-force	**-f**	Force the action without prompting.

Example

```
lunash:>sysconf snmp user clear

WARNING !!  This command deletes all user account information from the SNMP Agent.
If you are sure that you wish to proceed, then type 'proceed', otherwise type 'quit'.

> proceed

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

sysconf snmp user delete

Delete a specific (named) user that is currently configured to use the SNMP command with this Luna appliance (allowed to access the SNMP agent).

Syntax

lunash:> **sysconf snmp user delete -secname** <userid>

Parameter	Shortcut	Description
-secname	**-s**	Specifies the user name of the user you want to delete.

Example

```
lunash:>sysconf snmp user delete -secname localsnmp

SNMP user account information deleted

Command Result : 0 (Success)
```

sysconf snmp user list

Display a list of the users that are currently configured to use the SNMP command with this Luna appliance.

Syntax

sysconf snmp user list

Example

```
lunash:> sysconf snmp user list

SNMP  Users:
-----------
aUser
admin
admintoo
anotherUser
yetAnotherUser
```

sysconf ssh

Access commands that allow you to view or configure SSH options on the appliance.

Syntax

sysconf ssh

device
ip
password
port
publickey
regenkeypair
show

Parameter	Shortcut	Description
device	**d**	Set the SSH device restriction policy. See "sysconf ssh device" on page 442.
ip	**i**	Set the SSH IP restriction policy. See "sysconf ssh ip" on page 443.
password	**pa**	Enable or disable password authentication. See "sysconf ssh password" on page 444.
port	**po**	Set the SSHD listen port number (22, 1024-65535). See "sysconf ssh port" on page 447.
publickey	**pu**	View or configure SSH public keys. See "sysconf ssh publickey" on page 448.
regenKeyPair	**r**	Regenerate the SSH key pair. See "sysconf ssh regenkeypair" on page 451
show	**s**	Display the currently set SSH restriction policies. See "sysconf ssh show" on page 452

sysconf ssh device

Set the SSH device restriction policy.
This command restricts appliance/HSM administrative traffic (over SSH) to only the indicated Ethernet port. Use this where you need to segregate administrative traffic from client (NTLS) traffic. This command is an alternative to the command "sysconf ssh ip" on page 443, which performs the same action by specifying an IP address that corresponds to one of your network devices.

If you wish, SSH traffic restriction could complement client traffic restriction using the command "ntls bind" on page 212, which binds client (NTLS) traffic to a specific IP or device name on your Luna SA.

Syntax

sysconf ssh device <netdevice>

Parameter	Shortcut	Description
<netdevice>		Specifies the device to which you want to restrict the SSH service. **Valid values:** **all**: Allow SSH on all devices. **eth0**: Restrict SSH connections to the eth0 interface. **eth1**: Restrict SSH connections to the eth1 interface. **lo**: **Default:**

Example

```
lunash:>sysconf ssh device all

WARNING: SSH is already restricted to the specified IP address / ethernet
 card. No changes made.

Command Result : 0 (Success)

[myluna] lunash:>sysconf ssh device eth1
Success:  SSH now restricted to ethernet device eth1 (ip address 192.168.255.2).
             Restarting ssh service.
Stopping sshd:                                                [  OK  ]
Starting sshd:                                                [  OK  ]
Command Result : 0 (Success)

[myluna] lunash:>sysconf ssh show
SSHD configuration:
 SSHD Listen Port: 22 (Default)
SSH is restricted to ethernet device eth1 (ip address 192.168.255.2).
Password   authentication is enabled
Public key authentication is enabled

     Command Result : 0 (Success)
```

sysconf ssh ip

Set the SSH local-IP restriction policy.
This command restricts appliance/HSM administrative traffic (over SSH) to only the indicated IP address (bound to one of the Luna SA's Ethernet ports). Use this where you need to segregate administrative traffic from client (NTLS) traffic. This command is an alternative to the command "sysconf ssh device" on page 442, which performs the same action by specifying an Ethernet device.

If you wish, SSH traffic restriction could complement client traffic restriction using the command "ntls bind" on page 212, which binds client (NTLS) traffic to a specific IP or device name on your Luna SA.

Syntax

sysconf ssh ip <ipaddress>

Parameter	Shortcut	Description
<ipaddress>		Specifies the IP address associated with the Luna SA network interface device to which you want to restrict the SSH service. **Valid values:** Any ipv4 address.

Example

```
lunash:>sysconf ssh ip 192.20.10.200

Success:  SSH now restricted to ethernet device eth0 (ip address 192.20.10.200).
     Restarting ssh service.
Stopping sshd:                                              [  OK  ]
Starting sshd:                                              [  OK  ]

Command Result : 0 (Success)
```

sysconf ssh password

Access commands that allow you to enable or disable password authentication.

Syntax

sysconf ssh password

disable
enable

Parameter	Shortcut	Description
disable	**d**	Disable SSH password authentication. See "sysconf ssh password disable" on page 445.
enable	**e**	Enable SSH password authentication. See "sysconf ssh password enable" on page 446.

sysconf ssh password disable

Disable SSH password authentication.

Syntax

sysconf ssh password disable

Example

```
lunash:>sysconf ssh password disable

Password authentication disabled

Command Result : 0 (Success)
```

sysconf ssh password enable

Enable SSH password authentication.

Syntax

sysconf ssh password enable

Example

```
lunash:>sysconf ssh password enable

Password authentication enabled

Command Result : 0 (Success)
```

sysconf ssh port

Set the SSHD listen port number.

Syntax

sysconf ssh port <port>

Parameter	Shortcut	Description
<port>		Specifies the SSHD listen port number. **Range:** 22 or 1024-65535 **Default:** 22

Example

```
lunash:>sysconf ssh port 25

This command sets the SSHD listen port number.
Please make sure that you choose a new port number which is not used by other services.
Invalid New port number 25. It must be between 1024 and 65535 or 22.
Command Result : 65535 (Luna Shell execution)
[myluna] lunash:>sysconf ssh port 1024
This command sets the SSHD listen port number.
Please make sure that you choose a new port number which is not used by other services.
SSH Port Changed from 22 to:   Port 1024

Flushing firewall rules:                                       [  OK  ]
Setting chains to policy ACCEPT: filter                        [  OK  ]
Unloading iptables modules:                                    [  OK  ]
Applying iptables firewall rules:                              [  OK  ]
Loading additional iptables modules: ip_conntrack_netbios_n    [  OK  ]
Stopping sshd:                                                 [  OK  ]
Starting sshd:                                                 [  OK  ]

Command Result : 0 (Success)
```

sysconf ssh publickey

View or configure SSH public keys.

To add, list, delete, or clear public keys, see "my public-key" on page 182.

Once you enable public key authentication for an administration computer, the private SSH key (/root/.ssh/id_rsa) must be protected, and access to that computer must be restricted and password-protected. Anyone who can log into that computer can log into the Luna SA appliance without knowing the Luna shell (lunash:> admin password!

Note: The former commands to manage SSH publickeys have been removed
sysconf ssh publickey add
sysconf ssh publickey list
sysconf ssh publickey delete
sysconf ssh publickey clear

Those functions are now covered by equivalent commands:
my public-key add (See "my public-key add" on page 183)
my public-key clear (See "my public-key clear" on page 184)
my public-key delete (See "my public-key delete" on page 185)
my public-key list (See "my public-key list" on page 186)

Syntax

sysconf ssh publickey

disable
enable

Parameter	Shortcut	Description
disable	**di**	Disable SSH public key authentication. See "sysconf ssh publickey disable" on page 449.
enable	**e**	Enable SSH public key authentication. See "sysconf ssh publickey enable" on page 450.

sysconf ssh publickey disable

Disable SSH public key authentication.

Syntax

sysconf ssh publickey disable

Example

```
lunash:>sysconf ssh publicKey disable

Public key authentication disabled

Command Result : 0 (Success)
```

sysconf ssh publickey enable

Enable SSH public key authentication.

Once you enable public key authentication for an administration computer, the private SSH key (/root/.ssh/id_rsa) must be protected, and access to that computer must be restricted and password-protected. Anyone who can log into that computer can log into the Luna SA appliance without knowing the Luna shell (lunash:> admin password!

Syntax

sysconf ssh publickey enable

Example

```
lunash:>sysconf ssh publicKey enable

Public key authentication enabled

Command Result : 0 (Success)
```

sysconf ssh regenkeypair

Regenerate the SSH key pair.

Syntax

sysconf ssh regenkeypair

Example

```
lunash:>sysconf ssh regenkeypair

WARNING !!  This command regenerates SSH keypair.
WARNING !!  SSH will be restarted.

If you are sure that you wish to proceed, then type 'proceed', otherwise type 'quit'.
> proceed

 Proceeding...
Stopping sshd:                                   [  OK  ]
 Generating SSH1 RSA host key:                   [  OK  ]
Generating SSH2 RSA host key:                    [  OK  ]
 Generating SSH2 DSA host key:                   [  OK  ]
Starting sshd:                                   [  OK  ]

Command Result : 0 (Success)
```

sysconf ssh show

Display the currently configured SSH restrictions.

Syntax

sysconf ssh show

Example

```
lunash:>sysconf ssh show

SSHD configuration:

SSHD Listen Port: 22 (Default)
SSH is unrestricted.

Password   authentication is enabled
Public key authentication is enabled

Command Result : 0 (Success)
```

sysconf time

Set the appliance clock. Time and system date may be set to user-specified values. Specify the correct timezone before setting a new value for the system time. The hardware clock is automatically kept in sync whenever a change is made to the system date, time, or timezone.

You can determine the current date/time setting using the **status date** command.

Syntax

sysconf time <time> [<date>]

Parameter	Description
<time>	Specifies the time using 24-hour clock in the following format: HH:MM
<date>	Set the date along with system time. Specify the date using the following format: YYYYMMDD

Example

```
lunash:> sysconf time 15:37 20120202
Thu Feb 2 15:37:00 EST 2012
```

sysconf timezone

Show and set the timezone for the appliance's clock. This command allows the administrator to check and set the system timezone.

Syntax

sysconf timezone [**set** <timezone>] [**show**]

Parameter	Shortcut	Description
set	**se**	Set time zone.
show	**sh**	Shows the current timezone setting - but not in the format that the user needs to use when entering one;for example, it might show EST when the timezone code entered was EST5EDT.

Example

```
lunash:> sysconf timezone show
EST

lunash:> sysconf timezone set EST5EDT
Time zone set to EST5EDT
```

syslog

Access the syslog commands used to manage the system logs.

Syntax

syslog

cleanup
export
period
policy
remotehost
rotate
rotations
severity
show
tail
tarlogs

Parameter	Shortcut	Description
cleanup	**c**	Delete log files. See "sylog cleanup" on page 456.
export	**e**	Export syslog. See "syslog export" on page 457.
period	**p**	Set the syslog period. See "syslog period" on page 458.
remotehost	**re**	Configure Syslog remote hosts. See "syslog remotehost" on page 460.
rotate	**rotate**	Rotate log files. See "syslog rotate" on page 459.
rotations	**rotati**	Set syslog rotations. See "syslog rotations" on page 465
severity	**se**	Log severity. See "syslog severity set" on page 466.
show	**sh**	Get Syslog configuration. See "syslog show" on page 467.
tail	**tai**	Get last entries of log. See "syslog tail" on page 470.
tarlogs	**tar**	Archive log files. See "syslog tarlogs" on page 471.

sylog cleanup

Delete log files. Using this command following "syslog rotate" causes all grow-able log files to be deleted.

Syntax

syslog cleanup [**-force**]

Parameter	Parameter	Description
-force	**-f .**	Forces the command to proceed silently without prompting. Useful for scripting.

Example

```
lunash:>syslog cleanup
WARNING !!  This command creates an archive of the current logs then deletes ALL THE LOG FILES
except the hsm logs.
If you are sure that you wish to proceed, then type 'proceed', otherwise type 'quit'.
> proceed
Command Result : 0(Success)
```

syslog export

Prepare system logs for transfer from appliance. This command copies the current system log file to the export directory so that the user can use scp to transfer the file to another computer. Can be used for offline storage of old log files or to send to Technical Support for troubleshooting the Luna appliance.

Syntax

syslog export

Example

```
lunash:>syslog export

System log files successfully prepared for secure transfer.
Use scp from a client machine to get the file named: "syslog"

Command Result : 0 (Success)
```

syslog period

Set the time between syslog rotations.

Syntax

syslog period <syslogperiod>

Parameter	Shortcut	Description
<syslogperiod>		Specifies the log rotation period. **Valid values:** daily, weekly, monthly

Example

```
lunash:>syslog period daily

Log period set to daily.

Command Result : 0 (Success)
```

syslog rotate

Rotate log files immediately if they have not already been rotated on the same date. Logs cannot be rotated more than once per day.

Note: Using this command followed by "sysconf cleanup logs" causes all grow-able log files to be deleted.

EXCEPTION: The syslog rotate command does not rotate the NTP log file nor the hsm.log file. The HSM log is a small log file that provides critical information about the HSM. It does not grow very much throughout the life of the HSM.

Syntax

syslog rotate

Example

```
lunash:>syslog rotate
Command Result : 0 (Success)
```

syslog remotehost

Access the **syslog remotehost** commands to manage the syslog remote hosts.

Syntax

syslog remotehost

add
delete
list

Parameter	Shortcut	Description
add	**a**	Add a remote host. See "syslog remotehost add" on page 461.
clear	**c**	Delete All Remote Logging Servers. See "syslog remotehost clear" on page 462.
delete	**d**	Delete a remote host. See "syslog remotehost delete" on page 463.
list	**l**	List all syslog remote hosts. See "syslog remotehost list" on page 464.

syslog remotehost add

Add a remote host receiving the logs. Can be any system that provides the remote syslog service.

> **Note:** For this function to work you must open receiving udp port 514 on the remote log server.

Syntax

syslog remotehost add <hostname_or_IP_address>

Parameter	Shortcut	Description
<hostname_or_IP_address>		Specifies the hostname or the IP address of the remote computer system that will be accepting and storing the syslogs.

Example

```
lunash:>syslog remotehost add mylinuxbox

mylinuxbox added successfully
Please restart syslog with <service restart syslog> command
Make sure syslog service is started on mylinuxbox with -r option

Command Result : 0 (Success)
```

syslog remotehost clear

Delete all remote logging servers.

Syntax

syslog remotehost clear -force

Parameter	Shortcut	Description
-force	**-f**	Force the action; useful for scripting.

Example

```
[mylunasa6] lunash:>syslog remotehost clear

        All remote hosts receiving the logs will be deleted.
        Are you sure you wish to continue?

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

Shutting down kernel logger:                               [  OK  ]
Shutting down system logger:                               [  OK  ]
Starting system logger:                                    [  OK  ]
Starting kernel logger:                                    [  OK  ]

Command Result : 0 (Success)
[mylunasa6] lunash:>
```

syslog remotehost delete

Delete a remote host receiving the logs. Use "syslog remotehost list" to see which systems are receiving the logs.

Syntax

syslog remotehost delete <hostname_or_IP_address>

Parameter	Shortcut	Description
<hostname_or_IP_address>		Specifies the hostname or the IP address of the remote computer system to delete from the list.

Example

```
lunash:>syslog remotehost delete mylinuxbox

mylinuxbox deleted successfully
Please restart syslog with <service restart syslog> command
to stop logs to be sent to mylinuxbox

Command Result : 0 (Success)
```

syslog remotehost list

List the syslog remote hosts.

Syntax

syslog remotehost list

Example

```
lunash:>syslog remotehost list

List of syslog remote hosts:
mylinuxbox

Command Result : 0 (Success)
```

syslog rotations

Set the number of history files to keep when rotating system log files. For example, two rotations would keep the current log files and the most recent set; three rotations would keep the current log files and the two most recent sets. Specify a whole number less than 100.

Syntax

syslog rotations <syslog_rotations>

Parameter	Shortcut	Description
<syslog_rotations>		An integer that specifies the number of history files to keep when rotating system log files. **Range:** 1 to 100

Example

```
lunash:> syslog rotations 5

Log rotations set to 5

Command Result : 0 (Success)
```

lunash syslog Commands

syslog severity set

Set the log service severity threshold for events to be logged.

Syntax

syslog severity set -logname <logname> **-loglevel** <loglevel>

Parameter	Shortcut	Description
-loglevel	**-logl**	Specifies the severity level of the log messages to include in the logs. **Valid values:** (emergency,alert,critical,crit,error,err,warning,warn,notice,info,debug **Note:** These values are arranged from those which produce the fewest log entries to those which produce the most log entries.
-logname	**-logn**	The name of the log file to which you want to apply severity levels. Only lunalogs can have severity levels applied.

Example

```
lunash:>syslog severity set -logname lunalogs -loglevel error

This command sets the severity level of log messages.
Only messages with the severity of higher than or equal to the new
log level: "error" will be logged.
You must restart syslog using the "service restart syslog" command for
the changes to take effect.

Command Result : 0 (Success)
```

syslog show

Display the current log rotation configuration, and show the configured log levels. Optionally show a list of the log files.

Syntax

syslog show [**-files**]

Parameter	Shortcut	Description
-files	**-f**	Binary option. If this option is present, a list of all log files is presented. If this option is absent, then a summary of log configuration is shown, without the file list.

Example

In the example below, the asterisk beside the "hsm" entry indicates that ALL HSM events get logged and that this setting is not user configurable.

```
mylunasa6] lunash:>syslog show

Syslog configuration

   Rotations:         4
   Rotation Period:   weekly
   Log disk full policy:    tarlogs_cleanup

Configured Log Levels:
----------------------------
syslog:    *
lunalogs:  info
hsm:       *
secure:    *
cron:      notice
boot:      *

Note: '*' means all log levels.

Command Result : 0 (Success)
[mylunasa6] lunash:>


[mylunasa6] lunash:>syslog show -file

Syslog configuration

   Rotations:         4
   Rotation Period:   weekly
   Log disk full policy:    tarlogs_cleanup

Configured Log Levels:
----------------------------
syslog:    *
lunalogs:  info
```

```
hsm:       *
secure:    *
cron:      notice
boot:      *

Note: '*' means all log levels.

LogFileName                   Size Date Time
-------------------------------------------
acpid                          940  Apr 17 10:33
acpid-2014-04-09               439  Apr 9 2014
anaconda.log                140447  Mar 5 2013
anaconda.syslog              25575  Mar 5 2013
boot.log                         0  Apr 9 2014
btmp                          5760  Apr 2 00:53
btmp-20130516-0402             768  May 15 2013
btmp-2015-04-01               5376  Mar 6 14:38
cron                           456  Apr 29 04:02
cron-2015-04-05               1028  Apr 5 04:02
cron-2015-04-12                912  Apr 12 04:02
cron-2015-04-19                797  Apr 19 04:02
cron-2015-04-26                910  Apr 26 04:02
dmesg                        21618  Apr 17 10:33
faillog                          0  Feb 6 09:45
hsm.log                      50063  Apr 28 19:04
lastlog                      21900  Apr 29 14:36
lost+found                   16384  Mar 5 2013
lunalogs                   1353225  Apr 29 14:52
lunalogs-2015-04-05        2896633  Apr 5 04:02
lunalogs-2015-04-12        2892767  Apr 12 04:01
lunalogs-2015-04-19        2537642  Apr 19 04:01
lunalogs-2015-04-26        2746220  Apr 26 04:01
maillog                          0  Mar 5 2013
messages                   2604899  Apr 29 14:51
messages-2015-04-05        8710648  Apr 5 04:02
messages-2015-04-12        8709357  Apr 12 04:02
messages-2015-04-19        6948162  Apr 19 04:02
messages-2015-04-26        5284444  Apr 26 04:02
ntls_bt_2015-02-06_10_08_34     3112  Feb 6 10:08
ntls_bt_2015-02-06_14_17_11     3112  Feb 6 14:17
prelink                       4096  Mar 6 2013
rpmpkgs                       5719  Apr 29 04:02
rpmpkgs-20130310-0402         4649  Mar 9 2013
rpmpkgs-20130317-0402         4649  Mar 16 2013
rpmpkgs-20130516-0402         4649  Mar 20 2013
rpmpkgs-20130519-0402         4649  May 18 2013
rpmpkgs-2015-04-05            5719  Apr 4 04:02
rpmpkgs-2015-04-12            5719  Apr 11 04:02
rpmpkgs-2015-04-19            5719  Apr 18 04:02
rpmpkgs-2015-04-26            5719  Apr 25 04:02
secure                         248  Apr 29 14:36
secure-2015-04-05             9995  Apr 2 00:53
secure-2015-04-12              362  Apr 6 21:14
secure-2015-04-19             1662  Apr 17 13:36
secure-2015-04-26              720  Apr 20 13:55
spooler                          0  Mar 5 2013
tallylog                         0  Feb 6 09:45
```

```
update5_2_6_1.log              828  Feb 17 18:02
update6_0_0_31.log           11131  Feb 6 10:02
update6_0_0_33.log           10615  Feb 17 18:12
wtmp                        173184  Apr 29 14:36
wtmp-2015-04-23            1061760  Apr 23 03:14

Command Result : 0 (Success)
```

syslog tail

Display the last entries of the syslog. If no number is included, the command displays the entire syslog.

Syntax

syslog tail -logname <logname> [**-entries** <logentries>] [**-search** <string>]

Parameter	Shortcut	Description
-entries	**-e** <logname>	Specifies the number of entries to display. If this parameter is not specified, the entire log is displayed. **Range:** 0-2147483647
-logname	**-l** <logentries>	Specifies the log name. **Valid values:** lunalogs, messages, secure, hsm, ntp, snmp
-search	**-s** <string>	Search for the specified string.

Example

```
lunash:>syslog tail -logname hsm -entries 3

2011 Apr  3 14:49:02 myLuna  local6 info  oamp[2244]: INFO:     SM_Init OK
2011 Apr  3 14:49:02 myLuna  local6 info  oamp[2244]: INFO:     Supported callback I/O v.1
2011 Apr  3 14:49:02 myLuna  local6 info  oamp[2244]: INFO:     Supported callback protocol v.1

Command Result : 0 (Success)
```

syslog tarlogs

Archives log files to logs.tar file in scp temporary directory. A single logs.tgz file allows you to obtain all the logs in one operation.

Syntax

syslog tarlogs

Example

```
lunash:>syslog tarlogs

The tar file containing logs is now available via scp as filename 'logs.tgz'.

Command Result : 0 (Success)
```

token

Access the token-level commands. These commands are separate menus for token HSMs as backup devices or token HSMs used in PKI mode.

Syntax

token

backup
pki

Parameter	Shortcut	Description
backup	b	Access the **token backup** commands. See "token backup" on page 473.
pki	p	Access the **token pki** commands. See "token pki" on page 502.

token backup

Access the token backup commands.

Note: WHEN to USE lunash "token backup" commands, or use "vtl backup" commands?

Luna Shell (lunash:>) token backup commands operate a Luna Backup HSM attached directly to Luna SA via USB, and are **not** intended for use with remotely connected backup devices. You might have a *locally-connected backup HSM* *[connects directly to a Luna SA via USB cable]* and a locally connected serial terminal and be walking them from Luna SA to Luna SA in your server room to perform backups. Or you might be administering remotely via SSH and lunash:> commands, while a technician in your server center carries the backup HSM from one Luna SA to the next. In either case, these "token backup" commands are the method to use.The important distinction is where the backup HSM is physically connected - from the Luna SA perspective, those are both local backup operations to a Backup HSM that is locally connected to the appliance.

VTL backup commands operate a Luna Backup HSM connected to a computer, and located distantly from your primary Luna SA appliance. The VTL backup commands are **not** for use with a Luna Backup HSM that is connected directly to your Luna SA appliance. For true, hands-off, lights-out operation of your Luna appliances, use a Luna Remote Backup HSM located in your *administrator's office* *[or other convenient location]*, connected to a computer acting as a *Remote Backup server* *[this could be your administrative workstation, or it could be a completely separate computer]*. This means the computer and Backup HSM are located near you and remote/distant from your Luna SA appliance(s). For that application, use the **backup commands in the VTL utility** supplied with the Luna SA *Client software* *[which must be installed on the computer that is acting as Remote Backup server]* - the appliance token backup commands (previous paragraph) are not designed to work for Remote Backup.

Syntax

token backup

factoryreset
init
list
login
logout
partition
show
update

Parameter	Shortcut	Description
factoryreset	**f**	Reset a backup token to factory default settings. See "token backup factoryreset" on page 476.
init	**i**	Initializes the token with the specified serial number and prepares it to receive backup data. See "token backup init"

Parameter	Shortcut	Description
		on page 478.
list	**li**	List all backup tokens. See "token backup list" on page 480.
login	**logi**	Login backup token admin. See "token backup login" on page 482.
logout	**logo**	Logout backup token admin. See "token backup logout" on page 484.
partition	**p**	Access the token backup partition commands to manage your backup partitions. See "token backup partition" on page 485.
show	**s**	Get backup token information. See "token backup show" on page 493.
update	**u**	Update commands. See "token backup update" on page 495.

An external Luna HSM can be USB-connected to a Luna SA appliance for:

- local backup/restore operations (Luna Backup HSM)
- PKI bundle operations (Luna G5 HSM)

Luna SA does not pass PED operations and data through to an externally connected Luna HSM from a Luna PED that is connected locally to the Luna SA.

If the external HSM is PED-authenticated, then the options for Luna PED connection are:

- local PED connection, directly to the affected HSM, when needed, or
- Remote PED connection, passed through the Luna SA

Note: Support for PKI Bundles with Remote PED begins at firmware version 6.10.1 in the external HSM.

Note: Support for locally connected Backup HSM with Remote PED,
begins at firmware version 6.10.1 in the external HSM.

Note: Use of Remote PED with an external device is made possible when you set up with the commands
hsm ped vector init -serial <serial#_of_external_HSM>
and
hsm ped connect -serial <serial#_of_external_HSM>
before using **token pki** or **token backup** commands.

When labeling HSMs or partitions, never use a numeral as the first, or only, character in the name/label. Token backup commands allow slot-number OR label as identifier which can lead to confusion if the label is a string version of a slot number.

For example, if the token is initialized with the label "1" then the user cannot use the label to identify the target for purposes of backup, because VTL parses "1" as signifying the numeric ID of the first slot rather than as a text label for the target in whatever slot it really occupies (the target is unlikely to be in the first slot), so backup fails.

Luna shell (lunash:> token backup commands on Luna SA would be unable to see Luna Backup HSM slots maintained by Remote Backup server. Either connect the Backup HSM locally to the Luna SA USB port to use token backup commands, or use VTL commands directed to a Luna Remote Backup HSM connected to a computer configured as a backup server.

token backup factoryreset

Reset a backup token to factory default settings (destroys the KEK or permanently denies access to existing objects, erasesor authentication, so you need to initialize before using again). Can be run only from the local serial console.

The action is equivalent to the `hsm factoryReset` command that acts on the appliance's built-in HSM.

View a table that compares and contrasts various "deny access" events or actions that are sometimes confused. "Destroy" action/event scenarios (Right-click the link if you prefer that it not open in a new window.)

An external Luna HSM can be USB-connected to a Luna SA appliance for:

- local backup/restore operations (Luna Backup HSM)
- PKI bundle operations (Luna G5 HSM)

Luna SA does not pass PED operations and data through to an externally connected Luna HSM from a Luna PED that is connected locally to the Luna SA.

If the external HSM is PED-authenticated, then the options for Luna PED connection are:

- local PED connection, directly to the affected HSM, when needed, or
- Remote PED connection, passed through the Luna SA

Note: Support for PKI Bundles with Remote PED begins at firmware version 6.10.1 in the external HSM.

Note: Support for locally connected Backup HSM with Remote PED,
begins at firmware version 6.10.1 in the external HSM.

Note: Use of Remote PED with an external device is made possible when you set up with the commands
hsm ped vector init -serial <serial#_of_external_HSM>
and
hsm ped connect -serial <serial#_of_external_HSM>
before using **token pki** or **token backup** commands.

Note: WHEN to USE lunash "token backup" commands, or use "vtl backup" commands?

Luna Shell (lunash:>) token backup commands operate a Luna Backup HSM attached directly to Luna SA via USB, and are **not** intended for use with remotely connected backup devices. You might have a *locally-connected backup HSM* *[connects directly to a Luna SA via USB cable]* and a locally connected serial terminal and be walking them from Luna SA to Luna SA in your server room to perform backups. Or you might be administering remotely via SSH and lunash:> commands, while a technician in your server center carries the backup HSM from one Luna SA to the next. In either case, these "token backup" commands are the method to use.The important distinction is where the backup HSM is physically connected - from the

Luna SA perspective, those are both local backup operations to a Backup HSM that is locally connected to the appliance.

VTL backup commands operate a Luna Backup HSM connected to a computer, and located distantly from your primary Luna SA appliance. The VTL backup commands are **not** for use with a Luna Backup HSM that is connected directly to your Luna SA appliance.

For true, hands-off, lights-out operation of your Luna appliances, use a Luna Remote Backup HSM located in your *administrator's office* [*or other convenient location*], connected to a computer acting as a *Remote Backup server* [*this could be your administrative workstation, or it could be a completely separate computer*]. This means the computer and Backup HSM are located near you and remote/distant from your Luna SA appliance(s). For that application, use the **backup commands in the VTL utility** supplied with the Luna SA *Client software* [*which must be installed on the computer that is acting as Remote Backup server*] - the appliance token backup commands (previous paragraph) are not designed to work for Remote Backup.

Syntax

token backup factoryReset -serial <serialnum> [**-force**]

Parameter	Shortcut	Description
-serial	**-s**	Specifies the token serial number.
-force	**-f**	Force the action without prompting.

Example

```
lunash:> token backup factoryReset -serial 667788

Command Result : 0 (Success)
lunash:>

If you run the command via a network connection, the system refuses:
lunash:>token backup factoryReset

Error:  'token factoryReset' can only be run from the local
console. Login as 'admin' using the serial port on
the Luna SA before running this command.

Command Result : 0 (Success)
```

token backup init

Initializes the token with the specified serial number and prepares it to receive backup data. Both the "-label" and "-serial" parameters are required at the command line. For Luna SA with Password Authentication, the domain and Token Admin (SO) password are prompted, and your input is obscured by asterisk (*) symbols. For Luna SA with Trusted Path authentication, any typed values for domain or password are ignored and you are prompted for Luna PED operations with PED Keys.

Note: WHEN to USE lunash "token backup" commands, or use "vtl backup" commands?

Luna Shell (lunash:>) token backup commands operate a Luna Backup HSM attached directly to Luna SA via USB, and are **not** intended for use with remotely connected backup devices. You might have a *locally-connected backup HSM* *[connects directly to a Luna SA via USB cable]* and a locally connected serial terminal and be walking them from Luna SA to Luna SA in your server room to perform backups. Or you might be administering remotely via SSH and lunash:> commands, while a technician in your server center carries the backup HSM from one Luna SA to the next. In either case, these "token backup" commands are the method to use.The important distinction is where the backup HSM is physically connected - from the Luna SA perspective, those are both local backup operations to a Backup HSM that is locally connected to the appliance.

VTL backup commands operate a Luna Backup HSM connected to a computer, and located distantly from your primary Luna SA appliance. The VTL backup commands are **not** for use with a Luna Backup HSM that is connected directly to your Luna SA appliance. For true, hands-off, lights-out operation of your Luna appliances, use a Luna Remote Backup HSM located in your *administrator's office* *[or other convenient location]*, connected to a computer acting as a *Remote Backup server* *[this could be your administrative workstation, or it could be a completely separate computer]*. This means the computer and Backup HSM are located near you and remote/distant from your Luna SA appliance(s). For that application, use the **backup commands in the VTL utility** supplied with the Luna SA *Client software* *[which must be installed on the computer that is acting as Remote Backup server]* - the appliance token backup commands (previous paragraph) are not designed to work for Remote Backup.

Syntax

token backup init -label <label> **-serial** <serialnum> **[-domain** <domain>] **[-tokenadminpw** <password>] [**-force**]

Parameter	Shortcut	Description
-domain	**-d**	Backup Token Domain (required for Password authenticated HSMs, ignored for PED authenticated - if you prefer to not type it in the clear, on the command line, it is prompted later).
-force	**-f**	Force the action without prompting.
-label	**-l**	Token label.
-serial	**-s**	Token serial number.

Parameter	Shortcut	Description
-tokenadminpw	**-t**	Token Admin / SO Pas.sword (required for Password authenticated HSMs, ignored for PED authenticated - if you prefer to not type it in the clear, on the command line, it is prompted later).

An external Luna HSM can be USB-connected to a Luna SA appliance for:

- local backup/restore operations (Luna Backup HSM)
- PKI bundle operations (Luna G5 HSM)

Luna SA does not pass PED operations and data through to an externally connected Luna HSM from a Luna PED that is connected locally to the Luna SA.

If the external HSM is PED-authenticated, then the options for Luna PED connection are:

- local PED connection, directly to the affected HSM, when needed, or
- Remote PED connection, passed through the Luna SA

Note: Support for PKI Bundles with Remote PED begins at firmware version 6.10.1 in the external HSM.

Note: Support for locally connected Backup HSM with Remote PED,
begins at firmware version 6.10.1 in the external HSM.

Note: Use of Remote PED with an external device is made possible when you set up with the commands
hsm ped vector init -serial <serial#_of_external_HSM>
and
hsm ped connect -serial <serial#_of_external_HSM>
before using **token pki** or **token backup** commands.

Example

```
[myluna] lunash:> token init -label mytoken -serial 667788
Please enter a password for the Token Administrator:
> ********
Please enter a domain
> ********
Command result : 0 (Success)
[myluna] lunash:>
```

token backup list

Display a list all of the backup tokens on the system. This command shows all connected backup devices with their serial numbers. Use the serial number that you find with this command to identify specific backup HSMs or partitions that you can then query with the **token backup partition list** command for more detailed information.

Note: WHEN to USE lunash "token backup" commands, or use "vtl backup" commands?

Luna Shell (lunash:>) token backup commands operate a Luna Backup HSM attached directly to Luna SA via USB, and are **not** intended for use with remotely connected backup devices. You might have a *locally-connected backup HSM* *[connects directly to a Luna SA via USB cable]* and a locally connected serial terminal and be walking them from Luna SA to Luna SA in your server room to perform backups. Or you might be administering remotely via SSH and lunash:> commands, while a technician in your server center carries the backup HSM from one Luna SA to the next. In either case, these "token backup" commands are the method to use.The important distinction is where the backup HSM is physically connected - from the Luna SA perspective, those are both local backup operations to a Backup HSM that is locally connected to the appliance.

VTL backup commands operate a Luna Backup HSM connected to a computer, and located distantly from your primary Luna SA appliance. The VTL backup commands are **not** for use with a Luna Backup HSM that is connected directly to your Luna SA appliance. For true, hands-off, lights-out operation of your Luna appliances, use a Luna Remote Backup HSM located in your *administrator's office* *[or other convenient location]*, connected to a computer acting as a *Remote Backup server* *[this could be your administrative workstation, or it could be a completely separate computer]*. This means the computer and Backup HSM are located near you and remote/distant from your Luna SA appliance(s). For that application, use the **backup commands in the VTL utility** supplied with the Luna SA *Client software* *[which must be installed on the computer that is acting as Remote Backup server]* - the appliance token backup commands (previous paragraph) are not designed to work for Remote Backup.

Syntax

token backup list

Example

```
lunash:>token backup list

Token Details:
============
Token Label: G5backup2
Slot: 6
Serial #: 7000179
Firmware: 6.0.8
Hardware Model: Luna G5

Token Details:
============
Token Label: G5backup1
```

```
Slot: 7
Serial #: 700010
Firmware: 6.0.8
Hardware Model: Luna G5

Token Details:
============
Token Label: p1-15/04/2011
Slot: 1
Serial #: 5
Firmware: 4.8.6
Hardware Model: Luna PCM G4

Command Result : 0 (Success)
```

token backup login

Log the Backup Token Administrator into the backup token. This command is used immediately before performing a firmware update on a backup token.

Remember to always log out of the backup token using the **token backup logout** command.

Note: WHEN to USE lunash "token backup" commands, or use "vtl backup" commands?

Luna Shell (lunash:>) token backup commands operate a Luna Backup HSM attached directly to Luna SA via USB, and are **not** intended for use with remotely connected backup devices. You might have a *locally-connected backup HSM* *[connects directly to a Luna SA via USB cable]* and a locally connected serial terminal and be walking them from Luna SA to Luna SA in your server room to perform backups. Or you might be administering remotely via SSH and lunash:> commands, while a technician in your server center carries the backup HSM from one Luna SA to the next. In either case, these "token backup" commands are the method to use.The important distinction is where the backup HSM is physically connected - from the Luna SA perspective, those are both local backup operations to a Backup HSM that is locally connected to the appliance.

VTL backup commands operate a Luna Backup HSM connected to a computer, and located distantly from your primary Luna SA appliance. The VTL backup commands are **not** for use with a Luna Backup HSM that is connected directly to your Luna SA appliance. For true, hands-off, lights-out operation of your Luna appliances, use a Luna Remote Backup HSM located in your *administrator's office* *[or other convenient location]*, connected to a computer acting as a *Remote Backup server* *[this could be your administrative workstation, or it could be a completely separate computer]*. This means the computer and Backup HSM are located near you and remote/distant from your Luna SA appliance(s). For that application, use the **backup commands in the VTL utility** supplied with the Luna SA *Client software* *[which must be installed on the computer that is acting as Remote Backup server]* - the appliance token backup commands (previous paragraph) are not designed to work for Remote Backup.

An external Luna HSM can be USB-connected to a Luna SA appliance for:

- local backup/restore operations (Luna Backup HSM)
- PKI bundle operations (Luna G5 HSM)

Luna SA does not pass PED operations and data through to an externally connected Luna HSM from a Luna PED that is connected locally to the Luna SA.

If the external HSM is PED-authenticated, then the options for Luna PED connection are:

- local PED connection, directly to the affected HSM, when needed, or
- Remote PED connection, passed through the Luna SA

Note: Support for PKI Bundles with Remote PED begins at firmware version 6.10.1 in the external HSM.

Note: Support for locally connected Backup HSM with Remote PED, begins at firmware version 6.10.1 in the external HSM.

Note: Use of Remote PED with an external device is made possible when you set up with the commands
hsm ped vector init -serial <serial#_of_external_HSM>
and
hsm ped connect -serial <serial#_of_external_HSM>
before using **token pki** or **token backup** commands.

Syntax

token backup login -serial <serialnum> [**-password** <password>]

Parameter	Shortcut	Description
-serial	**-s**	Specifies the serial number of the backup HSM/token.
-password	**-p**	Specifies the Backup Token Administrator’s password. This parameter is mandatory in Luna SA with Password Authentication. It is ignored in Luna SA with PED Authentication.

Example

```
lunash:> token backup login -serial 667788

Luna PED operation required to login to backup token - use blue PED Key.
'token backup login' successful.
```

token backup logout

Log out the backup Token Administrator from the backup token.

Note: WHEN to USE lunash "token backup" commands, or use "vtl backup" commands?

Luna Shell (lunash:>) token backup commands operate a Luna Backup HSM attached directly to Luna SA via USB, and are **not** intended for use with remotely connected backup devices. You might have a *locally-connected backup HSM* *[connects directly to a Luna SA via USB cable]* and a locally connected serial terminal and be walking them from Luna SA to Luna SA in your server room to perform backups. Or you might be administering remotely via SSH and lunash:> commands, while a technician in your server center carries the backup HSM from one Luna SA to the next. In either case, these "token backup" commands are the method to use.The important distinction is where the backup HSM is physically connected - from the Luna SA perspective, those are both local backup operations to a Backup HSM that is locally connected to the appliance.

VTL backup commands operate a Luna Backup HSM connected to a computer, and located distantly from your primary Luna SA appliance. The VTL backup commands are **not** for use with a Luna Backup HSM that is connected directly to your Luna SA appliance. For true, hands-off, lights-out operation of your Luna appliances, use a Luna Remote Backup HSM located in your *administrator's office* *[or other convenient location]*, connected to a computer acting as a *Remote Backup server* *[this could be your administrative workstation, or it could be a completely separate computer]*. This means the computer and Backup HSM are located near you and remote/distant from your Luna SA appliance(s). For that application, use the **backup commands in the VTL utility** supplied with the Luna SA *Client software* *[which must be installed on the computer that is acting as Remote Backup server]* - the appliance token backup commands (previous paragraph) are not designed to work for Remote Backup.

Syntax

token backup logout -serial <serialnum>

Parameter	Shortcut	Description
-serial	**-s**	Specifies the serial number of the backup HSM/token.

Example

```
lunash:> token backup logout -serial 667788

'token logout' successful.
```

token backup partition

Access the token backup partition commands to manage your backup partitions.

Note: WHEN to USE lunash "token backup" commands, or use "vtl backup" commands?

Luna Shell (lunash:>) token backup commands operate a Luna Backup HSM attached directly to Luna SA via USB, and are **not** intended for use with remotely connected backup devices. You might have a *locally-connected backup HSM* *[connects directly to a Luna SA via USB cable]* and a locally connected serial terminal and be walking them from Luna SA to Luna SA in your server room to perform backups. Or you might be administering remotely via SSH and lunash:> commands, while a technician in your server center carries the backup HSM from one Luna SA to the next. In either case, these "token backup" commands are the method to use.The important distinction is where the backup HSM is physically connected - from the Luna SA perspective, those are both local backup operations to a Backup HSM that is locally connected to the appliance.

VTL backup commands operate a Luna Backup HSM connected to a computer, and located distantly from your primary Luna SA appliance. The VTL backup commands are **not** for use with a Luna Backup HSM that is connected directly to your Luna SA appliance. For true, hands-off, lights-out operation of your Luna appliances, use a Luna Remote Backup HSM located in your *administrator's office* *[or other convenient location]*, connected to a computer acting as a *Remote Backup server* *[this could be your administrative workstation, or it could be a completely separate computer]*. This means the computer and Backup HSM are located near you and remote/distant from your Luna SA appliance(s). For that application, use the **backup commands in the VTL utility** supplied with the Luna SA *Client software* *[which must be installed on the computer that is acting as Remote Backup server]* - the appliance token backup commands (previous paragraph) are not designed to work for Remote Backup.

An external Luna HSM can be USB-connected to a Luna SA appliance for:

- local backup/restore operations (Luna Backup HSM)
- PKI bundle operations (Luna G5 HSM)

Luna SA does not pass PED operations and data through to an externally connected Luna HSM from a Luna PED that is connected locally to the Luna SA.

If the external HSM is PED-authenticated, then the options for Luna PED connection are:

- local PED connection, directly to the affected HSM, when needed, or
- Remote PED connection, passed through the Luna SA

Note: Support for PKI Bundles with Remote PED begins at firmware version 6.10.1 in the external HSM.

Note: Support for locally connected Backup HSM with Remote PED, begins at firmware version 6.10.1 in the external HSM.

Note: Use of Remote PED with an external device is made possible when you set up with the commands
hsm ped vector init -serial <serial#_of_external_HSM>
and
hsm ped connect -serial <serial#_of_external_HSM>
before using **token pki** or **token backup** commands.

Syntax

token backup partition

delete
list
show

Parameter	Shortcut	Description
delete	**d**	Delete a backup partition. See
list	**l**	List the backup partitions. See
show	**s**	List the objects on a backup token. See

token backup partition delete

Delete a backup partition on the Backup device and free the license used by the HSM Partition. To use the token backup partition delete command you must be logged in to the Backup HSM as HSM Admin.

Note: WHEN to USE lunash "token backup" commands, or use "vtl backup" commands?

Luna Shell (lunash:>) token backup commands operate a Luna Backup HSM attached directly to Luna SA via USB, and are **not** intended for use with remotely connected backup devices. You might have a *locally-connected backup HSM* *[connects directly to a Luna SA via USB cable]* and a locally connected serial terminal and be walking them from Luna SA to Luna SA in your server room to perform backups. Or you might be administering remotely via SSH and lunash:> commands, while a technician in your server center carries the backup HSM from one Luna SA to the next. In either case, these "token backup" commands are the method to use.The important distinction is where the backup HSM is physically connected - from the Luna SA perspective, those are both local backup operations to a Backup HSM that is locally connected to the appliance.

VTL backup commands operate a Luna Backup HSM connected to a computer, and located distantly from your primary Luna SA appliance. The VTL backup commands are **not** for use with a Luna Backup HSM that is connected directly to your Luna SA appliance. For true, hands-off, lights-out operation of your Luna appliances, use a Luna Remote Backup HSM located in your *administrator's office* *[or other convenient location]*, connected to a computer acting as a *Remote Backup server* *[this could be your administrative workstation, or it could be a completely separate computer]*. This means the computer and Backup HSM are located near you and remote/distant from your Luna SA appliance(s). For that application, use the **backup commands in the VTL utility** supplied with the Luna SA *Client software* *[which must be installed on the computer that is acting as Remote Backup server]* - the appliance token backup commands (previous paragraph) are not designed to work for Remote Backup.

An external Luna HSM can be USB-connected to a Luna SA appliance for:

- local backup/restore operations (Luna Backup HSM)
- PKI bundle operations (Luna G5 HSM)

Luna SA does not pass PED operations and data through to an externally connected Luna HSM from a Luna PED that is connected locally to the Luna SA.

If the external HSM is PED-authenticated, then the options for Luna PED connection are:

- local PED connection, directly to the affected HSM, when needed, or
- Remote PED connection, passed through the Luna SA

Note: Support for PKI Bundles with Remote PED begins at firmware version 6.10.1 in the external HSM.

Note: Support for locally connected Backup HSM with Remote PED, begins at firmware version 6.10.1 in the external HSM.

Note: Use of Remote PED with an external device is made possible when you set up with the commands
hsm ped vector init -serial <serial#_of_external_HSM>
and
hsm ped connect -serial <serial#_of_external_HSM>
before using **token pki** or **token backup** commands.

Syntax

token backup partition delete -partition <partition_name> **-serial** <serialnum> [**-force**]

Parameter	Shortcut	Description
-force	**-f**	Specifies that the Backup Token partition is erased without prompting the user for a confirmation of this destructive command.
-partition	**-p**	Specifies the name of the Backup Token partition to delete. Obtain the Backup Token partition name by using the token backup partition list command.
-serial	**-s**	Specifies the serial number of the Backup Token partition to delete. Obtain the Backup Token partition serial number by using the token backup partition list command.

Example

```
lunash:> token backup partition -delete -partition b1 -serial 667788
CAUTION:  Are you sure you wish to delete the partition named:
b1
Type 'proceed' to delete the partition, or 'quit'
to quit now.
> quit
'token backup partition -delete' aborted.
lunash:> token backup partition -delete -partition b1
CAUTION:  Are you sure you wish to delete the partition named:
b1
Type 'proceed' to delete the partition, or 'quit'
to quit now.
> proceed
'token backup partition -delete' successful.
```

token backup partition list

Display a list of the partitions on the specified Luna Backup HSM. The serial number and name of each partition is displayed. Login as HSM Admin is not needed for execution of this command.

> **Note: WHEN to USE lunash "token backup" commands, or use "vtl backup" commands?**
>
> Luna Shell (lunash:>) token backup commands operate a Luna Backup HSM attached directly to Luna SA via USB, and are **not** intended for use with remotely connected backup devices. You might have a *locally-connected backup HSM* *[connects directly to a Luna SA via USB cable]* and a locally connected serial terminal and be walking them from Luna SA to Luna SA in your server room to perform backups. Or you might be administering remotely via SSH and lunash:> commands, while a technician in your server center carries the backup HSM from one Luna SA to the next. In either case, these "token backup" commands are the method to use.The important distinction is where the backup HSM is physically connected - from the Luna SA perspective, those are both local backup operations to a Backup HSM that is locally connected to the appliance.
>
> VTL backup commands operate a Luna Backup HSM connected to a computer, and located distantly from your primary Luna SA appliance. The VTL backup commands are **not** for use with a Luna Backup HSM that is connected directly to your Luna SA appliance. For true, hands-off, lights-out operation of your Luna appliances, use a Luna Remote Backup HSM located in your *administrator's office* *[or other convenient location]*, connected to a computer acting as a *Remote Backup server* *[this could be your administrative workstation, or it could be a completely separate computer]*. This means the computer and Backup HSM are located near you and remote/distant from your Luna SA appliance(s). For that application, use the **backup commands in the VTL utility** supplied with the Luna SA *Client software* *[which must be installed on the computer that is acting as Remote Backup server]* - the appliance token backup commands (previous paragraph) are not designed to work for Remote Backup.

The HSM firmware needs approximately 2K bytes of memory to manage each partition and data objects in it. To avoid you having to calculate the exact memory space available for data storage -- with you deducting the memory used by internal data structures --the "partition list" command adjusts the memory size attributes for you. Thus, the total available memory reported by "partition list" will be different than that reported by "token backup show" and "token backup partition list."

Syntax

token backup partition list -serial <serialnum>

Parameter	Shortcut	Description
-serial	**-s**	Specifies the serial number of the backup HSM/token.

-serial <serialnum> [mandatory] The serial number of the backup HSM/token.

Example

```
lunash:> token backup partition list -serial 667788
```

```
Partition: 65001001,     Name: ca1vin
Partition: 65001002,     Name: brigitte
```

token backup partition show

Display a list of objects on the backup token/HSM.

Note: WHEN to USE lunash "token backup" commands, or use "vtl backup" commands?

Luna Shell (lunash:>) token backup commands operate a Luna Backup HSM attached directly to Luna SA via USB, and are **not** intended for use with remotely connected backup devices. You might have a *locally-connected backup HSM* *[connects directly to a Luna SA via USB cable]* and a locally connected serial terminal and be walking them from Luna SA to Luna SA in your server room to perform backups. Or you might be administering remotely via SSH and lunash:> commands, while a technician in your server center carries the backup HSM from one Luna SA to the next. In either case, these "token backup" commands are the method to use.The important distinction is where the backup HSM is physically connected - from the Luna SA perspective, those are both local backup operations to a Backup HSM that is locally connected to the appliance.

VTL backup commands operate a Luna Backup HSM connected to a computer, and located distantly from your primary Luna SA appliance. The VTL backup commands are **not** for use with a Luna Backup HSM that is connected directly to your Luna SA appliance. For true, hands-off, lights-out operation of your Luna appliances, use a Luna Remote Backup HSM located in your *administrator's office* *[or other convenient location]*, connected to a computer acting as a *Remote Backup server* *[this could be your administrative workstation, or it could be a completely separate computer]*. This means the computer and Backup HSM are located near you and remote/distant from your Luna SA appliance(s). For that application, use the **backup commands in the VTL utility** supplied with the Luna SA *Client software* *[which must be installed on the computer that is acting as Remote Backup server]* - the appliance token backup commands (previous paragraph) are not designed to work for Remote Backup.

Syntax

token backup partition show -partition [<partitionName>] **-serial** <serialnum> **-password** <userPassword>

Parameter	Shortcut	Description
-password		Specifies the password of the partition for which to display information. If you do not specify a password, you are prompted to enter it when you execute the command.
-partition	**-par**	Specifies the name of the partition for which to display information. By default information about all partitions is shown. Obtain the partition name by using the **partition list** command.
-serial	**-s**	The serial number of the partition for which to display information. By default information about all partitions is shown. Obtain the partition name by using the **partition list** command.

Example

```
lunash:>token backup partition show -par mypartition1 -serial 667788
```

```
Please enter the user password for the token:
> ******
Partition Name:  mypartition1
Partition SN:    696969008
Number objects:  9

Object Label:  Generated DES3 Key
Object Type:   Symmetric Key

Object Label:  Generated RSA Public Key
Object Type:   Public Key

Object Label:  Generated RSA Private Key
Object Type:   Private Key

Object Label:  Generated RSA Public Key
Object Type:   Public Key

Object Label:  Generated RSA Private Key
Object Type:   Private Key

Object Label:  Generated DSA Public Key
Object Type:   Public Key

Object Label:  Generated DSA Private Key
Object Type:   Private Key

Object Label:  Generated DES Key
Object Type:   Symmetric Key

Object Label:  Generated AES Key
Object Type:   Symmetric Key

Command Result : 0 (Success)
```

token backup show

Displays the token label and firmware version for the specified backup token.

⚠ **CAUTION:** Wait at least 20 seconds before you run the **token backup show** command after performing a backup token backup firmware update.
If you run the **token backup show**command within 10 seconds or less following a successful completion of token backup update firmware, the **token backup show** command will hang and the green LED on the token reader will continue to flash. The work-around for the hanging state is to remove and re-insert the backup token and then rerun the **token backup show** command.

Note: WHEN to USE lunash "token backup" commands, or use "vtl backup" commands?

Luna Shell (lunash:>) token backup commands operate a Luna Backup HSM attached directly to Luna SA via USB, and are **not** intended for use with remotely connected backup devices.
You might have a *locally-connected backup HSM* *[connects directly to a Luna SA via USB cable]* and a locally connected serial terminal and be walking them from Luna SA to Luna SA in your server room to perform backups. Or you might be administering remotely via SSH and lunash:> commands, while a technician in your server center carries the backup HSM from one Luna SA to the next. In either case, these "token backup" commands are the method to use.The important distinction is where the backup HSM is physically connected - from the Luna SA perspective, those are both local backup operations to a Backup HSM that is locally connected to the appliance.

VTL backup commands operate a Luna Backup HSM connected to a computer, and located distantly from your primary Luna SA appliance. The VTL backup commands are **not** for use with a Luna Backup HSM that is connected directly to your Luna SA appliance.
For true, hands-off, lights-out operation of your Luna appliances, use a Luna Remote Backup HSM located in your *administrator's office* *[or other convenient location]*, connected to a computer acting as a *Remote Backup server* *[this could be your administrative workstation, or it could be a completely separate computer]*. This means the computer and Backup HSM are located near you and remote/distant from your Luna SA appliance(s). For that application, use the **backup commands in the VTL utility** supplied with the Luna SA *Client software* *[which must be installed on the computer that is acting as Remote Backup server]* - the appliance token backup commands (previous paragraph) are not designed to work for Remote Backup.

The HSM firmware needs approximately 2K bytes of memory to manage each partition and data objects in it. To avoid you having to calculate the exact memory space available for data storage -- with you deducting the memory used by internal data structures --the "partition list" command adjusts the memory size attributes for you. Thus, the total available memory reported by "partition list" will be different than that reported by "token backup show" and "token backup partition list."

Syntax

token backup show -serial <serialnum>

Parameter	Shortcut	Description
-serial	**-s**	The serial number of thebackup HSM/token.

Example

```
lunash:> token backup show -serial 667788
Token Details:
============
Token Label: samBK
Serial #: 667788
Firmware: 6.0.8
Hardware Model: Luna G5
Authentication Method: PED keys
Token Admin login status: Logged In
Token Admin login attempts left: 3 before Token zeroization!

Partition Information:
======================
Partitions licensed on token: 20
Partitions created on token: 0
----------------------

There are no partitions.

Token Storage Information:
==========================
Maximum Token Storage Space (Bytes): 16252928
Space In Use (Bytes): 0
Free Space Left (Bytes): 16252928

License Information:
====================
621010355-000 621-010355-000 G5 Backup Device Base
621000005-001 621-000005-001 Backup Device Partitions 20
621000006-001 621-000006-001 Backup Device Storage 15.5 MB
621000007-001 621-000007-001 Backup Device Store MTK Split Externally
621000008-001 621-000008-001 Backup Device Remote Ped Enable

Command result : 0 (Success)
```

token backup update

Access the token backup update commands to update the backup token capabilities or firmware.

A capability update or a firmware update is meant to be applied just one time to an HSM. If you attempt to re-apply a capability update to an HSM that already has the capability installed, the system throws an error like " C0000002 : RC_ GENERAL_ERROR ". A similar result occurs if you attempt to install a particular firmware update more than once on one HSM. This is expected behavior.

Note: WHEN to USE lunash "token backup" commands, or use "vtl backup" commands?

Luna Shell (lunash:>) token backup commands operate a Luna Backup HSM attached directly to Luna SA via USB, and are **not** intended for use with remotely connected backup devices. You might have a *locally-connected backup HSM* *[connects directly to a Luna SA via USB cable]* and a locally connected serial terminal and be walking them from Luna SA to Luna SA in your server room to perform backups. Or you might be administering remotely via SSH and lunash:> commands, while a technician in your server center carries the backup HSM from one Luna SA to the next. In either case, these "token backup" commands are the method to use.The important distinction is where the backup HSM is physically connected - from the Luna SA perspective, those are both local backup operations to a Backup HSM that is locally connected to the appliance.

VTL backup commands operate a Luna Backup HSM connected to a computer, and located distantly from your primary Luna SA appliance. The VTL backup commands are **not** for use with a Luna Backup HSM that is connected directly to your Luna SA appliance. For true, hands-off, lights-out operation of your Luna appliances, use a Luna Remote Backup HSM located in your *administrator's office* *[or other convenient location]*, connected to a computer acting as a *Remote Backup server* *[this could be your administrative workstation, or it could be a completely separate computer]*. This means the computer and Backup HSM are located near you and remote/distant from your Luna SA appliance(s). For that application, use the **backup commands in the VTL utility** supplied with the Luna SA *Client software* *[which must be installed on the computer that is acting as Remote Backup server]* - the appliance token backup commands (previous paragraph) are not designed to work for Remote Backup.

Syntax

token backup update

capability
firmware
show

Parameter	Shortcut	Description
capability		Update the capabilities for a backup token. See "token backup update capability" on page 497.
firmware		Update the firmware on a backup token. See "token backup update firmware" on page 499.

Parameter	Shortcut	Description
show		Show a list of the available backup token updates. See "token backup update show" on page 500.

token backup update capability

Update Backup Token Capability, using a capability update package that you have acquired from SafeNet and transferred via scp to the Luna appliance. Before you can use this command, you must:

- acquire the secure package update file from SafeNet and send the file to the Luna SA (using scp or pscp)
- open the file on the Luna SA with the lunash command **package update** <filename> **-authcode** <authcode>

Note: WHEN to USE lunash "token backup" commands, or use "vtl backup" commands?

Luna Shell (lunash:>) token backup commands operate a Luna Backup HSM attached directly to Luna SA via USB, and are **not** intended for use with remotely connected backup devices. You might have a *locally-connected backup HSM* *[connects directly to a Luna SA via USB cable]* and a locally connected serial terminal and be walking them from Luna SA to Luna SA in your server room to perform backups. Or you might be administering remotely via SSH and lunash:> commands, while a technician in your server center carries the backup HSM from one Luna SA to the next. In either case, these "token backup" commands are the method to use.The important distinction is where the backup HSM is physically connected - from the Luna SA perspective, those are both local backup operations to a Backup HSM that is locally connected to the appliance.

VTL backup commands operate a Luna Backup HSM connected to a computer, and located distantly from your primary Luna SA appliance. The VTL backup commands are **not** for use with a Luna Backup HSM that is connected directly to your Luna SA appliance. For true, hands-off, lights-out operation of your Luna appliances, use a Luna Remote Backup HSM located in your *administrator's office* *[or other convenient location]*, connected to a computer acting as a *Remote Backup server* *[this could be your administrative workstation, or it could be a completely separate computer]*. This means the computer and Backup HSM are located near you and remote/distant from your Luna SA appliance(s). For that application, use the **backup commands in the VTL utility** supplied with the Luna SA *Client software* *[which must be installed on the computer that is acting as Remote Backup server]* - the appliance token backup commands (previous paragraph) are not designed to work for Remote Backup.

A capability update or a firmware update is meant to be applied just one time to an HSM. If you attempt to re-apply a capability update to an HSM that already has the capability installed, the system throws an error like " C0000002 : RC_GENERAL_ERROR ". A similar result occurs if you attempt to install a particular firmware update more than once on one HSM. This is expected behavior.

Syntax

token backup update capability -serial <serialnum> **-capability** <capabilityname> [**-force**]

Parameter	Shortcut	Description
-capability	**-c**	Specifies the capability name.
-force	**-f**	Force the action without prompting.
-serial	**-s**	Specifies the token serial number.

Example

```
lunash:>token backup update capability -serial 667788 -capability newcapability

CAUTION:  This command updates the Token Capability.
This process cannot be reversed.

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

> proceed

This is a NON-destructive capability update

Update Result :0 (Capability newcapability added)

Command Result : 0 (Success)
```

token backup update firmware

Update the firmware on a backup token, using a firmware update package available on the Luna appliance. The package must be transferred to the Luna appliance by scp (individually or as a component of a system update), and you must login to the backup token as Token Administrator (using the **token backup login** command) or SO before the token backup update firmware command is run. The command requires no package name.

The term "token" in this case refers to removable token-format HSMs connected via Luna DOCK 2 and USB, or Luna Remote Backup HSM, connected via USB.

Before you can use this command, you must:

- acquire the secure package update file from SafeNet and send the file to the Luna SA (using scp or pscp)
- open the file on the Luna SA using the **package update** command.

Note: Firmware update is a local operation only, and is not supported remotely.

A capability update or a firmware update is meant to be applied just one time to an HSM. If you attempt to re-apply a capability update to an HSM that already has the capability installed, the system throws an error like " C0000002 : RC_GENERAL_ERROR ". A similar result occurs if you attempt to install a particular firmware update more than once on one HSM. This is expected behavior.

Syntax

token backup update firmware -serial <serialnum> [**-force**]

Parameter	Shortcut	Description
-force	**-f**	Force the action without prompting.
-serial	**-s**	Specifies the token serial number.

Example

```
lunash:>token backup update firmware -serial 667788

CAUTION: This command updates the Token firmware.
This process cannot be reversed.

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

>proceed

Success
Firmware updated.
```

token backup update show

Display information about any capability updates that are available for backup tokens. This refers to update files that have been uploaded to the Luna appliance and are available to be applied to an attached backup HSM.

Note: WHEN to USE lunash "token backup" commands, or use "vtl backup" commands?

Luna Shell (lunash:>) token backup commands operate a Luna Backup HSM attached directly to Luna SA via USB, and are **not** intended for use with remotely connected backup devices. You might have a *locally-connected backup HSM* *[connects directly to a Luna SA via USB cable]* and a locally connected serial terminal and be walking them from Luna SA to Luna SA in your server room to perform backups. Or you might be administering remotely via SSH and lunash:> commands, while a technician in your server center carries the backup HSM from one Luna SA to the next. In either case, these "token backup" commands are the method to use.The important distinction is where the backup HSM is physically connected - from the Luna SA perspective, those are both local backup operations to a Backup HSM that is locally connected to the appliance.

VTL backup commands operate a Luna Backup HSM connected to a computer, and located distantly from your primary Luna SA appliance. The VTL backup commands are **not** for use with a Luna Backup HSM that is connected directly to your Luna SA appliance. For true, hands-off, lights-out operation of your Luna appliances, use a Luna Remote Backup HSM located in your *administrator's office* *[or other convenient location]*, connected to a computer acting as a *Remote Backup server* *[this could be your administrative workstation, or it could be a completely separate computer]*. This means the computer and Backup HSM are located near you and remote/distant from your Luna SA appliance(s). For that application, use the **backup commands in the VTL utility** supplied with the Luna SA *Client software* *[which must be installed on the computer that is acting as Remote Backup server]* - the appliance token backup commands (previous paragraph) are not designed to work for Remote Backup.

Syntax

token backup update show -serial <serialnum>

Parameter	Shortcut	Description
-serial	**-s**	Specifies the serial number of the backup token.

Example

Capability updates are not available

```
lunash:> token backup update show -serial 667788

Capability Updates:
   There are no capability updates available.

Command Result : 0 (Success)
```

Capability updates are available

```
lunash:> token backup update show

Capability Updates:
   HsmStorage15.5Meg
   Partitions20

Command Result : 0 (Success)
```

token pki

Access the **token pki** commands. These commands allow you to operate token HSMs (with Luna G5 HSM connected to the Luna SA via USB) when used in PKI mode.

Note: The PKI Bundle feature is supported with PED-authenticated Luna SA, and the connected Luna G5 HSM must also be PED-authenticated.

PKI bundling with password-authenticated Luna SA or Luna G5 is not supported.

Note: The Luna SA PKI Bundle option does not support Per-Partition Security Officer (PPSO). That is, a Luna G5 HSM that is USB-connected to a Luna SA appliance can be configured with any compatible firmware, including firmware version 6.22.0 (or newer), but cannot have the PPSO capability applied.

Note: Luna SA PKI Bundle option **does not support** the use of Luna DOCK2 and removable PCMCIA token HSMs (Luna CA4).

An external Luna HSM can be USB-connected to a Luna SA appliance for:

- local backup/restore operations (Luna Backup HSM)
- PKI bundle operations (Luna G5 HSM)

Luna SA does not pass PED operations and data through to an externally connected Luna HSM from a Luna PED that is connected locally to the Luna SA.

If the external HSM is PED-authenticated, then the options for Luna PED connection are:

- local PED connection, directly to the affected HSM, when needed, or
- Remote PED connection, passed through the Luna SA

Note: Support for PKI Bundles with Remote PED begins at firmware version 6.10.1 in the external HSM.

Note: Support for locally connected Backup HSM with Remote PED,
begins at firmware version 6.10.1 in the external HSM.

Note: Use of Remote PED with an external device is made possible when you set up with the commands
hsm ped vector init -serial <serial#_of_external_HSM>
and
hsm ped connect -serial <serial#_of_external_HSM>
before using **token pki** or **token backup** commands.

Syntax

token pki

activate
changepin
clone
deploy
factoryreset
listall
listdeployed
predeploy
resetpin
undeploy
update

Parameter	Shortcut	Description
activate	**a**	Activate PKI Token for use with your application. See "token pki activate" on page 505.
changepin	**ch**	Change PKI Token PIN. See "token pki changepin" on page 506.
clone	**cl**	Clone PKI Token contents. See "token pki clone" on page 508.
deploy	**d**	Deploy PKI Token. See "token pki deploy" on page 510.
factoryreset	**fr**	Factory Reset PKI Token. See "token pki factoryreset" on page 512.
listall	**lista**	List All PKI Tokens. See "token pki listall" on page 513.
listdeployed	**listd**	List All Deployed Tokens. See "token pki listdeployed" on page 514.
predeploy	**p**	Pre-deploy PKI Token. See "token pki predeploy" on page 515.
resetpin	**r**	Reset PKI Token PIN. See "token pki resetpin" on page 517.
undeploy	**un**	Undeploy PKI Token. See "token pki undeploy" on page 519.
update	**up**	Access the token pki update commands.See "token pki update" on page 520.

Note: The above commands prepare an HSM, externally connected to a Luna SA appliance, for operation in the PKI use-case. However, once the external HSM has been deployed for PKI bundle, it must be assigned to the remote client, by means of the command "client assignpartition" on page 52.

token pki activate

Cache a deployed PKI token's PED key data. Clients can then connect, authenticate with their token password, and perform operations with token objects, without need for hands-on PED operations each time. Activation/cacheing endures until terminated by token removal or appliance power off. If a token has not been activated, then each access attempt by a Client causes a login call which initiates a Luna PED operation (requiring the appropriate black PED Key). Unattended operation is possible while the token is activated.

An external Luna HSM can be USB-connected to a Luna SA appliance for:

- local backup/restore operations (Luna Backup HSM)
- PKI bundle operations (Luna G5 HSM)

Luna SA does not pass PED operations and data through to an externally connected Luna HSM from a Luna PED that is connected locally to the Luna SA.

If the external HSM is PED-authenticated, then the options for Luna PED connection are:

- local PED connection, directly to the affected HSM, when needed, or
- Remote PED connection, passed through the Luna SA

Note: Support for PKI Bundles with Remote PED begins at firmware version 6.10.1 in the external HSM.

Note: Support for locally connected Backup HSM with Remote PED,
begins at firmware version 6.10.1 in the external HSM.

Note: Use of Remote PED with an external device is made possible when you set up with the commands
hsm ped vector init -serial <serial#_of_external_HSM>
and
hsm ped connect -serial <serial#_of_external_HSM>
before using **token pki** or **token backup** commands.

Snytax

token pki activate -label <token_label>

Parameter	Shortcut	Description
-label	**-l**	Specifies the name of the inserted, deployed token to activate. Use the **token pki listdeployed** command to get the token name.

Example

```
lunash:> token pki activate -label mylunaca4-1

'token activate' successful.
```

token pki changepin

Change the challenge secret or password for the indicated PKI device.

An external Luna HSM can be USB-connected to a Luna SA appliance for:

- local backup/restore operations (Luna Backup HSM)
- PKI bundle operations (Luna G5 HSM)

Luna SA does not pass PED operations and data through to an externally connected Luna HSM from a Luna PED that is connected locally to the Luna SA.

If the external HSM is PED-authenticated, then the options for Luna PED connection are:

- local PED connection, directly to the affected HSM, when needed, or
- Remote PED connection, passed through the Luna SA

Note: Support for PKI Bundles with Remote PED begins at firmware version 6.10.1 in the external HSM.

Note: Support for locally connected Backup HSM with Remote PED,
begins at firmware version 6.10.1 in the external HSM.

Note: Use of Remote PED with an external device is made possible when you set up with the commands
hsm ped vector init -serial <serial#_of_external_HSM>
and
hsm ped connect -serial <serial#_of_external_HSM>
before using **token pki** or **token backup** commands.

Syntax

token pki changePin -serial <tokenserialnumber> [**-force**]

Parameter	Shortcut	Description
-force	**-f**	Force the action with no prompting.
-serial	**-s**	Specifies the serial number of the inserted token, whose password or challenge is to change. Use the **token pki list** command to get the token serial number.

Example

```
lunash:> token pki changepin -serial 1766711

Please type "proceed" to continue, anything else to abort: proceed

**********************************************
*                                            *
*     About to change the user password      *
*     Please pay attention to the PED        *
*                                            *
**********************************************
Please enter the current user challenge:

The partition has not been activated yet.

Luna PED operation required to activate partition on HSM - use User or
Partition Owner (black) PED key.

Please enter the new user challenge:

Please re-enter the new user challenge:

Success changing the user password for slot 4 !

Command Result : 0 (Success)
```

token pki clone

Clone a source PKI device to a target PKI device.

An external Luna HSM can be USB-connected to a Luna SA appliance for:

- local backup/restore operations (Luna Backup HSM)
- PKI bundle operations (Luna G5 HSM)

Luna SA does not pass PED operations and data through to an externally connected Luna HSM from a Luna PED that is connected locally to the Luna SA.

If the external HSM is PED-authenticated, then the options for Luna PED connection are:

- local PED connection, directly to the affected HSM, when needed, or
- Remote PED connection, passed through the Luna SA

Note: Support for PKI Bundles with Remote PED begins at firmware version 6.10.1 in the external HSM.

Note: Support for locally connected Backup HSM with Remote PED,
begins at firmware version 6.10.1 in the external HSM.

Note: Use of Remote PED with an external device is made possible when you set up with the commands
hsm ped vector init -serial <serial#_of_external_HSM>
and
hsm ped connect -serial <serial#_of_external_HSM>
before using **token pki** or **token backup** commands.

Syntax

token pki clone -source <serial_number> **-target** <serial_number> [**-force**]

Parameter	Shortcut	Description
-force	**-f**	Force the action with no prompting.
-source	**-s**	Specifies the serial number of the inserted PKI token HSM, whose contents are to be securely copied (cloned) to another HSM. Use the **token pki list** command to get the token serial number.
-target	**-t**	Specifies the serial number of the inserted PKI token HSM, which is to receive the securely copied (cloned) contents of the source HSM. Use the **token pki list** command to get the token serial number.

Example

```
lunash:> token pki clone -source 700180 -target 700179

Please type "proceed" to continue, anything else to abort: proceed
Please enter the user challenge for source token:

Please enter the user challenge for target token:
Successfully cloned object 14 from source slot 5 to object 11 on target slot 4
Successfully cloned object 15 from source slot 5 to object 12 on target slot 4
Successfully cloned object 16 from source slot 5 to object 13 on target slot 4
Successfully cloned object 17 from source slot 5 to object 14 on target slot 4
Successfully cloned object 18 from source slot 5 to object 15 on target slot 4
Successfully cloned object 19 from source slot 5 to object 16 on target slot 4
Successfully cloned object 20 from source slot 5 to object 17 on target slot 4
Successfully cloned object 21 from source slot 5 to object 18 on target slot 4
Successfully cloned object 22 from source slot 5 to object 19 on target slot 4
Successfully cloned object 23 from source slot 5 to object 20 on target slot 4
Successfully cloned object 24 from source slot 5 to object 21 on target slot 4
Successfully cloned object 25 from source slot 5 to object 22 on target slot 4
Successfully cloned object 26 from source slot 5 to object 23 on target slot 4
Successfully cloned object 27 from source slot 5 to object 24 on target slot 4
Successfully cloned object 28 from source slot 5 to object 25 on target slot 4
Successfully cloned object 29 from source slot 5 to object 26 on target slot 4
Successfully cloned object 30 from source slot 5 to object 27 on target slot 4
Successfully cloned object 31 from source slot 5 to object 28 on target slot 4
Successfully cloned object 32 from source slot 5 to object 29 on target slot 4
Successfully cloned object 33 from source slot 5 to object 30 on target slot 4

Success cloning 20 objects from source slot 5 to destination slot 4

Success cloning token with serial num: 700180 to token with serial num: 700179!

Command Result : 0 (Success)
```

token pki deploy

Make the pre-deployed (initialized) token/hsm available to the Luna SA appliance as another (removable) HSM partition or PKCS#11 slot, for use by your application(s).

Note: It may take up to one minute for the token to be visible to all clients.

An external Luna HSM can be USB-connected to a Luna SA appliance for:

- local backup/restore operations (Luna Backup HSM)
- PKI bundle operations (Luna G5 HSM)

Luna SA does not pass PED operations and data through to an externally connected Luna HSM from a Luna PED that is connected locally to the Luna SA.

If the external HSM is PED-authenticated, then the options for Luna PED connection are:

- local PED connection, directly to the affected HSM, when needed, or
- Remote PED connection, passed through the Luna SA

Note: Support for PKI Bundles with Remote PED begins at firmware version 6.10.1 in the external HSM.

Note: Support for locally connected Backup HSM with Remote PED,
begins at firmware version 6.10.1 in the external HSM.

Note: Use of Remote PED with an external device is made possible when you set up with the commands
hsm ped vector init -serial <serial#_of_external_HSM>
and
hsm ped connect -serial <serial#_of_external_HSM>
before using **token pki** or **token backup** commands.

Syntax

token pki deploy -label <token_label> **-serial** <serial_number>

Parameter	Shortcut	Description
-label	**-l**	Specifies the name of the inserted, pre-deployed token to deploy.
-serial	**-s**	Specifies the serial number of the inserted, pre-deployed token to deploy.

Example

```
lunash:> token pki deploy -label mylunag5pki -serial 475289
```

```
**********************************************
*                                            *
*   About to activate the token for testing. *
*   Please pay attention to the PED          *
*                                            *
**********************************************

Please enter the current user challenge:

Success deploying token mylunag5pki with serial num 475289 !

Command Result : 0 (Success)
```

Note: The above command prepares an HSM, externally connected to a Luna SA appliance, for operation in the PKI use-case. However, once the external HSM has been deployed for PKI bundle, it must be assigned to the remote client, by means of the command "client assignpartition" on page 52.

token pki factoryreset

Resets the backup token to factory default. You must run this command from the local serial console.

This command works on a removable PKI token in a connected Luna DOCK 2, or on a Luna G5 HSM. If both are connected, both are seen. If two Luna G5 HSMs are connected for PKI, both are seen. With multiple PKI devices connected, the "tokenfactoryreset" command affects only the device that you identify by serial number. If a backup device (token or Luna Remote Backup HSM) is connected, it is ignored by the "token pki..." command.

The action is equivalent to the **hsm factoryReset** command that acts on the appliance's built-in HSM.

See "Destroy action/event scenarios" to view a table that compares and contrasts various "deny access" events or actions that are sometimes confused.

Syntax

token pki factoryreset -serial <serial_number> [**-force**]

Parameter	Shortcut	Description
-force	**-l**	Force the action without prompting.
-serial	**-s**	Specifies the serial number of the token to reset.

Example

```
lunash:> token pki factoryReset -serial 123456

Command Result : 0 (Success)
```

token pki listall

Lists all PKI devices on the system. For a list of only the deployed devices, run the **token pki listdeployed** command.

Syntax

token pki list

Example

```
lunash:> token pki listall

Token Details:
============
Token Label:      G5PKI1
Slot:             5
Serial #:         7000180
Firmware:         6.0.8
Hardware Model:   Luna G5

Token Details:
============
Token Label:      CA4
Slot:             2
Serial #:         10007
Firmware:         4.8.6
Hardware Model:   Luna PCM G4
```

token pki listdeployed

Lists all deployed PKI devices.

Syntax

token pki listdeployed

Example

```
lunash:> token pki listdeployed

Label                   Serial Num
----------------------------------
G5PKI1                  7000180
```

token pki predeploy

Initialize a G5 HSM/token for use as a PKI device in Luna SA. This command prepares the token to be recognized and deployed.

Note: The PKI Bundle feature is supported with PED-authenticated Luna SA. The connected Luna G5 HSM must be PED-authenticated. PKI bundling with password-authenticated Luna SA or Luna G5 is not supported.

Syntax

lunash:> token pki predeploy -label <tokenlabel> -serial <serialnum> [-force]

Parameter	Shortcut	Description
-force	**-f**	Force the action without prompting.
-label	**-l**	Specifies the name of the inserted token to pre-deploy.
-serial	**-s**	Specifies the serial number of the token to pre-deploy.

Example

```
lunash:> token pki predeploy -label myPKI -serial 777199 -force

Please type "proceed" to continue, anything else to abort: proceed
********************************************
*                                          *
*     About to factory Reset the HSM       *
*                                          *
********************************************
********************************************
*                                          *
*   About to initialize the HSM            *
*   Please pay attention to the PED        *
*                                          *
********************************************

Do you want to use FIPS-approved algorithms and key strengths only (yes or no)? yes

********************************************
*                                          *
*   About to change the HSM FIPS policy    *
*   Please pay attention to the PED        *
*                                          *
********************************************
********************************************
*                                          *
*   About to create a partition on the HSM *
*   Please pay attention to the PED        *
*                                          *
********************************************
********************************************
*                                          *
*   About to set the partition policies    *
*   Please pay attention to the PED        *
*                                          *
********************************************
********************************************
*                                          *
*   About to create a partition challenge  *
*   and activate the partition.            *
*   Please pay attention to the PED        *
*   Please write down the PED secret!      *
*                                          *
********************************************

Please enter the partition challenge:

        Please attend to the PED.
Success predeploying the token!!

Command Result : 0 (Success)
```

token pki resetpin

Reset the challenge secret or password for the indicated PKI device.

An external Luna HSM can be USB-connected to a Luna SA appliance for:

- local backup/restore operations (Luna Backup HSM)
- PKI bundle operations (Luna G5 HSM)

Luna SA does not pass PED operations and data through to an externally connected Luna HSM from a Luna PED that is connected locally to the Luna SA.

If the external HSM is PED-authenticated, then the options for Luna PED connection are:

- local PED connection, directly to the affected HSM, when needed, or
- Remote PED connection, passed through the Luna SA

Note: Support for PKI Bundles with Remote PED begins at firmware version 6.10.1 in the external HSM.

Note: Support for locally connected Backup HSM with Remote PED, begins at firmware version 6.10.1 in the external HSM.

Note: Use of Remote PED with an external device is made possible when you set up with the commands
hsm ped vector init -serial <serial#_of_external_HSM>
and
hsm ped connect -serial <serial#_of_external_HSM>
before using **token pki** or **token backup** commands.

Syntax

token pki resetPin -serial <token_serial_number> [**-force**]

Parameter	Shortcut	Description
-force	**-f**	Force the action without prompting.
-serial	**-s**	Specifies the serial number of the inserted token, whose password or challenge is to be reset. Use the token pki list command to get the token serial number.

Example

```
lunash:> token pki resetPin -serial 475289


Please type "proceed" to continue, anything else to abort: proceed
Luna PED operation required to login as HSM Administrator - use Security Officer (blue) PED key.
```

```
Please ensure that you copy the password from the Luna PED
and that you keep it in a safe place.


Command Result : 0 (Success)
```

token pki undeploy

Makes the deployed token/hsm unavailable to the Luna SA appliance - no longer visible as another (removable) HSM partition or PKCS#11 slot, no longer accessible for use by your application(s).

Syntax

token pki undeploy -label <tokenlabel> [**-force**]

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

Example

```
lunash:> token pki undeploy -label myG5Pki

Please type "proceed" to continue, anything else to abort: proceed
Success undeploying token myG5Pki

Command Result : 0 (Success)
```

token pki update

Access the pki update commands to update the token capabilities or firmware.

Luna shell (lunash:>) token pki commands on Luna SA would be unable to see Luna G5 HSM PKI slots connected to a remote workstation. Either connect the Luna G5 HSM locally to the Luna SA USB port to use token backup commands, or use VTL commands on an HSM connected to a computer configured as a Client of your Luna SA.

An external Luna HSM can be USB-connected to a Luna SA appliance for:

- local backup/restore operations (Luna Backup HSM)
- PKI bundle operations (Luna G5 HSM)

Luna SA does not pass PED operations and data through to an externally connected Luna HSM from a Luna PED that is connected locally to the Luna SA.

If the external HSM is PED-authenticated, then the options for Luna PED connection are:

- local PED connection, directly to the affected HSM, when needed, or
- Remote PED connection, passed through the Luna SA

Note: Support for PKI Bundles with Remote PED begins at firmware version 6.10.1 in the external HSM.

Note: Support for locally connected Backup HSM with Remote PED, begins at firmware version 6.10.1 in the external HSM.

Note: Use of Remote PED with an external device is made possible when you set up with the commands
hsm ped vector init -serial <serial#_of_external_HSM>
and
hsm ped connect -serial <serial#_of_external_HSM>
before using **token pki** or **token backup** commands.

A capability update or a firmware update is meant to be applied just one time to an HSM. If you attempt to re-apply a capability update to an HSM that already has the capability installed, the system throws an error like " C0000002 : RC_GENERAL_ERROR ". A similar result occurs if you attempt to install a particular firmware update more than once on one HSM. This is expected behavior.

Syntax

pki update

capability
firmware
login
logout
show

Parameter	Shortcut	Description
capability	**c**	Update the token capabilities. See "token pki update capability" on page 522.
firmware	**f**	Update the token firmware. See "token pki update firmware" on page 524.
login	**logi**	Login the PKI token Admin. See "token pki update login" on page 525.
logout	**logo**	Logout the PKI token Admin. See "token pki update logout" on page 526.
show	**s**	Show the available token updates. See "token pki update show" on page 527.

token pki update capability

Update PKI Token Capability, using a capability update package available on the Luna appliance (that is, a package that you have acquired from SafeNet, and transferred via scp, to the Luna appliance). Before you can use this command, you must:

a) acquire the secure package update file from SafeNet and send the file to the Luna SA (using scp or pscp)

b) open the file on the Luna SA with the lunash command "package update <filename> -authcode <authcode>"

An external Luna HSM can be USB-connected to a Luna SA appliance for:

- local backup/restore operations (Luna Backup HSM)
- PKI bundle operations (Luna G5 HSM)

Luna SA does not pass PED operations and data through to an externally connected Luna HSM from a Luna PED that is connected locally to the Luna SA.

If the external HSM is PED-authenticated, then the options for Luna PED connection are:

- local PED connection, directly to the affected HSM, when needed, or
- Remote PED connection, passed through the Luna SA

Note: Support for PKI Bundles with Remote PED begins at firmware version 6.10.1 in the external HSM.

Note: Support for locally connected Backup HSM with Remote PED,
begins at firmware version 6.10.1 in the external HSM.

Note: Use of Remote PED with an external device is made possible when you set up with the commands
hsm ped vector init -serial <serial#_of_external_HSM>
and
hsm ped connect -serial <serial#_of_external_HSM>
before using **token pki** or **token backup** commands.

A capability update or a firmware update is meant to be applied just one time to an HSM. If you attempt to re-apply a capability update to an HSM that already has the capability installed, the system throws an error like " C0000002 : RC_GENERAL_ERROR ". A similar result occurs if you attempt to install a particular firmware update more than once on one HSM. This is expected behavior.

Syntax

token pki update capability -serial <serialnum> **-capability** <capabilityname> [**-force**]

Parameter	Shortcut	Description
-capability	**-c**	Specifies the capability name.

Parameter	Shortcut	Description
-force	**-f**	Force the action without prompting.
-serial	**-l**	Specifies the token serial number.

Example

```
lunash:> token pki update capability -serial 777199-capability newcapability -f

Success
Capability newcapability added.

Command result : 0 (Success)
```

token pki update firmware

Update Token firmware, using a firmware update package available on the Luna appliance.
The package must be transferred to the Luna appliance by scp (individually or as a component of a system update), and you must login to the PKI token as Token Administrator or SO before the 'token pki update firmware' command is run. The command requires no package name.

The term "token" in this case refers to removable token-format HSMs connected via Luna DOCK 2 and USB (legacy equipment), or to a Luna G5 HSM, connected via USB.

Before you can use this command, you must:

- acquire the secure package update file from SafeNet and send the file to the Luna SA (using scp or pscp)
- open the file on the Luna SA with the lunash command package update <filename> -authcode <authcode>

A capability update or a firmware update is meant to be applied just one time to an HSM. If you attempt to re-apply a capability update to an HSM that already has the capability installed, the system throws an error like " C0000002 : RC_ GENERAL_ERROR ". A similar result occurs if you attempt to install a particular firmware update more than once on one HSM. This is expected behavior.

Syntax

token pki update firmware -serial <serialnum> [**-force**]

Parameter	Shortcut	Description
-force	**-f**	Force the action without prompting.
-serial	**-s**	Specifies the token serial number.

Example

```
lunash:> token pki update firmware -serial 475289


CAUTION:  This command updates the Token firmware.
          This process cannot be reversed.

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

        Partition #: 14 Name: Cryptoki User     Status: Passed

Update Result : 0 (Success)

Command Result : 0 (Success)
```

token pki update login

Logs in the PKI token admin - required before you can update the token firmware or token capabilities.

Syntax

token pki update login -serial <serialnum>

Parameter	Shortcut	Description
-serial	**-s**	Specifies the token serial number.

Example

```
lunash:> token pki update login -serial 777199

Luna PED operation required to login to Token  - use Security Officer (blue) PED Key.

'token pki login' successful.

Command result : 0 (Success)
```

token pki update logout

Log out the PKI token admin.

Syntax

token pki update logout -serial <serialnum>

Parameter	Shortcut	Description
-serial	**-s**	Specifies the token serial number.

Example

```
lunash:> token pki update logout -serial 777199

Command result : 0 (Success)
```

token pki update show

Show the available token capability updates.

Syntax

token pki update show

Example

```
lunash:> token pki update show
Capability Updates:

     There are no capability updates available.

Command Result : 0 (Success)
```

user

Access the user-level command. With the user commands, the HSM Appliance admin can create (add) additional named users and assign them roles of greater or lesser capability on the system. The admin can also lock (disable), unlock (enable) such accounts, set/reset their passwords, or delete them entirely, as needed.

Users without the "admin" role cannot execute any "user" command, even to change their own password. They should use the **my password set** command to change their own password.

The current implementation creates named users that are separate from the roles that those users can hold. The purpose is to allow administrators to assign any of the roles to multiple people, to allow logged tracking, by name, of the actions of each user in a given role (this was not possible previously when the role was the user, and only one of each could exist).

Syntax

user

add
delete
disable
enable
list
password
role

Parameter	Shortcut	Description
add	**a**	Add Luna Shell user. See "user add" on page 529.
delete	**de**	Delete a named Luna Shell user. See "user delete" on page 530.
disable	**di**	Disable a Luna Shell user (but the user still exists with role(s) assigned. See "user disable" on page 531
enable	**e**	Enable a locked Luna Shell user (with whatever roles are assigned to that user). See "user enable" on page 532.
list	**l**	List the Luna Shell user accounts. See "user list" on page 533.
password	**p**	Set User Password. See "user password" on page 534.
role	**ro**	Access the user role commands. See "user role" on page 536.

user add

Add a Luna shell user. Adds a new administrative lunash (command line) user. This command is available only to the ‘admin’ account. Administrative users' names can be a single character or as many as 128 characters, chosen from letters a-z, or A-Z, numbers 0-9, the dash, the dot, or the underscore. No spaces.

abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789-._

After the new, named administrative user is created, its default password is PASSWORD. The newly-created administrative user cannot do anything in the Luna Shell until the 'admin' assigns it a role with the **user role add** command.

Syntax

user add -username <clientname>

Parameter	Shortcut	Description
-username	**-u**	Specifies the user name of the user to create.

Example

```
lunash:> user add -u smith
Stopping sshd:                          [  OK  ]
Starting sshd:                          [  OK  ]
Command Result : 0 (Success)
```

user delete

Delete a role from a user. This command removes a Luna shell user. Works on any named users that you have created. Does not affect the permanent users 'admin', 'operator', and 'monitor'. A user must be logged out before you can delete that user.

Syntax

user delete -username <clientname>

Parameter	Shortcut	Description
-username	**-u**	Specifies the user name of the user being removed.

Example

```
lunash:>user list
Users      Roles        Status            RADIUS
admin      admin        enabled           no
bob        monitor      enabled           no
john       admin        enabled           no
monitor    monitor      enabled           no
operator   operator     enabled           no

Command Result : 0 (Success)

lunash:>user delete -userName john
Command Result : 0 (Success)

lunash:>user list
Users      Roles        Status            RADIUS
admin      admin        enabled           no
bob        monitor      enabled           no
monitor    monitor      enabled           no
operator   operator     enabled           no

Command Result : 0 (Success)
```

user disable

Disable a named Luna shell user.

Syntax

user disable -username <clientname>

Parameter	Shortcut	Description
-username	**-u**	Specifies the user name of the user to disable.

Example

```
lunash:>user  disable -username indigo
indigo was disabled successfully.

Command Result : 0 (Success)
```

user enable

Enable a locked Luna shell user.

Syntax

user enable -username <clientname>

Parameter	Shortcut	Description
-username	**-u**	Specifies the user name of the user being enabled.

Example

```
lunash:>user  enable -username indigo
indigo was enabled successfully.

Command Result : 0 (Success)
```

user list

List all of the Luna shell user accounts

Syntax

user list

Example

```
lunash:>user list
Users      Roles        Status            RADIUS
admin      admin        enabled           no
audit      audit        enabled           no
bob        monitor      enabled           no
john       admin        enabled           no
monitor    monitor      enabled           no
operator   operator     enabled           no

Command Result : 0 (Success)
```

user password

Sets/changes the specified user's password. This command allows the Luna appliance admin to change a user's password. The user with ‘admin’ role may set the password for any user. Non-admin users may set only their own password using the **my password set** command.

Syntax

user password [<clientname>]

Parameter	Shortcut	Description
<clientname>		This parameter is required when the admin user sets other user's passwords. It is optional for other users setting their own passwords. The user name option can be used by the admin user to specify any user that has been created. Users other than ‘admin’ may specify their own user name or leave the option blank. Users with the "admin" role can change their own passwords and other named users' passwords. The password is not input with the command - it is prompted after the command is issued, and the typed input is not displayed, for security reasons.

Example

```
lunash:> user password smith

Changing password for user smith.
You can now choose the new password.
A valid password should be a mix of upper and lower-case letters,
digits, and other characters. You should use a minimum 8-character-long
password with characters from at least 3 of these 4 classes.
An upper case letter that begins the password and a digit that
ends it do not count towards the number of character classes used.

Enter new password:
Re-type new password:
passwd: all authentication tokens updated successfully.


Command Result: 0 (Success)
```

user radiusadd

Add a RADIUS-authenticated user. This command adds a new administrative lunash (command line) user. This command is available only to the ‘admin’ account. Administrative users' names can be a single character or as many as 128 characters, chosen from letters a-z, or A-Z, numbers 0-9, the dash, the dot, or the underscore. No spaces.

abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789-._

After the new, named administrative user is created, it can authenticate via RADIUS only. The newly-created administrative user cannot do anything in the Luna Shell until the 'admin' assigns it a role with the **user role add** command.

Syntax

user radiusadd -username <clientname>

Parameter	Shortcut	Description
-username	**-u**	Specifies the user name of the user to add.

Example

```
lunash:> user radiusadd -u smith


Stopping sshd:             [  OK  ]
Starting sshd:             [  OK  ]


Command Result : 0 (Success)
```

user role

Access the user role commands to manage the roles associated with a user account.

Syntax

user role

add
clear
delete
list

Parameter	Shortcut	Description
add	**a**	Add a role to a Luna Shell user. See "user role add" on page 537.
clear	**c**	Clears user role assignments. See "user role clear" on page 538.
delete	**d**	Delete a role from a Luna Shell user. See "user role delete" on page 539.
list	**l**	List the possible role assignments. See "user role list" on page 540.

user role add

Add a role to a Luna shell administrative user. This command is available only to the original ‘admin’ account, and cannot be used to modify the "built-in" 'admin', 'user' or 'monitor' accounts (whose names are the same as their roles).

Syntax

user add -username <clientname> **-role** <rolename>

Parameter	Shortcut	Description
-username	**-u**	Specifies the the name of the user account to which the role is being added.
-role	**-r**	The user name of role being added to that user. The available roles, in descending order of capability are admin, operator and monitor.

Example

```
lunash:>user role add -role operator -username indigo

User indigo was successfully modified.

Command Result : 0 (Success)
```

user role clear

Clears all roles assigned to an account. This command is available only to the ‘admin account and cannot be used to modify the admin, monitor or operator accounts. If user has only one role, then the effect is the same as the user role delete command. This command is infrastructure for possible future functionality.

Syntax

user role clear -username <clientname>

Parameter	Shortcut	Description
-username	**-u**	Specifies the the name of the user account to which the role is being removed.

Example

```
lunash:>user role clear  -username indigo

User indigo was successfully modified.

Command Result : 0 (Success)
```

user role delete

Delete a role from a user account. This command is available only to the original ‘admin’ account and cannot be used to modify the admin, monitor or operator accounts.

Syntax

user role delete -role <clientname> **-username** <clientname>

Parameter	Shortcut	Description
-username	**-u**	Specifies the the name of the user account to which the role is being removed.
-role	**-r**	The user name of the role being removed from the user. The available roles, in descending order of capability are admin, operator and monitor.

Example

```
lunash:>user role delete -role operator -username indigo

User indigo was successfully modified.

Command Result : 0 (Success)
```

user role list

List the available user roles that can be assigned to a user. The "built-in" account called 'admin' has the full "admin" role, the "built-in" account called 'operator' has the "operator" role, and "built-in" account called 'monitor' has the "monitor" role. Those three roles can also be applied/assigned, as desired, to any new named account that the original, built-in 'admin' user cares to create.

Syntax

user role list

Example

```
lunash:>user role list

Available  Roles:
--------------------------------------------------
admin
audit
monitor
operator

Command Result : 0 (Success)
```