THALES

Thales Luna Network HSM 7

LUNASH COMMAND REFERENCE

Document Information

Last Updated	2025-08-27 10:32:35 GMT-05:00

Trademarks, Copyrights, and Third-Party Software

Copyright 2001-2025 Thales Group. All rights reserved. Thales and the Thales logo are trademarks and service marks of Thales and/or its subsidiaries and are registered in certain countries. All other trademarks and service marks, whether registered or not in specific countries, are the property of their respective owners.

Disclaimer

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

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

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

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

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

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

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

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

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

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

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

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

Regulatory Compliance

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

USA, FCC

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

Canada

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

Europe

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

CONTENTS

Preface: About the LunaSH Command Reference 17
- Customer Release Notes 17
- Audience 17
- Document Conventions 17
- Support Contacts 20

Chapter 1: Using LunaSH 21
- LunaSH Features 21
- Accessing LunaSH 21
- Seeing More Commands 22
- Exiting LunaSH 22

Chapter 2: LunaSH Commands 23
- LunaSH Command Summary 24
- audit 47
- audit changePwd 49
- audit config 51
- audit init 54
- audit log 56
- audit log clear 58
- audit log list 59
- audit log tail 61
- audit log tarlogs 63
- audit log untarlogs 64
- audit log verify 65
- audit login 68
- audit logout 70
- audit remotehost 71
- audit remotehost add 72
- audit remotehost cert 74
- audit remotehost cert delete 75
- audit remotehost cert deleteCA 76
- audit remotehost cert gen 77
- audit remotehost cert install 79
- audit remotehost cert installCA 80
- audit remotehost cert status 81
- audit remotehost clear 82
- audit remotehost delete 83
- audit remotehost list 84
- audit secret 85
- audit secret export 86

audit secret import 87
audit show 88
audit sync 90
client 91
client addCA 93
client assignPartition 94
client delete 95
client deleteCA 96
client dn 97
client dn assign 98
client dn delete 99
client dn show 100
client fingerprint 101
client hostip 102
client hostip map 103
client hostip show 104
client hostip unmap 105
client list 106
client listCAs 107
client register 108
client revokePartition 110
client show 111
client update 111
cluster 112
cluster admin 114
cluster admin disable 115
cluster admin enable 116
cluster admin status 117
cluster backup 117
cluster backup config 118
cluster backup disable 119
cluster backup enable 120
cluster backup run 120
cluster backup show 121
cluster client 122
cluster client assign 123
cluster client deregister 124
cluster client disable 125
cluster client enable 126
cluster client list 127
cluster client register 128
cluster client show 129
cluster client unassign 130
cluster config 131
cluster config set 133
cluster config show 135
cluster create 136

cluster delete 137
cluster disable 138
cluster enable 139
cluster group list 140
cluster join 141
cluster leave 142
cluster list 143
cluster member 144
cluster member authorize 145
cluster member config 146
cluster member delete 147
cluster member list 148
cluster member partition migration 149
cluster member partition migration begin 149
cluster member partition migration end 151
cluster member partition object 152
cluster member partition object assign 153
cluster member partition object list 154
cluster member show 156
cluster restore 158
cluster restore run 158
cluster restore show 160
cluster show 160
cluster status 162
hsm 163
hsm backup 166
hsm changePolicy 167
hsm changePw 169
hsm checkCertificates 171
hsm displayLicenses 172
hsm factoryReset 173
hsm firmware 176
hsm firmware rollback 177
hsm firmware show 179
hsm firmware upgrade 180
hsm fm 181
hsm fm delete 182
hsm fm load 183
hsm fm recover 183
hsm fm smfs activate 185
hsm fm status 186
hsm generateDAK 187
hsm information 188
hsm information monitor 189
hsm information reset 192
hsm information show 193
hsm init 194

hsm loadCustomerCert 197
hsm login 198
hsm logout 199
hsm ped 200
hsm ped connect 201
hsm ped deselect 205
hsm ped disconnect 206
hsm ped show 207
hsm ped select 209
hsm ped server 210
hsm ped server delete 211
hsm ped server list 212
hsm ped server register 213
hsm ped set 214
hsm ped timeout 215
hsm ped timeout set 216
hsm ped timeout show 218
hsm ped vector 219
hsm ped vector erase 220
hsm ped vector init 221
hsm qos metrics 222
hsm qos metrics reset 222
hsm qos metrics show 225
hsm restart 230
hsm restore 231
hsm selfTest 232
hsm setLegacyDomain 233
hsm show 234
hsm showPolicies 237
hsm stc 243
hsm stc activationtimeout 245
hsm stc activationTimeOut set 246
hsm stc activationTimeOut show 247
hsm stc cipher 248
hsm stc cipher disable 249
hsm stc cipher enable 250
hsm stc cipher show 251
hsm stc disable 252
hsm stc enable 253
hsm stc hmac 254
hsm stc hmac disable 255
hsm stc hmac enable 256
hsm stc hmac show 257
hsm stc identity 258
hsm stc identity create 259
hsm stc identity delete 260
hsm stc identity initialize 262

hsm stc identity partition 264
hsm stc identity partition deregister 265
hsm stc identity partition register 266
hsm stc identity show 267
hsm stc partition 268
hsm stc partition export 269
hsm stc partition show 270
hsm stc rekeythreshold 271
hsm stc rekeyThreshold set 272
hsm stc rekeyThreshold show 273
hsm stc status 274
hsm stm 275
hsm stm recover 276
hsm stm show 278
hsm stm transport 279
hsm supportInfo 281
hsm tamper 282
hsm tamper clear 283
hsm tamper show 284
hsm time 284
hsm time get 285
hsm time sync 286
hsm update 287
hsm update capability 288
hsm update show 290
hsm zeroize 291
keyring 292
keyring create 293
keyring delete 294
keyring disable 295
keyring enable 296
keyring list 297
keyring reset 298
keyring show 299
keyring unlock 300
my 302
my file 303
my file clear 304
my file delete 305
my file list 306
my password 307
my password expiry show 308
my password set 309
my public-key 310
my public-key add 311
my public-key clear 312
my public-key delete 313

my public-key list 314
network 315
network dns 316
network dns add 317
network dns add nameserver 318
network dns add searchdomain 320
network dns delete 322
network dns delete nameserver 323
network dns delete searchdomain 324
network hostname 325
network interface 327
network interface bonding 329
network interface bonding config 330
network interface bonding disable 338
network interface bonding enable 340
network interface bonding show 342
network interface delete 345
network interface dhcp 346
network interface slaac 349
network interface speed 351
network interface speed set-auto 352
network interface speed set 353
network interface speed show 354
network interface static 355
network ping 358
network route 359
network route add 360
network route clear 363
network route delete 364
network route metric 366
network route show 367
network show 369
ntls 377
ntls bind 378
ntls certificate 380
ntls certificate monitor 381
ntls certificate monitor disable 382
ntls certificate monitor enable 383
ntls certificate monitor show 384
ntls certificate monitor trap trigger 385
ntls certificate show 386
ntls information 388
ntls information reset 389
ntls information show 390
ntls ipcheck 392
ntls ipcheck disable 393
ntls ipcheck enable 394

ntls ipcheck show 395
ntls show 396
ntls tcp_keepalive 397
ntls tcp_keepalive set 398
ntls tcp_keepalive show 400
ntls threads 401
ntls threads set 402
ntls threads show 404
ntls timer 405
ntls timer set 406
ntls timer show 407
package 408
package deletefile 409
package erase 410
package list 411
package listfile 414
package update 415
package verify 417
partition 418
partition activate 420
partition backup 422
partition changePolicy 426
partition changePw 428
partition clear 430
partition create 432
partition createChallenge 434
partition deactivate 436
partition delete 437
partition init 438
partition init co 442
partition init cu 446
partition list 447
partition rename 448
partition resize 450
partition restore 452
partition show 455
partition showContents 457
partition showPolicies 459
partition stcidentity 462
partition stcIdentity export 463
partition stcIdentity show 464
service 465
service list 466
service restart 467
service start 469
service status 470
service stop 471

status 472
status cpu 474
status date 475
status disk 476
status handles 478
status interface 480
status mac 481
status mem 482
status memmap 483
status netstat 485
status ps 491
status sensors 493
status sysstat 496
status sysstat code 497
status sysstat show 499
status time 500
status zone 501
stc 502
stc activationtimeout 503
stc activationTimeOut set 504
stc activationTimeOut show 505
stc cipher 506
stc cipher disable 507
stc cipher enable 509
stc cipher show 510
stc hmac 511
stc hmac disable 512
stc hmac enable 513
stc hmac show 514
stc partition 515
stc partition export 516
stc partition show 517
stc rekeythreshold 518
stc rekeyThreshold set 519
stc rekeyThreshold show 520
sysconf 521
sysconf appliance 523
sysconf appliance hardReboot 524
sysconf appliance poweroff 525
sysconf appliance reboot 526
sysconf appliance rebootonpanic 528
sysconf appliance rebootOnPanic disable 529
sysconf appliance rebootOnPanic enable 530
sysconf appliance rebootOnPanic show 531
sysconf banner 532
sysconf banner add 533
sysconf banner clear 535

sysconf config 536
sysconf config backup 537
sysconf config clear 540
sysconf config delete 541
sysconf config export 542
sysconf config factoryReset 543
sysconf config import 547
sysconf config list 549
sysconf config restore 550
sysconf config show 553
sysconf ctc 555
sysconf ctc class 556
sysconf ctc class assign 557
sysconf ctc class define 558
sysconf ctc class delete 560
sysconf ctc class revoke 561
sysconf ctc class show 562
sysconf ctc client show 564
sysconf ctc disable 565
sysconf ctc enable 566
sysconf ctc measurement 567
sysconf ctc measurement disable 568
sysconf ctc measurement enable 569
sysconf ctc measurement show 570
sysconf ctc show 572
sysconf drift 573
sysconf drift init 574
sysconf drift reset 575
sysconf drift set 576
sysconf drift startmeasure 577
sysconf drift status 578
sysconf drift stopmeasure 579
sysconf fingerprint 580
sysconf fingerprint license 581
sysconf fingerprint ntls 582
sysconf fingerprint ssh 583
sysconf forceSOLogin 584
sysconf forceSOLogin disable 586
sysconf forceSOLogin enable 587
sysconf forceSOLogin show 589
sysconf installCert 590
sysconf license 592
sysconf license apply 593
sysconf license list 594
sysconf license revoke 595
sysconf ntp 596
sysconf ntp addserver 598

sysconf ntp autokeyauth 600
sysconf ntp autokeyAuth clear 601
sysconf ntp autokeyAuth generate 602
sysconf ntp autokeyAuth install 604
sysconf ntp autokeyAuth list 605
sysconf ntp autokeyAuth update 606
sysconf ntp deleteserver 607
sysconf ntp disable 608
sysconf ntp enable 609
sysconf ntp listservers 610
sysconf ntp log tail 611
sysconf ntp ntpdate 612
sysconf ntp show 613
sysconf ntp status 614
sysconf ntp ntsAuth cert 616
sysconf ntp ntsAuth cert add 616
sysconf ntp ntsAuth cert clear 617
sysconf ntp ntsAuth cert delete 617
sysconf ntp ntsAuth cert list 618
sysconf ntp symmetricauth 619
sysconf ntp symmetricauth key 620
sysconf ntp symmetricAuth key add 621
sysconf ntp symmetricAuth key clear 623
sysconf ntp symmetricAuth key delete 624
sysconf ntp symmetricAuth key list 625
sysconf ntp symmetricauth trustedkeys 626
sysconf ntp symmetricAuth trustedKeys add 627
sysconf ntp symmetricAuth trustedKeys clear 628
sysconf ntp symmetricAuth trustedKeys delete 629
sysconf ntp symmetricAuth trustedKeys list 630
sysconf radius 631
sysconf radius addServer 632
sysconf radius deleteServer 633
sysconf radius disable 634
sysconf radius enable 635
sysconf radius show 636
sysconf regenCert 637
sysconf reimage 641
sysconf reimage start 642
sysconf reimage tarlog 646
sysconf scp 646
sysconf scp disable 647
sysconf scp enable 647
sysconf scp show 649
sysconf snmp 650
sysconf snmp disable 651
sysconf snmp enable 652

sysconf snmp notification 653
sysconf snmp notification add 654
sysconf snmp notification clear 656
sysconf snmp notification delete 657
sysconf snmp notification list 658
sysconf snmp show 659
sysconf snmp trap 660
sysconf snmp trap clear 661
sysconf snmp trap delete 662
sysconf snmp trap disable 663
sysconf snmp trap enable 664
sysconf snmp trap set 665
sysconf snmp trap show 667
sysconf snmp trap test 668
sysconf snmp user 670
sysconf snmp user add 671
sysconf snmp user clear 673
sysconf snmp user delete 674
sysconf snmp user list 675
sysconf ssh 676
sysconf ssh ciphers 677
SSH Ciphers before Luna Network HSM 7.8.0 677
sysconf ssh ciphers reset 679
sysconf ssh ciphers set 681
sysconf ssh ciphers show 684
SSH Ciphers before Luna Network HSM 7.8.0 685
sysconf ssh client 688
sysconf ssh client add 690
sysconf ssh client clear 694
sysconf ssh client delete 697
sysconf ssh client list 700
sysconf ssh client showRejectedClients 701
sysconf ssh device 702
sysconf ssh ip 703
sysconf ssh password 704
sysconf ssh password disable 705
sysconf ssh password enable 706
sysconf ssh port 707
sysconf ssh publickey 708
sysconf ssh publickey disable 709
sysconf ssh publickey enable 710
sysconf ssh regenKeyPair 711
sysconf ssh show 712
sysconf time 713
sysconf timezone 714
sysconf timezone list 715
sysconf timezone set 716

sysconf timezone show 717
sysconf tls ciphers 718
sysconf tls ciphers reset 719
sysconf tls ciphers set 722
sysconf tls ciphers show 727
sysconf user 730
sysconf user login 731
sysconf user password 733
sysconf user password expire 734
sysconf user password history 736
sysconf user password length 738
sysconf user show 740
syslog 741
syslog cleanup 742
syslog export 743
syslog period 744
syslog rotate 745
syslog remotehost 746
syslog remotehost add 747
syslog remotehost cert 749
syslog remotehost cert delete 750
syslog remotehost cert deleteCA 751
syslog remotehost cert gen 752
syslog remotehost cert install 754
syslog remotehost cert installCA 755
syslog remotehost clear 756
syslog remotehost delete 757
syslog remotehost list 758
syslog rotations 759
syslog severity set 760
syslog show 761
syslog tail 762
syslog tarlogs 764
token backup 765
token backup factoryReset 767
token backup init 769
token backup list 771
token backup login 772
token backup logout 773
token backup partition 774
token backup partition delete 775
token backup partition list 777
token backup partition show 778
token backup show 781
token backup update 784
token backup update capability 785
token backup update firmware 787

token backup update show 789
user 790
user add 792
user delete 794
user disable 795
user enable 796
user list 797
user password 798
user radiusAdd 800
user role 801
user role add 802
user role clear 804
user role delete 805
user role import 806
user role list 808
webserver 809
webserver bind 810
webserver certificate 812
webserver certificate generate 813
webserver certificate show 815
webserver ciphers 817
webserver ciphers reset 818
webserver ciphers set 819
webserver ciphers show 821
webserver disable 823
webserver enable 824
webserver origin 825
webserver origin clear 826
webserver origin set 827
webserver origin show 828
webserver show 829

PREFACE: About the LunaSH Command Reference

This document describes how to access and use the LunaSH command line interface. It contains the following chapters:

> "Using LunaSH" on page 21

> "LunaSH Commands" on page 23

The preface includes the following information about this document:

> "Customer Release Notes" below

> "Audience" below

> "Document Conventions" below

> "Support Contacts" on page 20

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

Customer Release Notes

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

Audience

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

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

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

Document Conventions

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

Notes

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

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

Cautions

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

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

Warnings

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

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

Command syntax and typeface conventions

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

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

Support Contacts

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

Customer Support Portal

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

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

Telephone

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

 Copyright 2001-2025 Thales Group

CHAPTER 1: Using LunaSH

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

> "LunaSH Features" below
> "Accessing LunaSH" below
> "Seeing More Commands" on the next page
> "Exiting LunaSH" on the next page

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

LunaSH is the command interface for Luna Network HSM 7.

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 LunaSH 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 Network HSM 7 command shell (LunaSH). The commands are described in alphabetical order and provide:

> A brief description of the command function

> The users who are able to access the command

> The command syntax and parameter descriptions

> Usage examples

See "LunaSH Command Summary" on the next page for a list of all of the LunaSH commands and the user privileges required to access them.

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

Argument(s)	Shortcut	Description
audit	**a**	Perform HSM auditing tasks. These commands are available only to the Audit user. See "audit" on page 47.
client	**cli**	Manage HSM clients and their access to application partitions. See "client" on page 91.
cluster	**clu**	Manage clusters and cluster configuration on the appliance. See "cluster" on page 112.
hsm	**hs**	Manage the HSM on the appliance. See "hsm" on page 163.
keyring	**k**	Manage keyrings on a cluster. See "keyring" on page 292.
my	**m**	Manage the current user's files, passwords, and public keys. See "my" on page 302.
network	**ne**	View and configure network settings. See "network" on page 315.
ntls	**nt**	Manage the network trust link service (NTLS). See "ntls" on page 377.
package	**pac**	Manage secure package updates. See "package" on page 408.
partition	**par**	Manage partitions on the HSM. See "partition" on page 418.

Argument(s)	Shortcut	Description
service	**se**	View or manage services. See "service" on page 465.
status	**sta**	View the current system status. See "status" on page 472.
stc	**stc**	Configure and manage secure trusted channel (STC) network links between partitions and clients. See "stc" on page 502.
sysconf	**sysc**	Configure the appliance. See "sysconf" on page 521.
syslog	**sysl**	Manage the system logs. See "syslog" on page 741.
token backup	**t b**	Access backup commands. See "token backup" on page 765.
user	**u**	Manage users and their roles. See "user" on page 790.
webserver	**w**	Configure REST API services (if you have the upgrade installed). See "webserver" on page 809.

LunaSH Command Summary

This section provides a summary of all of the LunaSH commands, and which users are able to access the commands.

The standard administrative LunaSH user accounts on the Luna Network HSM 7 appliance are:

admin	All commands, except some specialized **audit** commands. This is the highest-level, full-access administrative role.
operator	Most commands, except some configuration commands for the system and the HSM.
monitor	Only commands that present information about the appliance or the HSM.
audit	Only commands governing HSM audit logging functions.

When you log into the appliance as one of the standard users (or a custom user assigned one of the standard roles), you are able to access the subset of commands listed in the relevant column below. You can also create custom user roles and specify the list of commands that user role is able to access (see Appliance Users and Roles).

Some commands are restricted to the HSM SO or Auditor; these will not work until you log in to the HSM using **hsm login** or **audit login**.

> **NOTE** The commands marked "configurable" do not require "hsm login" on page 198 by default. You can use "sysconf forceSOLogin enable" on page 587 to require "hsm login" on page 198 for these commands (see "sysconf forceSOLogin" on page 584).

Command	admin	operator	monitor	audit	hsm or audit login required
exit	✓	✓	✓	✓	
help	✓	✓	✓	✓	
audit	**admin**	**operator**	**monitor**	**audit**	**audit login required**
"audit changePwd" on page 49				✓	
"audit config" on page 51				✓	✓
"audit init" on page 54				✓	
"audit log clear" on page 58				✓	
"audit log list" on page 59				✓	
"audit log tail" on page 61				✓	
"audit log tarlogs" on page 63				✓	
"audit log untarlogs" on page 64				✓	
"audit log verify" on page 65				✓	
"audit login" on page 68				✓	
"audit logout" on page 70				✓	✓
"audit remotehost add" on page 72				✓	
"audit remotehost cert delete" on page 75				✓	
"audit remotehost cert gen" on page 77				✓	
"audit remotehost cert installCA" on page 80				✓	
"audit remotehost cert status" on page 81				✓	
"audit remotehost clear" on page 82				✓	
"audit remotehost delete" on page 83				✓	
"audit remotehost list" on page 84				✓	
"audit secret export" on page 86				✓	✓

Command	admin	operator	monitor	audit	hsm or audit login required
"audit secret import" on page 87				✓	✓
"audit show" on page 88				✓	
"audit sync" on page 90				✓	✓
client	**admin**	**operator**	**monitor**	**audit**	**hsm login required**
"client addCA" on page 93	✓	✓			
"client assignPartition" on page 94	✓	✓			configurable
"client delete" on page 95	✓	✓			configurable
"client deleteCA" on page 96	✓	✓			
"client dn assign" on page 98	✓	✓			
"client dn delete" on page 99	✓	✓			
"client dn show" on page 100	✓	✓	✓		
"client fingerprint" on page 101	✓	✓			
"client hostip map" on page 103	✓	✓			configurable
"client hostip show" on page 104	✓	✓	✓		
"client hostip unmap" on page 105	✓	✓			configurable
"client list" on page 106	✓	✓	✓		
"client listCAs" on page 107	✓	✓	✓		
"client register" on page 108	✓	✓			configurable
"client revokePartition" on page 110	✓	✓			configurable
"client show" on page 111	✓	✓	✓		
"client update" on page 111	✓	✓			configurable
cluster	**admin**	**operator**	**monitor**	**audit**	**hsm login required**
"cluster admin disable" on page 115	✓	✓			

Command	admin	operator	monitor	audit	hsm or audit login required
"cluster admin enable" on page 116	✓	✓			
"cluster admin status" on page 117	✓	✓			
"cluster backup config" on page 118	✓				
"cluster backup disable" on page 119	✓				
"cluster backup enable" on page 120	✓				
"cluster backup run" on page 120	✓				
"cluster backup show" on page 121	✓	✓	✓		
"cluster client deregister" on page 124	✓				
"cluster client disable" on page 125			✓		
"cluster client enable" on page 126			✓		
"cluster client list" on page 127	✓	✓	✓		
"cluster client register" on page 128	✓				
"cluster config" on page 131	✓	✓			
"cluster config set" on page 133	✓				
"cluster config show" on page 135	✓	✓	✓		
"cluster create" on page 136	✓				
"cluster delete" on page 137	✓				
"cluster disable" on page 138	✓				
"cluster enable" on page 139	✓				
"cluster group list" on page 140	✓	✓	✓		
"cluster join" on page 141	✓				
"cluster leave" on page 142	✓				
"cluster list" on page 143	✓	✓	✓		
"cluster member authorize" on page 145	✓				

Command	admin	operator	monitor	audit	hsm or audit login required
"cluster member config" on page 146	✓				
"cluster member delete" on page 147	✓				
"cluster member list" on page 148	✓	✓	✓		
cluster member partition list	✓	✓	✓		
cluster member partition select	✓	✓			
"cluster member partition migration begin" on page 149					
"cluster member partition migration end" on page 151					
"cluster member partition object assign" on page 153					
"cluster member partition object list" on page 154	✓	✓			
"cluster member show" on page 156	✓	✓	✓		
"cluster restore run" on page 158	✓				
"cluster restore show" on page 160	✓	✓	✓		
"cluster show" on page 160	✓	✓	✓		
"cluster status" on page 162	✓	✓	✓		
hsm	**admin**	**operator**	**monitor**	**audit**	**hsm login required**
"hsm backup" on page 166	✓	✓			
"hsm changePolicy" on page 167	✓				✓
"hsm changePw" on page 169	✓				
"hsm checkCertificates" on page 171	✓	✓	✓		
"hsm displayLicenses" on page 172	✓	✓	✓		
"hsm factoryReset" on page 173	✓				

Command	admin	operator	monitor	audit	hsm or audit login required
"hsm firmware rollback" on page 177	✓	✓			✓
"hsm firmware show" on page 179	✓	✓	✓		
"hsm firmware upgrade" on page 180	✓	✓			✓
"hsm fm delete" on page 182	✓				✓
"hsm fm load" on page 183	✓				✓
"hsm fm recover" on page 183	✓				✓
"hsm fm smfs activate" on page 185	✓				✓
"hsm fm status" on page 186	✓				
"hsm generateDAK" on page 187	✓	✓			
"hsm information monitor" on page 189	✓	✓	✓		
"hsm information reset" on page 192	✓	✓			
"hsm information show" on page 193	✓	✓	✓		
"hsm init" on page 194	✓				
"hsm loadCustomerCert" on page 197	✓	✓			
"hsm login" on page 198	✓	✓			
"hsm logout" on page 199	✓	✓			✓
"hsm ped connect" on page 201	✓	✓		✓	
"hsm ped deselect" on page 205	✓	✓		✓	
"hsm ped disconnect" on page 206	✓	✓		✓	
"hsm ped select" on page 209	✓	✓		✓	
"hsm ped server delete" on page 211	✓				
"hsm ped server list" on page 212	✓	✓	✓		
"hsm ped server register" on page 213	✓				
"hsm ped set" on page 214	✓				

Command	admin	operator	monitor	audit	hsm or audit login required
"hsm ped show" on page 207	✓	✓	✓	✓	
"hsm ped timeout set" on page 216	✓	✓		✓	
"hsm ped timeout show" on page 218	✓	✓	✓	✓	
"hsm ped vector erase" on page 220	✓				
"hsm ped vector init" on page 221	✓				✓
"hsm qos metrics reset" on page 222	✓				✓
"hsm qos metrics show" on page 225	✓				✓
"hsm restore" on page 231	✓	✓			✓
"hsm selfTest" on page 232	✓	✓	✓		
"hsm setLegacyDomain" on page 233	✓				
"hsm show" on page 234	✓	✓	✓		
"hsm showPolicies" on page 237	✓	✓	✓	✓	
"hsm stc activationTimeOut set" on page 246	✓	✓			
"hsm stc activationTimeOut show" on page 247	✓	✓			
"hsm stc cipher disable" on page 249	✓	✓			
"hsm stc cipher enable" on page 250	✓	✓			
"hsm stc cipher show" on page 251	✓	✓			
"hsm stc disable" on page 252	✓	✓			
"hsm stc enable" on page 253	✓	✓			
"hsm stc hmac disable" on page 255	✓	✓			
"hsm stc hmac enable" on page 256	✓	✓			
"hsm stc hmac show" on page 257	✓	✓			
"hsm stc identity create" on page 259	✓	✓			

Command	admin	operator	monitor	audit	hsm or audit login required
"hsm stc identity delete" on page 260	✓	✓			
"hsm stc identity initialize" on page 262	✓	✓			
"hsm stc identity partition deregister" on page 265	✓	✓			
"hsm stc identity partition register" on page 266	✓	✓			
"hsm stc identity show" on page 267	✓	✓			
"hsm stc partition export" on page 269	✓	✓			✓
"hsm stc partition show" on page 270	✓	✓			
"hsm stc rekeyThreshold set" on page 272	✓	✓			✓
"hsm stc rekeyThreshold show" on page 273	✓	✓			
"hsm stc status" on page 274	✓	✓	✓		
"hsm stm recover" on page 276	✓	✓			✓
"hsm stm show" on page 278	✓	✓	✓		
"hsm stm transport" on page 279	✓	✓			✓
"hsm supportInfo" on page 281	✓	✓	✓		
"hsm tamper clear" on page 283	✓				✓
"hsm time" on page 284	✓	✓			✓
"hsm time get" on page 285	✓	✓			✓
"hsm time sync" on page 286	✓	✓			✓
"hsm tamper show" on page 284	✓	✓	✓		
"hsm update capability" on page 288	✓	✓			
"hsm update show" on page 290	✓	✓			
"hsm zeroize" on page 291	✓				

Command	admin	operator	monitor	audit	hsm or audit login required
keyring	**admin**	**operator**	**monitor**	**audit**	**hsm login required**
"keyring create" on page 293	✓				
"keyring delete" on page 294	✓				
"keyring disable" on page 295	✓				
"keyring enable" on page 296	✓				
"keyring list" on page 297	✓	✓	✓		
"keyring reset" on page 298	✓				
"keyring show" on page 299	✓	✓	✓		
"keyring unlock" on page 300	✓				
my	**admin**	**operator**	**monitor**	**audit**	**hsm login required**
"my file clear" on page 304	✓	✓	✓	✓	
"my file delete" on page 305	✓	✓	✓	✓	
"my file list" on page 306	✓	✓	✓	✓	
"my password expiry show" on page 308	✓	✓	✓	✓	
"my password set" on page 309	✓	✓	✓	✓	
"my public-key add" on page 311	✓	✓	✓	✓	
"my public-key clear" on page 312	✓	✓	✓	✓	
"my public-key delete" on page 313	✓	✓	✓	✓	
"my public-key list" on page 314	✓	✓	✓	✓	
network	**admin**	**operator**	**monitor**	**audit**	**hsm login required**
"network dns add nameserver" on page 318	✓	✓			
"network dns add searchdomain" on page 320	✓	✓			

Command	admin	operator	monitor	audit	hsm or audit login required
"network dns delete nameserver" on page 323	✓	✓			
"network dns delete searchdomain" on page 324	✓	✓			
"network hostname" on page 325	✓	✓			
"network interface bonding config" on page 330	✓	✓			
"network interface bonding disable" on page 338	✓	✓			
"network interface bonding enable" on page 340	✓	✓			
"network interface bonding show" on page 342	✓	✓	✓		
" network interface delete" on page 345	✓	✓			
"network interface dhcp" on page 346	✓	✓			
"network interface slaac" on page 349	✓	✓			
"network interface speed set-auto" on page 352	✓	✓			
"network interface speed set" on page 353	✓	✓			
"network interface speed show" on page 354	✓	✓	✓		
"network interface static" on page 355	✓	✓			
"network ping" on page 358	✓	✓	✓	✓	
"network route add" on page 360	✓	✓			
"network route clear" on page 363	✓	✓			
"network route delete" on page 364	✓	✓			
"network route show" on page 367	✓	✓	✓		

Command	admin	operator	monitor	audit	hsm or audit login required
"network show" on page 369	✓	✓	✓	✓	
ntls	**admin**	**operator**	**monitor**	**audit**	**hsm login required**
"ntls bind" on page 378	✓	✓			configurable
"ntls certificate monitor disable" on page 382	✓	✓			configurable
"ntls certificate monitor enable" on page 383	✓	✓			configurable
"ntls certificate monitor show" on page 384	✓	✓	✓		
"ntls certificate monitor trap trigger" on page 385	✓	✓			configurable
"ntls certificate show" on page 386	✓	✓	✓		
"ntls information reset" on page 389	✓	✓			configurable
"ntls information show" on page 390	✓	✓	✓		
"ntls ipcheck disable" on page 393	✓	✓			configurable
"ntls ipcheck enable" on page 394	✓	✓			configurable
"ntls ipcheck show" on page 395	✓	✓	✓		
"ntls show" on page 396	✓	✓	✓		
"ntls tcp_keepalive set" on page 398	✓	✓			configurable
"ntls tcp_keepalive show" on page 400	✓	✓	✓		
"ntls threads set" on page 402	✓	✓			configurable
"ntls threads show" on page 404	✓	✓	✓		
"ntls timer set" on page 406	✓	✓			configurable
"ntls timer show" on page 407	✓	✓	✓		
package	**admin**	**operator**	**monitor**	**audit**	**hsm login required**

Command	admin	operator	monitor	audit	hsm or audit login required
"package deletefile" on page 409	✓	✓			
"package erase" on page 410	✓	✓			✓
"package list" on page 411	✓	✓	✓		
"package listfile" on page 414	✓	✓	✓		
"package update" on page 415	✓	✓			✓
"package verify" on page 417	✓	✓			✓
partition	**admin**	**operator**	**monitor**	**audit**	**hsm login required**
"partition activate" on page 420	✓	✓			
"partition backup" on page 422	✓	✓			
"partition changePolicy" on page 426	✓	✓			
"partition changePw" on page 428	✓	✓			
"partition clear" on page 430	✓	✓			
"partition create" on page 432	✓	✓			✓
"partition createChallenge" on page 434	✓	✓			
"partition deactivate" on page 436	✓	✓			
"partition delete" on page 437	✓	✓			✓
"partition init" on page 438	✓	✓			✓
"partition init co" on page 442	✓	✓			✓
"partition init cu" on page 446	✓	✓			
"partition list" on page 447	✓	✓	✓		
"partition rename" on page 448	✓	✓			✓
"partition resize" on page 450	✓	✓			✓
"partition restore" on page 452	✓	✓			

Command	admin	operator	monitor	audit	hsm or audit login required
"partition show" on page 455	✓	✓	✓		
"partition showContents" on page 457	✓	✓			
"partition showPolicies" on page 459	✓	✓			
"partition stcIdentity export" on page 463	✓	✓			✓
"partition stcIdentity show" on page 464	✓	✓			
service	**admin**	**operator**	**monitor**	**audit**	**hsm login required**
"service list" on page 466	✓	✓	✓		
"service restart" on page 467	✓	✓			
"service start" on page 469	✓	✓			
"service status" on page 470	✓	✓	✓		
"service stop" on page 471	✓	✓			
status	**admin**	**operator**	**monitor**	**audit**	**hsm login required**
"status cpu" on page 474	✓	✓	✓		
"status date" on page 475	✓	✓	✓		
"status disk" on page 476	✓	✓	✓		
"status handles" on page 478	✓	✓	✓		
"status interface" on page 480	✓	✓	✓		
"status mac" on page 481	✓	✓	✓		
"status mem" on page 482	✓	✓	✓		
"status memmap" on page 483	✓	✓	✓		
"status netstat" on page 485	✓	✓	✓		
"status ps" on page 491	✓	✓	✓		
"status sensors" on page 493	✓	✓	✓		

Command	admin	operator	monitor	audit	hsm or audit login required
"status sysstat code" on page 497	✓	✓	✓		
"status sysstat show" on page 499	✓	✓	✓		
"status time" on page 500	✓	✓	✓		
"status zone" on page 501	✓	✓	✓		
stc	**admin**	**operator**	**monitor**	**audit**	**hsm login required**
"stc activationTimeOut set" on page 504	✓	✓			✓
"stc activationTimeOut show" on page 505	✓	✓	✓		✓
"stc cipher disable" on page 507	✓	✓			✓
"stc cipher enable" on page 509	✓	✓			✓
"stc cipher show" on page 510	✓	✓	✓		✓
"stc hmac disable" on page 512	✓	✓			✓
"stc hmac enable" on page 513	✓	✓			✓
"stc hmac show" on page 514	✓	✓	✓		✓
"stc partition export" on page 516	✓	✓			✓
"stc partition show" on page 517	✓	✓	✓		✓
"stc rekeyThreshold set" on page 519	✓	✓			✓
"stc rekeyThreshold show" on page 520	✓	✓	✓		✓
sysconf	**admin**	**operator**	**monitor**	**audit**	**hsm login required**
"sysconf appliance hardReboot" on page 524	✓				
"sysconf appliance poweroff" on page 525	✓	✓			
"sysconf appliance reboot" on page 526	✓	✓			

Command	admin	operator	monitor	audit	hsm or audit login required
"sysconf appliance rebootOnPanic disable" on page 529	✓	✓			
"sysconf appliance rebootOnPanic enable" on page 530	✓	✓			
"sysconf appliance rebootOnPanic show" on page 531	✓	✓	✓		
"sysconf banner add" on page 533	✓				
"sysconf banner clear" on page 535	✓				
"sysconf config backup" on page 537	✓				
"sysconf config clear" on page 540	✓				
"sysconf config delete" on page 541	✓				
"sysconf config export" on page 542	✓				
"sysconf config factoryReset" on page 543	✓				configurable
"sysconf config import" on page 547	✓				
"sysconf config list" on page 549	✓	✓	✓		
"sysconf config restore" on page 550	✓				
"sysconf config show" on page 553	✓	✓	✓		
"sysconf ctc class assign" on page 557	✓	✓			
"sysconf ctc class define" on page 558	✓	✓			
"sysconf ctc class delete" on page 560	✓	✓			
"sysconf ctc class revoke" on page 561	✓	✓			
"sysconf ctc class show" on page 562	✓	✓			
"sysconf ctc client show" on page 564	✓	✓			
"sysconf ctc disable" on page 565	✓	✓			
"sysconf ctc enable" on page 566	✓	✓			

Command	admin	operator	monitor	audit	hsm or audit login required
"sysconf ctc measurement disable" on page 568	✓	✓			
"sysconf ctc measurement enable" on page 569	✓	✓			
"sysconf ctc measurement show" on page 570	✓	✓			
"sysconf ctc show" on page 572	✓	✓			
"sysconf drift init" on page 574	✓	✓			
"sysconf drift reset" on page 575	✓	✓			
"sysconf drift set" on page 576	✓	✓			
"sysconf drift startmeasure" on page 577	✓	✓			
"sysconf drift status" on page 578	✓	✓	✓		
"sysconf drift stopmeasure" on page 579	✓	✓			
"sysconf fingerprint license" on page 581	✓	✓	✓		
"sysconf fingerprint ntls" on page 582	✓	✓	✓		
"sysconf fingerprint ssh" on page 583	✓	✓	✓		
"sysconf forceSOLogin disable" on page 586	✓				✓
"sysconf forceSOLogin enable" on page 587	✓				✓
"sysconf forceSOLogin show" on page 589	✓				
"sysconf installCert" on page 590	✓				
"sysconf license apply" on page 593	✓				✓
"sysconf license list" on page 594	✓	✓	✓		
"sysconf license revoke" on page 595	✓				✓
"sysconf ntp addserver" on page 598	✓	✓			

Command	admin	operator	monitor	audit	hsm or audit login required
"sysconf ntp autokeyAuth clear" on page 601	✓	✓			
"sysconf ntp autokeyAuth generate" on page 602	✓	✓			
"sysconf ntp autokeyAuth install" on page 604	✓	✓			
"sysconf ntp autokeyAuth list" on page 605	✓	✓			
"sysconf ntp autokeyAuth update" on page 606	✓	✓			
"sysconf ntp deleteserver" on page 607	✓	✓			
"sysconf ntp disable" on page 608	✓	✓			
"sysconf ntp enable" on page 609	✓	✓			
"sysconf ntp listservers" on page 610	✓	✓	✓		
"sysconf ntp log tail" on page 611	✓	✓			
"sysconf ntp ntpdate" on page 612	✓	✓			
"sysconf ntp show" on page 613	✓	✓	✓		
"sysconf ntp status" on page 614	✓	✓	✓		
"sysconf ntp symmetricAuth key add" on page 621	✓	✓			
"sysconf ntp symmetricAuth key clear" on page 623	✓	✓			
"sysconf ntp symmetricAuth key delete" on page 624	✓	✓			
"sysconf ntp symmetricAuth key list" on page 625	✓	✓	✓		
"sysconf ntp symmetricAuth trustedKeys add" on page 627	✓	✓			

Command	admin	operator	monitor	audit	hsm or audit login required
"sysconf ntp symmetricAuth trustedKeys clear" on page 628	✓	✓			
"sysconf ntp symmetricAuth trustedKeys delete" on page 629	✓	✓			
"sysconf ntp symmetricAuth trustedKeys list" on page 630	✓	✓	✓		
"sysconf radius addServer" on page 632	✓				
"sysconf radius deleteServer" on page 633	✓				
"sysconf radius disable" on page 634	✓				
"sysconf radius enable" on page 635	✓				
"sysconf radius show" on page 636	✓				
"sysconf regenCert" on page 637	✓				configurable
"sysconf reimage start" on page 642	✓				✓
"sysconf reimage tarlog" on page 646	✓				
"sysconf scp disable" on page 647	✓	✓			
"sysconf scp enable" on page 647	✓	✓			
"sysconf scp show" on page 649	✓	✓	✓		
"sysconf snmp disable" on page 651	✓	✓			
"sysconf snmp enable" on page 652	✓	✓			
"sysconf snmp notification add" on page 654	✓	✓			
"sysconf snmp notification clear" on page 656	✓	✓			
"sysconf snmp notification delete" on page 657	✓	✓			
"sysconf snmp notification list" on page 658	✓	✓	✓		

Command	admin	operator	monitor	audit	hsm or audit login required
"sysconf snmp show" on page 659	✓	✓	✓		
"sysconf snmp trap clear" on page 661	✓	✓			
"sysconf snmp trap disable" on page 663	✓	✓			
"sysconf snmp trap enable" on page 664	✓	✓			
"sysconf snmp trap set" on page 665	✓	✓			
"sysconf snmp trap show" on page 667	✓	✓	✓		
"sysconf snmp trap test" on page 668	✓	✓			
"sysconf snmp user add" on page 671	✓	✓			
"sysconf snmp user clear" on page 673	✓	✓			
"sysconf snmp user delete" on page 674	✓	✓			
"sysconf snmp user list" on page 675	✓	✓	✓		
"sysconf ssh client add" on page 690	✓	✓			
"sysconf ssh client clear" on page 694	✓	✓			
"sysconf ssh client delete" on page 697	✓	✓			
"sysconf ssh client list" on page 700	✓	✓	✓		
"sysconf ssh client showRejectedClients" on page 701	✓	✓			
"sysconf ssh ciphers reset" on page 679	✓	✓			
"sysconf ssh ciphers set" on page 681	✓	✓			
"sysconf ssh ciphers show" on page 684	✓	✓	✓		
"sysconf ssh device" on page 702	✓	✓			
"sysconf ssh ip" on page 703	✓	✓			
"sysconf ssh password disable" on page 705	✓	✓			

Command	admin	operator	monitor	audit	hsm or audit login required
"sysconf ssh password enable" on page 706	✓	✓			
"sysconf ssh port" on page 707	✓				
"sysconf ssh publickey disable" on page 709	✓	✓			
"sysconf ssh publickey enable" on page 710	✓	✓			
"sysconf ssh regenKeyPair" on page 711	✓	✓			
"sysconf ssh show" on page 712	✓	✓	✓		
"sysconf time" on page 713	✓	✓			
"sysconf timezone list" on page 715	✓	✓	✓		
"sysconf timezone set" on page 716	✓	✓			
"sysconf timezone show" on page 717	✓	✓	✓		
"sysconf tls ciphers reset" on page 719	✓				
"sysconf tls ciphers set" on page 722	✓				
"sysconf tls ciphers show" on page 727	✓	✓	✓		
syslog	**admin**	**operator**	**monitor**	**audit**	**hsm login required**
"syslog cleanup" on page 742	✓				
"syslog export" on page 743	✓	✓			
"syslog period" on page 744	✓	✓			
"syslog remotehost add" on page 747	✓	✓			
"syslog remotehost cert" on page 749	✓	✓			
"syslog remotehost cert delete" on page 750	✓	✓			
"syslog remotehost cert deleteCA" on page 751	✓	✓			

Command	admin	operator	monitor	audit	hsm or audit login required
"syslog remotehost cert gen" on page 752	✓	✓			
"syslog remotehost cert install" on page 754	✓	✓			
"syslog remotehost cert installCA" on page 755	✓	✓			
"syslog remotehost clear" on page 756	✓	✓			
"syslog remotehost delete" on page 757	✓	✓			
"syslog remotehost list" on page 758	✓	✓			
"syslog rotate" on page 745	✓	✓			
"syslog rotations" on page 759	✓	✓			
"syslog severity set" on page 760	✓				
"syslog show" on page 761	✓	✓	✓		
"syslog tail" on page 762	✓	✓	✓		
"syslog tarlogs" on page 764	✓	✓	✓		
token	**admin**	**operator**	**monitor**	**audit**	**hsm login required**
"token backup factoryReset" on page 767	✓	✓			
"token backup init" on page 769	✓	✓			
"token backup list" on page 771	✓	✓	✓		
"token backup login" on page 772	✓	✓			
"token backup logout" on page 773	✓	✓			
"token backup partition delete" on page 775	✓	✓			
"token backup partition list" on page 777	✓	✓	✓		

Command	admin	operator	monitor	audit	hsm or audit login required
"token backup partition show" on page 778	✓	✓	✓		
"token backup show" on page 781	✓	✓	✓		
"token backup update capability" on page 785	✓	✓			
"token backup update firmware" on page 787	✓	✓			
"token backup update show" on page 789	✓	✓	✓		
user	**admin**	**operator**	**monitor**	**audit**	**hsm login required**
"user add" on page 792	✓				
"user delete" on page 794	✓				
"user disable" on page 795	✓				
"user enable" on page 796	✓				
"user list" on page 797	✓				
"user password" on page 798	✓				
"user radiusAdd" on page 800	✓				
"user role add" on page 802	✓				
"user role clear" on page 804	✓				
"user role delete" on page 805	✓				
"user role import" on page 806	✓				
"user role list" on page 808	✓				
webserver	**admin**	**operator**	**monitor**	**audit**	**hsm login required**
"webserver bind" on page 810	✓				
"webserver certificate generate" on page 813	✓				

Command	admin	operator	monitor	audit	hsm or audit login required
"webserver certificate show" on page 815	✓				
"webserver ciphers reset" on page 818	✓				
"webserver ciphers set" on page 819	✓				
"webserver ciphers show" on page 821	✓				
"webserver disable" on page 823	✓				
"webserver enable" on page 824	✓				
"webserver origin clear" on page 826	✓				
"webserver origin set" on page 827	✓				
"webserver origin show" on page 828	✓	✓	✓		
"webserver show" on page 829	✓				

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.
>
> Audit log and syslog entries are timestamped in UTC format.

> **TIP** ***Performance and Audit Logging***
>
> Secure Audit Logging consumes HSM resources, so consider minimizing the intensity of logging that you invoke.
>
> For example, when choosing asymmetric key usage, you have the option to specify event values to record with **-value asymmetric** or **first**.
> When choosing symmetric key usage logging you can opt for the corresponding **symmetric** and **symfirst**.
>
> An HMAC is generated for each log, so "**first**" and "**symfirst**" record the first use of a key (asymmetric sig/ver or symmetric enc/dec respectively) and are much more sparing of HSM cycles, and therefore preferred to configuring for a log entry at every individual use of a given key -- unless that level of detailed logging is mandated.

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 234 > 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 200.
my	Provides a set of commands equivalent to those provided to other non-admin users. See "my" on page 302
network	Provides only the **show** and **ping** commands. See "network" on page 315.

Syntax

audit

- **changepwd**
- **config**
- **init**
- **log**
- **login**
- **logout**
- **remotehost**

secret
show
sync

Argument(s)	Shortcut	Description
changepwd	**ch**	Changes the audit user password or PED key. See "audit changePwd" on the next page.
config	**co**	Set the audit parameters. See "audit config" on page 51.
init	**i**	Initialize the audit role. See "audit init" on page 54.
log	**log**	Access commands that allow you to manage audit log files. See "audit log" on page 56.
login	**logi**	Login as the audit user. See "audit login" on page 68.
logout	**logo**	Logout the audit user. See "audit logout" on page 70.
remotehost	**r**	Configure audit logging remote hosts. See "audit remotehost" on page 71.
secret	**se**	Export or import the audit logging secret. See "audit secret" on page 85.
show	**sh**	Display the current audit logging configuration. See "audit show" on page 88.
sync	**sy**	Synchronizes the HSM time to the host time. See "audit sync" on page 90.

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 Network HSM 7 with multifactor quorum authentication.

[For the appliance-level audit role (to make SSH or serial connection to lunash command line, before you can access the HSM) see "my password set" on page 309.]

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

> Regular credential rotation as part of your organization's security policy

> Compromise of a role or secret due to loss or theft of a PED key

> Personnel changes in your organization or changes to individual security clearances

> Changes to your security scheme (implementing/revoking M of N, PINs, or shared secrets)

User Privileges

Only specialized Audit users can access audit commands.

Syntax

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

Argument(s)	Shortcut	Description
-newpw <password>	**-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 <password>	**-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 <serialnum>	**-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 USB HSM 7).

Example

```
lunash:>audit changePwd

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

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

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


Command Result : 0 (Success)
```

audit config

Set the configuration parameters for audit logging.

The callback service (**cbs**) on the appliance creates the audit log files when it reads the audit records from the HSM card. This happens as needed and as configured, unless the service stops or the appliance disk becomes full.

> **NOTE** Audit log and syslog entries are timestamped in UTC format.

> **TIP** ***Performance and Audit Logging***
>
> Secure Audit Logging consumes HSM resources, so consider minimizing the intensity of logging that you invoke.
>
> For example, when choosing asymmetric key usage, you have the option to specify event values to record with **-value asymmetric** or **first**.
> When choosing symmetric key usage logging you can opt for the corresponding **symmetric** and **symfirst**.
>
> An HMAC is generated for each log, so "**first**" and "**symfirst**" record the first use of a key (asymmetric sig/ver or symmetric enc/dec respectively) and are much more sparing of HSM cycles, and therefore preferred to configuring for a log entry at every individual use of a given key -- unless that level of detailed logging is mandated.

User Privileges

Only specialized Audit users can access audit commands.

Syntax

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

Argument(s)	Shortcut	Description
-parameter <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 <serialnum>	**-s**	Reserved for future use. Specifies the serial number of the HSM. This option allows the system to distinguish between two connected HSMs.

Argument(s)	Shortcut	Description
-value <value>	**-v**	**Event Values** 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 [**n**] 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) > **asymmetri[c]**: asymmetric key usage (sig/ver) > **fi[r]st**: first asymmetric key usage only (sig/ver) > **s[y]mmetric**: symmetric key usage (enc/dec) > **symf[i]rst**: first symmetric key usage only (enc/dec) > **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 **Rotation Values** If **-parameter** is set to **rotation**, this specifies the log rotation interval. **Valid values** The value enclosed in parentheses [] indicates a shortcut: > **[h]ourly** > **[d]aily** > **[w]eekly** > **[m]onthly** > **[n]ever**

Example

The following table provides some command usage examples:

Argument(s)	Description
`lunash:> audit config -parameter event -value all`	Log everything.

Argument(s)	Description
`lunash:> audit config -parameter event -value none`	Log nothing.
`lunash:> audit config -parameter event -value failure`	Log all command failures.
`lunash:> audit config -parameter event -value failure,success,asymmetric`	Log all key usage requests, both success and failure.
`lunash:> audit config -parameter rotation -value daily`	Rotate the log daily.

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.
>
> Audit log and syslog entries are timestamped in UTC format.

User Privileges

Only specialized Audit users can access audit commands.

Syntax

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

Argument(s)	Shortcut	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 multifactor quorum-authenticated HSMs.
-domain <auditdomain>	**-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 multifactor quorum-authenticated HSMs.
-force	**-f**	Force the action without prompting.
-password <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.

Argument(s)	Shortcut	Description
-serial <serialnum>	**-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 USB HSM 7).

Example

```
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 multifactor quorum-authenticated HSMs, after you type "proceed" you are referred to the Luna 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.

> **NOTE** Audit log and syslog entries are timestamped in UTC format.

Syntax

audit log

clear
list
tail
tarlogs
untarlogs
verify

Argument(s)	Shortcut	Description
clear	**c**	Clears all of the audit logs from an HSM. See "audit log clear" on page 58.
list	**l**	Lists all of the audit logs on an HSM. See "audit log list" on page 59.
tail	**tai**	Displays the most recent entries in an audit log. See "audit log tail" on page 61.
tarlogs	**tar**	Archives an audit log. See "audit log tarlogs" on page 63.
untarlogs	**u**	Unarchives a previously archived audit log. See "audit log untarlogs" on page 64.
verify	**v**	Verifies a set of records within an audit log. See "audit log verify" on page 65.

TIP Depending on how busy the HSM is, and the level of audit logging and the rotation interval you have configured (with "audit config" on page 51), audit logs might take a long time to fill, or might fill up very quickly. We recommend that you sftp the logs out of the Luna Network HSM 7 appliance and clear logs every day, to avoid filling the disk. You can do this manually, but a simple example of automating the process with a script on an external computer might look similar to this bash script:

```
host_list="" # list of hosts
for host in host_list
 do
 ssh audit@host "audit log tarlogs" || exit
 sftp audit@host:audit-*.tgz . || exit
 ssh audit@host "audit log clear -force" || exit
 ssh audit@host "service restart cbs" || exit
 …
 …
 done
```

Naturally, you should modify and test any such solution before you deploy it in an operational environment. The take-away message is to be aware of the extent and rapidity of your audit logging, and to ensure that the resulting files are properly maintained.

audit log clear

Clear all of the audit log files from an HSM. The callback service (CBS), that gets log entries from the HSM card to the appliance file system, is stopped prior to clearing logs, so there is no interference with the current log entries being exported to file. CBS then resumes prior to the next configured log-entry transfer.

> **NOTE** Audit log and syslog entries are timestamped in UTC format.

User Privileges

Only specialized Audit users can access audit commands.

Syntax

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

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

   *** WARNING ***

        All audit logs for this HSM will be destroyed!!!

        Are you sure you wish to continue?

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


Command Result : 0 (Success)
```

audit log list

Display a list of the audit log files.

User Privileges

Only specialized Audit users can access audit commands.

> **NOTE** Audit log and syslog entries are timestamped in UTC format.

> **TIP** The **audit show** command can show "`HSM is currently storing 0 log records`", while the **audit log list** command shows some number of log files. This is normal and means that the **c**all**b**ack **s**ervice (cbs), running on the HSM appliance is storing audit log records from the cryptographic module into the HSM appliance file system.
>
> The cbs is temporarily stopped when an "audit log tarlogs" on page 63 action is being performed, then cbs resumes.
>
> If a number other than zero records persists and grows on the cryptographic module, then either the cbs is not running, or something else is preventing cbs from writing to the file system.
>
> Verify with "service status" on page 470 that cbs is running. If cbs is running, check that /var/audit usage is less than 200GB with "status disk" on page 476.

Syntax

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

Argument(s)	Shortcut	Description
-serial <serialnum>	**-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

Logs that are in progress

116280 Feb 27 17:03 hsm_66331_0000000a.log

Logs that are ready for archive:

1624728 Feb 27 17:00 hsm_66331_00000009.log
2224824 Feb 27 16:00 hsm_66331_00000008.log
1902432 Feb 27 15:00 hsm_66331_00000007.log
1923864 Feb 27 14:00 hsm_66331_00000006.log
1910184 Feb 27 13:00 hsm_66331_00000005.log
1925232 Feb 27 12:00 hsm_66331_00000004.log
1937088 Feb 27 11:00 hsm_66331_00000003.log
```

```
 445968 Feb 27 10:00 hsm_66331_00000002.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.

User Privileges

Only specialized Audit users can access audit commands.

Syntax

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

Argument(s)	Shortcut	Description
-entries <logentries>	**-e**	Specifies the number of log entries to display.
-file <filename>	**-f**	Specifies the name of the log file to view.
-search <string>	**-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 <serialnum>	**-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

Last 10 entries

```
lunash:>audit log tail -file hsm_66331_00000009.log -entries 10

301176,17/02/28 02:59:56,S/N 154438865286 session 2 Access 2147483651:3 operation LUNA_CLOSE_
SESSION returned RC_OK(0x00000000) session handle 2
301177,17/02/28 02:59:56,S/N 154438865286 session 2 Access 2147483651:3 operation LUNA_OPEN_
SESSION returned RC_OK(0x00000000) session handle 2
301178,17/02/28 02:59:56,S/N 154438865286 session 2 Access 2147483651:3 operation LUNA_CLOSE_
SESSION returned RC_OK(0x00000000) session handle 2
301179,17/02/28 02:59:56,S/N 154438865286 session 2 Access 2147483651:3 operation LUNA_OPEN_
SESSION returned RC_OK(0x00000000) session handle 2
301180,17/02/28 02:59:56,S/N 154438865286 session 2 Access 2147483651:3 operation LUNA_CLOSE_
SESSION returned RC_OK(0x00000000) session handle 2
301181,17/02/28 02:59:56,S/N 154438865286 session 2 Access 2147483651:3 operation LUNA_OPEN_
SESSION returned RC_OK(0x00000000) session handle 2
301182,17/02/28 02:59:56,S/N 154438865286 session 2 Access 2147483651:3 operation LUNA_CLOSE_
SESSION returned RC_OK(0x00000000) session handle 2
301183,17/02/28 02:59:56,S/N 154438865286 session 2 Access 2147483651:3 operation LUNA_OPEN_
SESSION returned RC_OK(0x00000000) session handle 2
301184,17/02/28 02:59:56,S/N 154438865286 session 2 Access 2147483651:3 operation LUNA_CLOSE_
SESSION returned RC_OK(0x00000000) session handle 2
```

```
0, ,0000000000000000000000000000000000000000000000000000000000000000000000000000000000000000

Command Result : 0 (Success)
```

Entries within the last 10 containing "OPEN_SESSION"

```
lunash:>audit log tail -file hsm_66331_00000009.log -entries 10 -search OPEN_SESSION

301177,17/02/28 02:59:56,S/N 154438865286 session 2 Access 2147483651:3 operation LUNA_OPEN_
SESSION returned RC_OK(0x00000000) session handle 2
301179,17/02/28 02:59:56,S/N 154438865286 session 2 Access 2147483651:3 operation LUNA_OPEN_
SESSION returned RC_OK(0x00000000) session handle 2
301181,17/02/28 02:59:56,S/N 154438865286 session 2 Access 2147483651:3 operation LUNA_OPEN_
SESSION returned RC_OK(0x00000000) session handle 2
301183,17/02/28 02:59:56,S/N 154438865286 session 2 Access 2147483651:3 operation LUNA_OPEN_
SESSION returned RC_OK(0x00000000) session handle 2

Command Result : 0 (Success)
```

Example

audit log tarlogs

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

The **audit log tarlogs** and **untarlogs** commands affect the appliance file system, and do not involve the HSM -- they are working on logs that have previously been exported from the HSM.

User Privileges

Only specialized Audit users can access audit commands.

Syntax

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

Argument(s)	Shortcut	Description
-serial <serialnum>	**-s**	Specifies the serial number of the HSM from which you want to tar 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

WARNING: You will need to export the encrypted log secret 66331.lws
         by running the 'audit secret export' command in order to
         verify these logs on another HSM!

Compressing log files:

66331/
66331/ready_for_archive/
66331/ready_for_archive/hsm_66331_00000004.log
66331/ready_for_archive/hsm_66331_00000006.log
66331/ready_for_archive/hsm_66331_00000002.log
66331/ready_for_archive/hsm_66331_00000007.log
66331/ready_for_archive/hsm_66331_00000009.log
66331/ready_for_archive/hsm_66331_00000008.log
66331/ready_for_archive/hsm_66331_00000005.log
66331/ready_for_archive/hsm_66331_00000003.log
66331/hsm_66331_0000000a.log

The tar file containing logs is now available as file 'audit-66331.tgz'.
If you wish to verify your logs on another SA, scp/sftp them to another SA's audit
directory then use the 'audit log untar' command.

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.

The **audit log tarlogs** and **untarlogs** commands affect the appliance file system, and do not involve the HSM -- they are working on logs that have previously been exported from the HSM.

User Privileges

Only specialized Audit users can access audit commands.

Syntax

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

Argument(s)	Shortcut	Description
-file <logfilename>	**-f**	Specifies the name of the archived log file to restore.

Example

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

Cannot find the file in /home/audit/lush_files/
Found files:
66331  audit-66331.tgz

Command Result : 65535 (Luna Shell execution)



lunash:>audit log untarlogs -file audit-66331.tgz

Extracting logs to audit home:

66331/
66331/ready_for_archive/
66331/ready_for_archive/hsm_66331_00000004.log
66331/ready_for_archive/hsm_66331_00000006.log
66331/ready_for_archive/hsm_66331_00000002.log
66331/ready_for_archive/hsm_66331_00000007.log
66331/ready_for_archive/hsm_66331_00000009.log
66331/ready_for_archive/hsm_66331_00000008.log
66331/ready_for_archive/hsm_66331_00000005.log
66331/ready_for_archive/hsm_66331_00000003.log
66331/hsm_66331_0000000a.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.

User Privileges

Only specialized Audit users can access audit commands.

Syntax

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

Argument(s)	Shortcut	Description
-end <number>	**-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 <filename>	**-f**	Specifies the name of the log file to verify.
-serialsource <serialnum>	**-serials**	Specifies the serial number of the HSM that generated the log file that is being verified.
-serialtarget <serialnum>	**-serialt**	Specifies the serial number of the HSM that is performing the verification.
-start <number>	**-st**	Specifies the starting record of the subset of records to be verified from the file.

Example

Verification of local log file, with local secret

```
lunash:>audit log verify -file hsm_66331_00000002.log

Log file being verified ready_for_archive/hsm_66331_00000002.log.

Verifying log on HSM with serial 66331
```

```
Verified messages 270723 to 271699

Command Result : 0 (Success)
```

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 sftp.

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 Network HSM 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_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, sftp them to another SA's audit
directory then use the 'audit log untar' command.

Command Result : 0 (Success)
```

Here is where we sftp the secret file and the .tgz file to a different Luna Network HSM

```
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_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 -
serialsource 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)
```

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].

audit login

Log into the HSM Audit user.

The name "audit" is

For password-authenticated HSM, login needs the most recently set password for the "audit" HSM role.

For an HSM with multifactor quorum authentication, a new audit role secret was created on the HSM and imprinted on a white PED key, or otherwise an existing audit secret role secret was 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. (This might also include a PED PIN secret that was optionally entered from the PED keypad and must now be provided in order to complete the secret that the HSM needs from the white iKey. Further, the audit role secret might have been split initially by invoking MofN greater than 1, and so a quorum (M) of the N splits must be presented at login.)

User Privileges

Only specialized Audit users can access audit commands.

Syntax

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

Argument(s)	Shortcut	Description
-serial <serialnum>	**-s**	HSM Serial Number - identifies which HSM is to accept the login if you have multiple HSMs (for example a Backup HSM or a Luna USB HSM 7 locally connected to your host).
-password <password>	**-p**	The password of the HSM you are logging into. Used for password-authenticated HSMs. If you prefer not to write the password, in the clear, on the command line, leave it out and you will be prompted for it. Ignored for multifactor quorum-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 multifactor quorum-authenticated HSMs.

Example

Multifactor Quorum-Authenticated HSM

```
lunash:>audit login

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

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

Password-Authenticated HSM

```
lunash:>audit login

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

Command Result : 0 (Success)
```

audit logout

Log out the HSM Audit user.

User Privileges

Only specialized Audit users can access audit commands.

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
cert
clear
delete
list

Argument(s)	Shortcut	Description
add	**a**	Adds a Remote Logging Server. See "audit remotehost add" on the next page.
cert	**ce**	Add or delete CA and Client certificates. See "audit remotehost cert" on page 74.
clear	**cl**	Deletes all Remote Logging Servers. See "audit remotehost clear" on page 82.
delete	**d**	Delete a Remote Logging Server. See "audit remotehost delete" on page 83.
list	**l**	Display a list of all currently configured Remote Logging Servers. See "audit remotehost list" on page 84.

audit remotehost add

Add an identified Remote Logging Server.

> **NOTE** Using Luna Appliance Software 7.8.5 or newer, you have the option to choose **tls** for security when transferring audit logs to a remote logging server.

User Privileges

Only specialized Audit users can access audit commands.

Syntax

audit remotehost add -host <hostnameoripaddress> [**-protocol** <protocol>] [**-port** <port>] [**-mode** <authmode>] [**-name** <commonname>] [**-tls**]

Argument(s)	Shortcut	Description
-host <hostnameoripaddress>	**-h**	Specifies the Remote Logging Server Host Name or IP address.
-mode <authmode>	**-m**	Authentication mode. This option requires Luna Appliance Software 7.8.5 or newer. **Valid values:** server,mutual **Default:** server
-name <hostcommonname>	**-n**	Specifies the Remote Logging Server common name. This option requires Luna Appliance Software 7.8.5 or newer.
-port <port>	**-po**	Specifies the server port to use for the Remote Logging Server. **Range:** 0 to 65535 **Default:** 514
-protocol <protocol>	**-pr**	Specifies the protocol for remote logging with the specified server. The **-name** option is required when the protocol is **relp** **Valid values:** tcp,udp,relp **Default:** udp The **-name** option is required when the protocol is **relp**.
-tls	**-t**	Setup host with TLS. Not used with **udp** protocol. This option requires Luna Appliance Software 7.8.5 or newer.

Example

```
lunash:>audit remotehost add -host 192.20.11.64

Stopping syslog:                                           [  OK  ]

Starting syslog:                                           [  OK  ]
```

```
iptables: Saving firewall rules to /etc/sysconfig/iptables:[  OK  ]

Command Result : 0 (Success)
```

Example using Luna Appliance Software 7.8.5 or newer

```
lunash:>audit remotehost add -host 192.20.11.64 -protocol tcp -port 54 -mode server -tls

Stopping syslog:                                           [  OK  ]

Starting syslog:                                           [  OK  ]
iptables: Saving firewall rules to /etc/sysconfig/iptables:[  OK  ]

Command Result : 0 (Success)
```

audit remotehost cert

Access the **audit remotehost cert** commands to manage the syslog remote host certificates. See Remote Audit Logging.

> **NOTE** This command is available using Luna Appliance Software 7.8.5 or newer.

These commands parallel the equivalent syslog commands, and act upon the same certificates. The appliance *admin* user and the *audit* user can both modify their remote logging configurations independently, but the certificates that secure remote syslogging and remote audit logging are used in common and must remain intact if one or the other party needs them; either party should inform the other if any change to the certs is about to occur.

Syntax

audit remotehost cert

delete
deleteCA
gen
install
installCA
status

Argument(s)	Shortcut	Description
delete	**d**	Delete an HSM certificate. See "audit remotehost cert delete" on the next page.
deleteCA	**deleteC**	Delete a CA certificate. See "audit remotehost cert deleteCA" on page 76.
gen	**g**	Generates a CSR or client certificate. See "audit remotehost cert gen" on page 77.
install	**i**	Installs the HSM certificate. See "audit remotehost cert install" on page 79.
installCA	**installC**	Installs the CA certificate. See "audit remotehost cert installCA" on page 80.
status	**s**	Displays the certificate configuration status. See "audit remotehost cert status" on page 81.

audit remotehost cert delete

Delete an existing certificate.

> **NOTE** This command is available using Luna Appliance Software 7.8.5 or newer.

> **CAUTION!** The certificate used by remote audit logging is the same certificate configured for NTLS connections on the appliance.
> If the -force option is not used when attempting to delete a certificate, and a certificate exists, then an alert is issued. An existing certificate might have been configured by the audit user previously, or might be in use for Luna Network HSM 7 by the appliance admin user for operational traffic (NTLS, etc.), and should be deleted only if affected parties are aware.

User Privileges

Only specialized Audit users can access audit commands.

Syntax

audit remotehost cert delete -force

Argument(s)	Shortcut	Description
-force	**-f**	Forces the deletion without prompting.

Example

```
lunash:>audit remotehost cert delete -force


Command Result : 0 (Success)
```

audit remotehost cert deleteCA

Deletes the CA certificate.

> **NOTE** This command is available using Luna Appliance Software 7.8.5 or newer.

User Privileges

Only specialized Audit users can access audit commands.

Syntax

audit remotehost cert deleteCA [**-force**]

Argument(s)	Shortcut	Description
-force	**-f**	Deletes the installed CA certificate without warning the user if it already exists.

Example

```
lunash:>audit remotehost cert deleteCA -force


Command Result : 0 (Success)
```

audit remotehost cert gen

Generates a private key and CSR or self-signed certificate.

> **NOTE** This command is available using Luna Appliance Software 7.8.5 or newer.

> **CAUTION!** The **syslog remotehost cert gen** command and the **audit remotehost cert gen** command affect the same certificate, in the same file system location within the Luna Network HSM 7appliance. If either the *admin* user or the *audit* user makes a change to an existing certificate, it affects both:
>
> > the encrypted remote logging of appliance events and
> >
> > the encrypted remote logging of cryptographic module events.
>
> Before using the **...cert gen** command, in either context (*admin* and syslog remotehost, or *audit* and audit remotehost) use the respective **...cert status** command to see whether a shared certificate is already configured.

User Privileges

Only specialized Audit users can access audit commands.

Syntax

audit remotehost cert gen [<ipaddress>] [**-startdate** <startdate>] [**-days** <days>] [**-country** <iso_country_code>] [**-state** <name_of_state_province_region>] [**-location** <city_name>] [**-organization** <organization_legal_name>] [**-orgunit** <division_within_org>] [**-email** <contact_email_address>] [**-san** <SAN>] [**-keysize** <size>] [**-keytype** <key_type>] [**-curve** <curve_name>] [**-csr**] [**-force**]

Argument(s)	Shortcut	Description
.	. <ipaddress>	Generates a CSR, or the self-signed client certificate client_syslog.pem in the file-space of the user that generated the cert Default: 1.2.3.4
-startdate <startdate>	**-star**	Certificate start date(not available with -csr) (0-99991231).
-days <days>	**-d**	Certificate validity days (1-3653)
-country <country code>	**-co**	The country in which your organization is located, entered as a two-letter ISO code.
-state <State/Region/Province (full name)>	**-stat**	The state or region in which your organization is located. (Example Québec)
-location <city name>	**-l**	The city in which your organization is located.

Argument(s)	Shortcut	Description
-organization	**-orga**	The full legal name of your organization, including suffixes such as LLC, Corp, etc.
-orgunit	**-orgu**	The division in your organization that deals with this certificate.
-email	**-e**	Email address used to contact the owner.
-san <subject alternative name>	**-sa**	In addition to the FQDN if you intend to support other subdomains
-keysize <size>	**-keys**	RSA key size: Default: 2048 (choose among 2048,3072,4096)
-keytype <keytype>	**-keyt**	Key type (ecc,rsa) Default: rsa
-curve <curve_name>	**-cu**	Elliptic Curve name Supported values: secp256k1, secp384r1, secp521r1, prime256v1 Default: secp384r1
-csr	**-cs**	Generate CSR - client certificate request file `client_syslog_csr.csr` in the file-space of the user that generated the cert request
-force	**-f**	Deletes the installed certificate without warning the user if it already exists.

An error is shown if CSR generation fails, or if certificate generation fails.

Disallowed option combinations

Do not included the **-curve** option if the **-keytype** is "rsa".

Do not included the **-keysize** option if the **-keytype** is "ecc".

Example

```
lunash:>audit remotehost cert gen 192.168.79.157 -csr -startdate 20230410 -days 10 -country CA
-state ON -organization Thales -orgunit dis -location OT -email example@thales.com


Command Result : 0 (Success)
```

audit remotehost cert install

Install an HSM certificate to enable TLS.

> **NOTE** This command is available using Luna Appliance Software 7.8.5 or newer.

User Privileges

Only specialized Audit users can access audit commands.

Syntax

audit remotehost cert install <filename> [**-force**]

Argument(s)	Shortcut	Description
.	<file name>	Install CA certificate.
-force	**-f**	Force the action .

Example

```
lunash:>my file list

1176 May  6 14:44 ca.pem

Command Result : 0 (Success)
lunash:>
lunash:>audit remotehost cert installCA ca.pem

Attempting to install ca.pem

Stopping syslog:                                          [  OK  ]

Starting syslog:                                          [  OK  ]

CA certificate installed successfully.

Command Result : 0 (Success)

lunash:>audit remotehost cert status

  CA Certificate:  Configured
  HSM Certificate: Not Configured
  HSM Private Key: Not Configured

Command Result : 0 (Success)
```

audit remotehost cert installCA

Install a CA certificate.

> **NOTE** This command is available using Luna Appliance Software 7.8.5 or newer.

User Privileges

Only specialized Audit users can access audit commands.

Syntax

audit remotehost cert installCA <filename> [**-force**]

Argument(s)	Shortcut	Description
.	<file name>	Install CA certificate.
-force	**-f**	Force the action .

Example

```
lunash:>my file list

1176 May  6 14:44 ca.pem

Command Result : 0 (Success)
lunash:>
lunash:>audit remotehost cert installCA ca.pem

Attempting to install ca.pem

Stopping syslog:                                          [  OK  ]

Starting syslog:                                          [  OK  ]

CA certificate installed successfully.

Command Result : 0 (Success)

lunash:>audit remotehost cert status

  CA Certificate:  Configured
  HSM Certificate: Not Configured
  HSM Private Key: Not Configured

Command Result : 0 (Success)
```

audit remotehost cert status

Displays the certificate configuration and key status.

> **NOTE** This command is available using Luna Appliance Software 7.8.5 or newer.

User Privileges

Only specialized Audit users can access audit commands.

Syntax

audit remotehost cert -status

Example

```
lunash:>audit remotehost cert -status


CA Certificate:   Configured

HSM Certificate:  Configured

HSM Private key:  Configured

Command Result : 0 (Success)
```

audit remotehost clear

Deletes the remote audit logging servers (any host and port combination(s)). Certificates are maintained, and this command does not affect syslog servers.

> **NOTE** No configuration added by the **admin** user is affected. The **audit** user cannot view, delete, or clear any configuration made by the **admin** user.

User Privileges

Only specialized Audit users can access audit commands.

Syntax

audit remotehost clear [**-force**]

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

Example

```
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

Stopping syslog:                                           [  OK  ]

Starting syslog:                                           [  OK  ]
iptables: Saving firewall rules to /etc/sysconfig/iptables:[  OK  ]


Command Result : 0 (Success)
```

audit remotehost delete

Deletes the specified remote audit server from the list.

> **NOTE** No configuration added by the **admin** user is affected. The **audit** user cannot view, delete, or clear any configuration made by the **admin** user.

User Privileges

Only specialized Audit users can access audit commands.

Syntax

audit remotehost delete -host <hostname/IP> **-port** <port> [**-force**]

Argument(s)	Shortcut	Description
-host <hostname/IP>	**-h**	Specifies the host name or IP address of the remote logging server.
-port <port>	**-h**	Remote Logging Server Port Number (0-65535). This option requires Luna Appliance Software 7.8.5 or newer. **Default:** 514
-force	**.**	Force the action without prompt.

Example

```
lunash:>audit remotehost delete -host 192.20.11.64

Stopping syslog:                                           [  OK  ]

Starting syslog:                                           [  OK  ]
iptables: Saving firewall rules to /etc/sysconfig/iptables:[  OK  ]

Command Result : 0 (Success)
```

audit remotehost list

Display a list of the currently configured remote logging servers.

> **NOTE** No configuration added by the **admin** user is affected. The **audit** user cannot view, delete, or clear any configuration made by the **admin** user.

User Privileges

Only specialized Audit users can access audit commands.

Syntax

audit remotehost list

Example

```
lunash:>audit remotehost list

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

  192.20.11.64:514, 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

Argument(s)	Shortcut	Description
export	**e**	Export the audit logging secret. See "audit secret export" on the next page
import	**i**	Import the audit logging secret. See "audit secret import" on page 87.

 Copyright 2001-2025 Thales Group

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.

User Privileges

Only specialized Audit users can access audit commands.

Syntax

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

Argument(s)	Shortcut	Description
-serial <serialnum>	**-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

The encrypted log secret file 66331.lws now available for scp/sftp.

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)
```

 Copyright 2001-2025 Thales Group

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.

User Privileges

Only specialized Audit users can access audit commands.

Syntax

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

Argument(s)	Shortcut	Description
-file <filename>	**-f**	Specifies the name of the audit secret file to import.
-serialsource <serialnum>	**-serials**	Specifies the serial number of the source HSM from which the logging secret was exported.
-serialtarget <serialnum>	**-serialt**	Specifies the serial number of the target HSM to which the logging secret will be imported.

Example

```
lunash:>audit secret import -serialtarget 532018 -serialsource 66331 -file 66331.lws

Successfully imported the encrypted log secret 66331.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)
```

audit show

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

> **TIP** The **audit show** command can show "`HSM is currently storing 0 log records`", while the **audit log list** command shows some number of log files. This is normal and means that the **c**all**b**ack **s**ervice (cbs), running on the HSM appliance is storing audit log records from the cryptographic module into the HSM appliance file system.
>
> The cbs is temporarily stopped when an "audit log tarlogs" on page 63 action is being performed, then cbs resumes.
>
> If a number other than zero records persists and grows on the cryptographic module, then either the cbs is not running, or something else is preventing cbs from writing to the file system.
>
> Verify with "service status" on page 470 that cbs is running. If cbs is running, check that /var/audit usage is less than 200GB with "status disk" on page 476.

User Privileges

Only specialized Audit users can access audit commands.

Syntax

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

Argument(s)	Shortcut	Description
-serial <serialnum>	**-s**	Specifies the serial number of the cryptographic module (HSM) whose audit logging information you want to display. The default is to use the embedded HSM.

Example (audit user logged in)

```
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)
```

Example (audit role not configured)

```
lunash:>audit show
       HSM Logging Status:

              HSM found logging daemon
              Logging has not yet been configured for this HSM
              HSM is currently storing 3209 log records.

        HSM Audit Role: not initialized

HSM Time  : Mon Dec 17 17:50:35 2021
HOST Time : Mon Dec 17 17:51:07 2021

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 Network HSM 7 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.

> **NOTE** Audit log and syslog entries are timestamped in UTC format.

User Privileges

Only specialized Audit users can access audit commands.

Syntax

audit sync

Example

```
lunash:>audit sync

Command Result : 0 (Success)
```

client

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

Syntax

client

- **addCA**
- **assignPartition**
- **delete**
- **deleteCA**
- **fingerprint**
- **hostip**
- **list**
- **listCAs**
- **register**
- **revokePartition**
- **show**
- **update**

Argument(s)	Shortcut	Description
addCA	**ad**	Add a client Certificate Authority (CA) certificate to the truststore. See "client addCA" on page 93.
assignPartition	**a**	Assign partition access rights to a client. See "client assignPartition" on page 94.
delete	**d**	Delete a client. See "client delete" on page 95.
deleteCA	**deleteC**	Delete a client Certificate Authority (CA) certificate from the truststore. See "client deleteCA" on page 96.
fingerprint	**f**	Display the certificate fingerprint for a registered client. See "client fingerprint" on page 101.
hostip	**h**	Display or configure the client-to-IP mapping. See "client hostip" on page 102.
list	**l**	Display a list of the registered clients by client name. See "client list" on page 106.
listCAs	**listC**	Display a list of the registered client certificates. See "client listCAs" on page 107.

Argument(s)	Shortcut	Description
register	**reg**	Add a client to the list of clients that can access the Luna appliance's NTLS. See "client register" on page 108.
revokePartition	**rev**	Revoke access privileges to the specified partition from the specified client. See "client revokePartition" on page 110.
show	**s**	Display the hostname or IP address of a client, and any partitions assigned to the client. See "client show" on page 111.
update	**u**	Update the certificate for a client that is already registered on the appliance. See "client update" on page 111.

client addCA

Add a Certificate Authority (CA) chain certificate to the trust store.

> **NOTE** The certificate file must be available in the appliance filesystem (see "my file list" on page 306).
> This feature requires Luna Network HSM 7 Appliance Software 7.7.0 or newer.

User Privileges

Users with the following privileges can perform this command:

- Admin
- Operator

Syntax

client addCA <cert_name>

Argument(s)	Description
<cert_name>	The file name of the CA certificate to be added.

Example

```
lunash:>client addCA CAroot

Attempting to install CA cert CAroot

Command Result : 0 (Success)
```

client assignPartition

Assign access privileges for a registered NTLS 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.

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**).

User Privileges

Users with the following privileges can perform this command:

> Admin

> Operator

Syntax

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

Argument(s)	Shortcut	Description
-client <clientname>	**-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 <name>	**-p**	Specifies the name of the partition to which the client will gain access. Use the **partition list** command to obtain the partition name.

Example

```
lunash:>client assignPartition -client 192.20.11.91 -partition par001


'client assignPartition' successful.


Command Result : 0 (Success)
```

client delete

Remove a client from the list of clients registered to use the Luna Network HSM 7 appliance. The command requires user interaction to verify that deletion should occur. This can be overridden with the **-force** option.

User Privileges

Users with the following privileges can perform this command:

- Admin
- Operator

Syntax

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

Argument(s)	Shortcut	Description
-client <clientname>	**-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 192.20.11.91


CAUTION:  Are you sure you wish to delete client named:
            192.20.11.91
          Type 'proceed' to delete the client, or 'quit'
          to quit now.
          > proceed
'client delete' successful.


Command Result : 0 (Success)
```

client deleteCA

Delete a Certificate Authority (CA) chain certificate from the trust store.

> **NOTE** This feature requires Luna Network HSM 7 Appliance Software 7.7.0 or newer.

User Privileges

Users with the following privileges can perform this command:

- Admin
- Operator

Syntax

client deleteCA <cert_name>

Argument(s)	Description
<cert_name>	The name of the certificate to be deleted.

Example

```
lunash:>client deleteCA CAroot

Attempting to remove CA cert CAroot

Command Result : 0 (Success)
```

client dn

Access commands that allow you to display or configureclient Distinguished Name (DN) filters.

> **NOTE** This command requires Luna Appliance Software 7.8.4 or newer.

Syntax

client dn

assign
delete
show

Argument(s)	Shortcut	Description
assign	**a**	Assign a Distinguished Name (DN) filter to a client. See "client dn assign" on the next page.
delete	**s**	Delete a Distinguished Name (DN) filter assigned to a client. See "client dn delete" on page 99.
show	**d**	View a client's configured Distinguished Name (DN) filter. See "client dn show" on page 100.

client dn assign

Assign a Distinguished Name (DN) filter to a client.

> **NOTE** This command requires Luna Appliance Software 7.8.4 or newer.

User Privileges

Users with the following privileges can perform this command:

- Admin
- Operator

Syntax

client dn assign -client <clientname> **-dn** <dnfilter>

Argument(s)	Shortcut	Description
-client <clientname>	**-c**	Specifies the name of the registered client to which the filter applies.
-dn <dnfilter string>	**-d**	Distinguished name filter string to uniquely validate a calling client.
-force	**-f**	Force the action, for scripting/automation.

Example

```
lunash:>client dn assign -c 10.124.79.157 -dn "C=CA/ST=Ontario/L=Ottawa/O=My
company/DC=thales/DC=com/CN=192.168.79.157/OU=DIS/GN=John/SN=Doe/serialNumber=001/emailAddress=
example@example.com/initials=PB/pseudonym=PBS"


'client DN filter assignment' successful.


Command Result : 0 (Success)
```

client dn delete

Delete a Distinguished Name (DN) filter assigned to a client.

> **NOTE** This command requires Luna Appliance Software 7.8.4 or newer.

User Privileges

Users with the following privileges can perform this command:

- Admin
- Operator

Syntax

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

Argument(s)	Shortcut	Description
-client <clientname>	**-c**	Specifies the name of the registered client to which a filter applies.
-force	**-f**	Force the filter deletion with no further warning, for scripting/automation.

Example

```
lunash:>client dn delete -c 192.168.79.157


WARNING! This will delete the DN filter for the client.
If you are sure that you wish to proceed, then type 'proceed', otherwise type 'quit'

> proceed
Proceeding...


'client DN filter deletion' successful.

Command Result : 0 (Success)
```

client dn show

View a client's configured Distinguished Name (DN) filter.

> **NOTE** This command requires Luna Appliance Software 7.8.4 or newer.

User Privileges

Users with the following privileges can perform this command:

- Admin
- Operator
- Monitor

Syntax

client dn show -client <clientname>

Argument(s)	Shortcut	Description
-client <clientname>	**-c**	Specifies the name of the registered client to which a filter applies.

Example

```
lunash:>client dn show -c 192.168.79.157


Configured Filter :  C=CA/ST=Ontario/L=Ottawa/O=My
company/DC=thales/DC=com/CN=192.168.79.157/OU=DIS/GN=John/SN=Doe/serialNumber=001/emailAddress=
example@example.com/initials=PB/pseudonym=PBS


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.

User Privileges

Users with the following privileges can perform this command:

- Admin
- Operator

Syntax

client fingerprint -client <clientname>

Argument(s)	Shortcut	Description
-client <clientname>	**-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 192.20.11.91


Certificate fingerprint: 7D:8F:9F:45:11:13:30:AC:10:86:E0:3B:04:B0:89:DB:91:DE:05:D7


Command Result : 0 (Success)
```

client hostip

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

If you registered your client by host name, the appliance will need to use a DNS server to look up the device IP address. To ensure that the client is reachable in the event of a DNS failure, you can use these commands to map the client host name to its IP address, and save the mapping locally on the appliance.

Syntax

client hostip

map
show
unmap

Argument(s)	Shortcut	Description
map	**m**	Map a client to an IP address. See "client hostip map" on the next page.
show	**s**	Shows current client-host-to-IP mapping. See "client hostip show" on page 104.
unmap	**u**	Remove a client-to-IP mapping. See "client hostip unmap" on page 105.

client hostip map

Map a client's host name to its IP address.

User Privileges

Users with the following privileges can perform this command:

> Admin

> Operator

Syntax

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

Argument(s)	Shortcut	Description
-client <clientname>	**-c**	Specifies the name of the client for which you want to create the association.
-ip <ipaddress>	**-i**	Specifies the IP address of the client for which you want to create the association.

Example

```
lunash:>client hostip map -client myPC -ipaddress 168.10.10.254

Command Result : 0 (Success)
```

client hostip show

Display the current client-to-IP mapping.

User Privileges

Users with the following privileges can perform this command:

- Admin
- Operator
- Monitor

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.

User Privileges

Users with the following privileges can perform this command:

- Admin
- Operator

Syntax

client hostip unmap -client <clientname>

Argument(s)	Shortcut	Description
-client <clientname>	**-c**	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 -client myPC

Command Result : 0 (Success)
```

client list

Display a list of the registered clients by client name.

User Privileges

Users with the following privileges can perform this command:

- Admin
- Operator
- Monitor

Syntax

client list

Example

```
lunash:>client list

registered client 1: 10.124.0.87
registered client 2: 192.20.11.91


Command Result : 0 (Success)
```

client listCAs

Display a list of the Certificate Authority (CA) chain certificates in the appliance trust store.

> **NOTE** This feature requires Luna Network HSM 7 Appliance Software 7.7.0 or newer.

User Privileges

Users with the following privileges can perform this command:

- Admin
- Operator
- Monitor

Syntax

client listCAs

Example

```
lunash:>client listCAs

CAroot
  subject= /CN=OTT1-TITAN-CA
  issuer= /CN=OTT1-TITAN-CA

Command Result : 0 (Success)
```

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 can be used to perform the registration, but is not needed (see the **-noCert** option below) as of appliance software version 7.8.3. Certificates can be exchanged later. If **-noCert** is not used, then a certificate named for hostname or IP is expected.
>
> NTLS always employs bilateral authentication thus the client certificate is definitely being used. What "**-nocert**" means is that the client certificate is not self-signed, thus only the CA certificates are required to be in the Luna Network HSM 7 appliance trust store.

User Privileges

Users with the following privileges can perform this command:

- Admin
- Operator

Syntax

client register -client <clientname> {**-hostname** <hostname> | **-ip** <IPaddress>} [**-noCert**] [**-force**]

Argument(s)	Shortcut	Description
-client <clientname>	**-c**	The new client's name. 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.

Argument(s)	Shortcut	Description
-hostname <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. Requirements for hostnames are tightened using Luna Appliance Software 7.9.0 or newer, to be more compliant with internet standards. If you have hostnames with embedded underscore characters "_", those will have that disallowed character removed during upgrade; so, for example, `my_hostname` becomes `myhostname`. Additionally, you may not start or end a hostname with a period "." character or a dash "-" character, but they are suitable to use *within* a hostname if you wish (example "host-name" or "my.host.name" are acceptable, but not ".hostname" or "hostname-"). Be sure to update scripts and any working notes or instructions.
-ip <IPaddress>	**-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.
-noCert	**-n**	Register a client without requiring a certificate. (See NOTE above on this page.)

Example

```
lunash:>client register -client 192.168.11.91 -ip 192.168.11.91


'client register' successful.


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.

User Privileges

Users with the following privileges can perform this command:

- Admin
- Operator

Syntax

client revokePartition -client <clientname> **-partition** <partitionname>

Argument(s)	Shortcut	Description
-client <clientname>	**-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 <partitionname>	**-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 192.20.11.91 -partition par001


'client revokePartition' successful.


Command Result : 0 (Success)
```

client show

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

User Privileges

Users with the following privileges can perform this command:

> Admin

> Operator

> Monitor

Syntax

client show -client <clientname>

Argument(s)	Shortcut	Description
-client <clientname>	**-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

```
lunash:>client show -client 192.20.11.91


ClientID:     192.20.11.91
IPAddress:    192.20.11.91
Partitions:   "par001"


Command Result : 0 (Success)
```

client update

Update the certificate for a client that is already registered on the appliance.

> **NOTE** The client's certificate file is needed to perform the registration. It must be present in the LunaSH user's files (see "my file list" on page 306) before running this command.
>
> This feature requires Luna Appliance Software 7.8.3 or newer.

User Privileges

Users with the following privileges can perform this command:

> Admin

> Operator

Syntax

client update -client <clientname> {**-hostname** <hostname> | **-ip** <IPaddress>} [**-force**]

Argument(s)	Shortcut	Description
-client <clientname>	**-c**	The client's name.
-force	**-f**	Force the action without prompting.
-hostname <hostname>	**-h**	The hostname of the 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 <IPaddress>	**-i**	The IP address of the 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.

Example

```
lunash:>client update -client 192.20.11.91 -ip 192.20.11.91


'client update' successful.


Command Result : 0 (Success)
```

cluster

Access commands that allow you to manage clusters and cluster configuration on the appliance. See also the "keyring" on page 292 commands.

> **NOTE** Thales requires minimum Luna Appliance Software 7.8.5 with the lnh_cluster-1.0.4 package, Luna HSM Firmware 7.8.4, and Luna HSM Client 10.7.2 to use clusters in production environments, or minimum Luna Appliance Software 7.9.0 with the lnh_cluster-1.0.5 package, Luna HSM Firmware 7.8.4, and Luna HSM Client 10.8.0 to migrate keys from Luna application partitions.

Syntax

cluster

- **admin**
- **backup**
- **client**
- **config**
- **config show**

create
delete
disable
enable
group list
join
leave
list
member
restore
show
status

Argument(s)	Shortcut	Description
admin	**a**	Access commands to enable or disable the **clusteradmin** service. This command is available using Luna Appliance Software 7.8.5 or newer, with the lnh_cluster-1.0.4 package or newer installed. See "cluster admin" on the next page.
backup	**b**	Access commands to configure scheduled backups of keyrings and objects on the cluster, or run manual backup operations. See "cluster backup" on page 117.
client	**cl**	Access commands to register or deregister the local appliance to a cluster. See "cluster client" on page 122.
config	**co**	Configure the cluster network settings. See "cluster config" on page 131.
config show	**co s**	Display the configured network settings for the cluster. See "cluster config show" on page 135.
create	**cr**	Create a new cluster on the appliance. See "cluster create" on page 136.
delete	**de**	Delete the cluster on the appliance. See "cluster delete" on page 137.
disable	**di**	Stop and disable the **cluster** service. If the service is disabled, it will not restart automatically. See "cluster disable" on page 138.
enable	**e**	Enables and starts the **cluster** service. When enabled, the service will restart automatically if it is interrupted. See "cluster enable" on page 139.
group list	**g l**	Display a list of affinity groups that have been created within the cluster. See "cluster group list" on page 140.

Argument(s)	Shortcut	Description
join	**j**	Join an existing cluster created on another Luna Network HSM 7. See "cluster join" on page 141.
leave	**le**	Remove a Luna Network HSM 7 member appliance from a cluster. See "cluster leave" on page 142.
list	**li**	Display a list of members on the cluster and their member IDs. See "cluster list" on page 143.
member	**me**	Access commands to get information about the members of a cluster, or manually authorize the local member to create keyrings and objects on the cluster. See "cluster member" on page 144.
restore	**r**	Access commands to restore keyrings to a cluster from backup. See "cluster restore" on page 158.
show	**sh**	Display information about the specified cluster, including the number of keyrings and keys created, number of authorized members, number of sessions and a breakdown of some crypto operations performed by the cluster. See "cluster show" on page 160.
status	**st**	Display the status of the **cluster** service. See "cluster status" on page 162.

cluster admin

Access commands to configure the **clusteradmin** service. This service allows you to use the cluster REST API (see Luna Cluster REST API Reference).

> **NOTE** This command is available using Luna Appliance Software 7.8.5 or newer, with the lnh_cluster-1.0.4 package or newer installed.
>
> Thales requires minimum Luna Appliance Software 7.8.5 with the lnh_cluster-1.0.4 package, Luna HSM Firmware 7.8.4, and Luna HSM Client 10.7.2 to use clusters in production environments, or minimum Luna Appliance Software 7.9.0 with the lnh_cluster-1.0.5 package, Luna HSM Firmware 7.8.4, and Luna HSM Client 10.8.0 to migrate keys from Luna application partitions.

Syntax

cluster admin

disable
enable
status

Argument(s)	Shortcut	Description
disable	**d**	Disable the **clusteradmin** service (*does not* restart automatically after appliance reboot). See "cluster admin disable" below.
enable	**e**	Enable the **clusteradmin** service (restarts automatically after appliance reboot). See "cluster admin enable" on the next page.
status	**s**	Display the status of the **clusteradmin** service. See "cluster admin status" on page 117.

cluster admin disable

Disable the **clusteradmin** service. When disabled, the service does not restart automatically after an appliance reboot. This service allows you to use the cluster REST API (see Luna Cluster REST API Reference).

> **NOTE** This command is available using Luna Appliance Software 7.8.5 or newer, with the lnh_cluster-1.0.4 package or newer installed.
>
> Thales requires minimum Luna Appliance Software 7.8.5 with the lnh_cluster-1.0.4 package, Luna HSM Firmware 7.8.4, and Luna HSM Client 10.7.2 to use clusters in production environments, or minimum Luna Appliance Software 7.9.0 with the lnh_cluster-1.0.5 package, Luna HSM Firmware 7.8.4, and Luna HSM Client 10.8.0 to migrate keys from Luna application partitions.

REST API: PATCH /api/lunasa/services/{serviceid}

User Privileges

Users with the following privileges can perform this command:

- Admin
- Operator

Syntax

cluster admin disable [**-force**]

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

Example

```
lunash:>cluster admin disable

WARNING !!  This operation will disable Cluster Administration Service!!!
If you are sure that you wish to proceed, then type 'proceed', otherwise type 'quit'
```

```
> proceed
Proceeding...


Command Result : 0 (Success)
```

cluster admin enable

Enable the **clusteradmin** service. When enabled, the service restarts automatically after an appliance reboot. This service allows you to use the cluster REST API (see Luna Cluster REST API Reference).

> **NOTE** This command is available using Luna Appliance Software 7.8.5 or newer, with the lnh_cluster-1.0.4 package or newer installed.
>
> Thales requires minimum Luna Appliance Software 7.8.5 with the lnh_cluster-1.0.4 package, Luna HSM Firmware 7.8.4, and Luna HSM Client 10.7.2 to use clusters in production environments, or minimum Luna Appliance Software 7.9.0 with the lnh_cluster-1.0.5 package, Luna HSM Firmware 7.8.4, and Luna HSM Client 10.8.0 to migrate keys from Luna application partitions.

REST API: PATCH /api/lunasa/services/{serviceid}

User Privileges

Users with the following privileges can perform this command:

- Admin
- Operator

Syntax

cluster admin disable [**-force**]

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

Example

```
lunash:>cluster admin enable

WARNING !!  This operation will enable Cluster Administration Service!!!
If you are sure that you wish to proceed, then type 'proceed', otherwise type 'quit'

> proceed
Proceeding...


Command Result : 0 (Success)
```

cluster admin status

Display the status of the **clusteradmin** service. This service allows you to use the cluster REST API (see Luna Cluster REST API Reference).

> **NOTE** This command is available using Luna Appliance Software 7.8.5 or newer, with the lnh_cluster-1.0.4 package or newer installed.
>
> Thales requires minimum Luna Appliance Software 7.8.5 with the lnh_cluster-1.0.4 package, Luna HSM Firmware 7.8.4, and Luna HSM Client 10.7.2 to use clusters in production environments, or minimum Luna Appliance Software 7.9.0 with the lnh_cluster-1.0.5 package, Luna HSM Firmware 7.8.4, and Luna HSM Client 10.8.0 to migrate keys from Luna application partitions.

REST API: GET /api/lunasa/services/{serviceid}

User Privileges

Users with the following privileges can perform this command:

- Admin
- Operator

Syntax

cluster admin status

Example

```
lunash:>cluster admin status

   Cluster Admin Service:
   ========================
   Configuration:         enabled
   Status:                running

Command Result : 0 (Success)
```

cluster backup

Access commands to configure scheduled backups of keyrings and objects on the cluster, or run manual backup operations.

> **NOTE** Thales requires minimum Luna Appliance Software 7.8.5 with the lnh_cluster-1.0.4 package, Luna HSM Firmware 7.8.4, and Luna HSM Client 10.7.2 to use clusters in production environments, or minimum Luna Appliance Software 7.9.0 with the lnh_cluster-1.0.5 package, Luna HSM Firmware 7.8.4, and Luna HSM Client 10.8.0 to migrate keys from Luna application partitions.

Syntax

cluster backup

config
disable
enable
run
show

Argument(s)	Shortcut	Description
config	**c**	Configure a scheduled cluster backup. See "cluster backup config" below.
disable	**d**	Disable any configured scheduled backups. See "cluster backup disable" on the next page.
enable	**e**	Enable the configured cluster backups. See "cluster backup enable" on page 120.
run	**r**	Run a cluster backup operation on demand. See "cluster backup run" on page 120.
show	**s**	Display the current scheduled cluster backup configuration. See "cluster backup show" on page 121.

cluster backup config

Configure a scheduled cluster backup.

> **NOTE** Thales requires minimum Luna Appliance Software 7.8.5 with the lnh_cluster-1.0.4 package, Luna HSM Firmware 7.8.4, and Luna HSM Client 10.7.2 to use clusters in production environments, or minimum Luna Appliance Software 7.9.0 with the lnh_cluster-1.0.5 package, Luna HSM Firmware 7.8.4, and Luna HSM Client 10.8.0 to migrate keys from Luna application partitions.

REST API: PUT /api/clusters/{clusterID}/backup

User Privileges

Users with the following privileges can perform this command:

> Admin

Syntax

cluster backup config -clusterid <string> **-filename** <filename> **-number** <number> **-time** <string>

Argument(s)	Shortcut	Description
-clusterid <string>	**-c**	Specifies the UUID of the cluster to configure backups for.
-filename <filename>	**-f**	Specifies the prefix to append to backup filenames.
-number <number>	**-n**	Specifies the number of backup files that will be stored. After this number of backups is reached, the oldest backup will be deleted to make room for each new backup file. **Valid Values: 1-15**
-time <string>	**-t**	Specifies the time to run backup operation(s) in the format **d:hh:mm** (where **d** is a number representing the day of the week as follows: **0** == Sunday, **1** == Monday, **2** == Tuesday, etc.)

Example

```
lunash:>cluster backup config -clusterid ac2a0f56-626e-4c91-a379-489b789a47e7 -filename
myScheduledBackup -number 5 -t 3:15:50

Success

Command Result : 0 (Success)
```

cluster backup disable

Disable any configured scheduled backups.

> **NOTE** Thales requires minimum Luna Appliance Software 7.8.5 with the lnh_cluster-1.0.4 package, Luna HSM Firmware 7.8.4, and Luna HSM Client 10.7.2 to use clusters in production environments, or minimum Luna Appliance Software 7.9.0 with the lnh_cluster-1.0.5 package, Luna HSM Firmware 7.8.4, and Luna HSM Client 10.8.0 to migrate keys from Luna application partitions.

REST API: PUT /api/clusters/{clusterID}/backup

User Privileges

Users with the following privileges can perform this command:

> Admin

Syntax

cluster backup disable

Example

```
lunash:>cluster backup disable

Success

Command Result : 0 (Success)
```

cluster backup enable

Enable the configured cluster backups. You must specify a backup password that will be required to restore from the scheduled backups.

> **NOTE** Thales requires minimum Luna Appliance Software 7.8.5 with the lnh_cluster-1.0.4 package, Luna HSM Firmware 7.8.4, and Luna HSM Client 10.7.2 to use clusters in production environments, or minimum Luna Appliance Software 7.9.0 with the lnh_cluster-1.0.5 package, Luna HSM Firmware 7.8.4, and Luna HSM Client 10.8.0 to migrate keys from Luna application partitions.

REST API: PUT /api/clusters/{clusterID}/backup

User Privileges

Users with the following privileges can perform this command:

> Admin

Syntax

cluster backup enable -backuppassword <password>

Argument(s)	Shortcut	Description
-backuppassword <password>	**-b**	Specifies a password that will be required to restore from the scheduled backups.

Example

```
lunash:>cluster backup enable -backupPassword myBUPassword

Success

Command Result : 0 (Success)
```

cluster backup run

Run a cluster backup operation on demand. This command does not back up the SMK used to encrypt the contents of the cluster. Refer to Backing Up/Restoring the Partition SMK for this procedure.

> **NOTE** Thales requires minimum Luna Appliance Software 7.8.5 with the lnh_cluster-1.0.4 package, Luna HSM Firmware 7.8.4, and Luna HSM Client 10.7.2 to use clusters in production environments, or minimum Luna Appliance Software 7.9.0 with the lnh_cluster-1.0.5 package, Luna HSM Firmware 7.8.4, and Luna HSM Client 10.8.0 to migrate keys from Luna application partitions.

Backup and restore operations can only be done on the primary member of the cluster.

REST API: PUT /api/clusters/{clusterID}/backup

User Privileges

Users with the following privileges can perform this command:

> Admin

Syntax

cluster backup run -clusterid <string> **-filename** <filename> **-backuppassword** <password>

Argument(s)	Shortcut	Description
-backuppassword <password>	**-b**	Specifies a password that will be required to restore from this backup.
-clusterid <string>	**-c**	The UUID of the cluster you want to back up.
-filename <filename>	**-f**	A filename for the backup file. Using the same filename as an existing backup will overwrite the existing file.

Example

```
lunash:>cluster backup run -clusterid ac2a0f56-626e-4c91-a379-489b789a47e7 -filename myBackup -
backupPassword myBUpassword

Successfully started job with ID 3

Command Result : 0 (Success)
```

cluster backup show

Display the current scheduled cluster backup configuration.

> **NOTE** Thales requires minimum Luna Appliance Software 7.8.5 with the lnh_cluster-1.0.4 package, Luna HSM Firmware 7.8.4, and Luna HSM Client 10.7.2 to use clusters in production environments, or minimum Luna Appliance Software 7.9.0 with the lnh_cluster-1.0.5 package, Luna HSM Firmware 7.8.4, and Luna HSM Client 10.8.0 to migrate keys from Luna application partitions.

REST API: PUT /api/clusters/{clusterID}/backup

User Privileges

Users with the following privileges can perform this command:

- Admin
- Operator
- Monitor

Syntax

cluster backup show

Example

```
lunash:>cluster backup show

Cluster backup configuration:
--------------------------------------------------------------------------------
Status:                          Enabled
File name:                       myScheduledBackup
Total backups:                   5
Time:                            Wednesday 15:50 (UTC: Wednesday 19:50)
Cluster UUID:                    ac2a0f56-626e-4c91-a379-489b789a47e7

Backup requests:

Id      Status        Finished Date          Description
201     Finished      02/21/2023, 10:47:14
202     Finished      02/21/2023, 10:49:50
203     Finished      02/21/2023, 10:50:03
```

> **NOTE** The **Description** column is reserved for use in a future version.

cluster client

Access commands to register or deregister clients to a cluster, and enable or disable clients that have been registered using a CSR. See Certificate-Based monitor Role Authentication.

> **NOTE** Thales requires minimum Luna Appliance Software 7.8.5 with the lnh_cluster-1.0.4 package, Luna HSM Firmware 7.8.4, and Luna HSM Client 10.7.2 to use clusters in production environments, or minimum Luna Appliance Software 7.9.0 with the lnh_cluster-1.0.5 package, Luna HSM Firmware 7.8.4, and Luna HSM Client 10.8.0 to migrate keys from Luna application partitions.

Syntax

cluster client

deregister
disable
enable
list
register

Argument(s)	Shortcut	Description
deregister	**de**	Remove a client's registration on the cluster. See "cluster client deregister" on the next page.
disable	**di**	Disable certificate authentication for a client that has been registered to the cluster using a Certificate Signing Request (CSR). See "cluster client disable" on page 125.
enable	**e**	Enable certificate authentication for a client that has been registered to the cluster using a Certificate Signing Request (CSR). See "cluster client enable" on page 126.
list	**l**	Display a list of clients connected to the specified cluster. See "cluster client list" on page 127.
register	**r**	Register a client Certificate Signing Request (CSR) to the cluster. See "cluster client register" on page 128.

cluster client assign

Assign a list of keyrings to a specified client. Only this client will be able to see the keyrings.

> **NOTE** This command requires minimum Luna Appliance Software 7.9.0 with the lnh_cluster-1.0.5 package installed.
>
> Thales requires minimum Luna Appliance Software 7.8.5 with the lnh_cluster-1.0.4 package, Luna HSM Firmware 7.8.4, and Luna HSM Client 10.7.2 to use clusters in production environments, or minimum Luna Appliance Software 7.9.0 with the lnh_cluster-1.0.5 package, Luna HSM Firmware 7.8.4, and Luna HSM Client 10.8.0 to migrate keys from Luna application partitions.

REST API: PATCH /api/cluster/client/{clientID}

User Privileges

Users with the following privileges can perform this command:

> Admin

Syntax

cluster client assign -clientid <UUID> **-keyringlist** <string>

Argument(s)	Shortcut	Description
-clientid	**-c**	Specifies the UUID of the client.
-keyringlist	**-k**	Specifies a colon-separated list of up to 6 keyring UUIDs to be assigned to this client. **NOTE** To assign or unassign more than 6 keyrings at a time, use the cluster REST API (see PATCH /api/cluster/client/{clientID}).

Example

```
lunash:>cluster client assign -clientid 5cb213f6-1465-4afa-96d3-ccafb233a95e -keyringlist
27aac110-f185-4f58-a5e4-929a68fda572:44f8d5f5-db53-4e0c-892b-3167f0648960:56271eb0-8a0d-4d7c-
b739-02cd65ff6c42

Success

Command Result : 0 (Success)
```

cluster client deregister

Remove a client's registration on the cluster.

> **NOTE** Thales requires minimum Luna Appliance Software 7.8.5 with the lnh_cluster-1.0.4 package, Luna HSM Firmware 7.8.4, and Luna HSM Client 10.7.2 to use clusters in production environments, or minimum Luna Appliance Software 7.9.0 with the lnh_cluster-1.0.5 package, Luna HSM Firmware 7.8.4, and Luna HSM Client 10.8.0 to migrate keys from Luna application partitions.

REST API: DELETE /api/clusters/{clusterID}/clients/{clientID}

User Privileges

Users with the following privileges can perform this command:

> Admin

Syntax

cluster client deregister -clientid <string>

Argument(s)	Shortcut	Description
-clientid	**-c**	Specifies the ID of the client to de-register.
-force	**-f**	De-register the client without asking for confirmation.

Example

```
lunash:>cluster client deregister -clientid 7ba8124c-05d3-412b-ac6b-fd2cbae6324a

WARNING: This operation will deregister Client from the Cluster!!!

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

proceed
Proceeding...

Client 7ba8124c-05d3-412b-ac6b-fd2cbae6324a was successfully deleted.

Command Result : 0 (Success)
```

cluster client disable

Disable certificate authentication for a client that has been registered to the cluster using a Certificate Signing Request (CSR). If certificate authentication is disabled, this client must authenticate using a LunaSH password. Only the specific role (**monitor** or a custom user with a **monitor** role) associated with the client can enable or disable it. See Certificate-Based monitor Role Authentication.

> **NOTE** Thales requires minimum Luna Appliance Software 7.8.5 with the lnh_cluster-1.0.4 package, Luna HSM Firmware 7.8.4, and Luna HSM Client 10.7.2 to use clusters in production environments, or minimum Luna Appliance Software 7.9.0 with the lnh_cluster-1.0.5 package, Luna HSM Firmware 7.8.4, and Luna HSM Client 10.8.0 to migrate keys from Luna application partitions.

REST API: PATCH /api/clusters/{clusterID}/clients/{clientID}

User Privileges

Users with the following privileges can perform this command:

> Monitor

Syntax

cluster client disable -clientid <string> [**-force**]

Argument(s)	Shortcut	Description
-clientid	**-c**	Specifies the ID of the client you want to disable.
-force	**-f**	Disable the client without prompting for confirmation.

Example

```
lunash:>cluster client disable -clientid 7ba8124c-05d3-412b-ac6b-fd2cbae6324a

WARNING !!  This operation will disable Client certificate authentication!!!
```

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

> proceed
Proceeding...

Success

Command Result : 0 (Success)
```

cluster client enable

Enable certificate authentication for a client that has been registered to the cluster using a Certificate Signing Request (CSR). If certificate authentication is disabled, this client must authenticate using a LunaSH password. Only the specific role (**monitor** or a custom user with a **monitor** role) associated with the client can enable or disable it. See Certificate-Based monitor Role Authentication.

> **NOTE** Thales requires minimum Luna Appliance Software 7.8.5 with the lnh_cluster-1.0.4 package, Luna HSM Firmware 7.8.4, and Luna HSM Client 10.7.2 to use clusters in production environments, or minimum Luna Appliance Software 7.9.0 with the lnh_cluster-1.0.5 package, Luna HSM Firmware 7.8.4, and Luna HSM Client 10.8.0 to migrate keys from Luna application partitions.

REST API: PATCH /api/clusters/{clusterID}/clients/{clientID}

User Privileges

Users with the following privileges can perform this command:

> Monitor

Syntax

cluster client enable -clientid <string> [**-force**]

Argument(s)	Shortcut	Description
-clientid	**-c**	Specifies the ID of the client you want to enable.
-force	**-f**	Enable the client without prompting for confirmation.

Example

```
lunash:>cluster client enable -clientid 7ba8124c-05d3-412b-ac6b-fd2cbae6324a

WARNING !!  This operation will enable Client certificate authentication!!!
If you are sure that you wish to proceed, then type 'proceed', otherwise type 'quit'

> proceed
Proceeding...
```

```
Success

Command Result : 0 (Success)
```

cluster client list

Display a list of clients connected to the specified cluster.

> **NOTE** Thales requires minimum Luna Appliance Software 7.8.5 with the lnh_cluster-1.0.4 package, Luna HSM Firmware 7.8.4, and Luna HSM Client 10.7.2 to use clusters in production environments, or minimum Luna Appliance Software 7.9.0 with the lnh_cluster-1.0.5 package, Luna HSM Firmware 7.8.4, and Luna HSM Client 10.8.0 to migrate keys from Luna application partitions.

REST API: GET /api/clusters/{clusterID}/clients

User Privileges

Users with the following privileges can perform this command:

- Admin
- Operator
- Monitor

Syntax

cluster client list -clusterid <string>

Argument(s)	Shortcut	Description
-clusterid	**-c**	Specifies the ID of the cluster to display clients for.

Example

```
lunash:>cluster client list -clusterid bbdf9d59-4194-49a5-ab71-7e0c9c9de01a

  Client Name                      User Name                Client ID
-----------------------------------------------------------------------------------------------
-
C 10.20.10.10                      N/A                      7ba8124c-05d3-412b-ac6b-
fd2cbae6324a
C 10.20.20.20                      monitor                  1d85903e-9e68-43c1-91aa-
3b04buk22914
C 10.20.30.30                      N/A                      31bd8b0a-9431-4452-b0bd-
2wefvsdf353c
C 10.20.40.40                      N/A                      890b05ca-d71b-4c2a-1234-
1a3f07050e88
C 10.20.50.50                      monitor                  326a6cd7-1ec8-4a50-23a6-
55657e5bee9a
C 10.20.60.60                      monitor                  68d869e4-c0a8-48d6-8bab-
1e4855812f3c
```

```
C 10.20.70.70                    N/A                    7c14ab34-82e0-4d4a-9cd9-
9326d26b7273
C 10.20.80.80                    monitor                ca01ef94-59de-48b4-3633-
e4e47ae1c8f6

Command Result : 0 (Success)
```

cluster client register

Register a client Certificate Signing Request (CSR) to the cluster.

> **NOTE** Thales requires minimum Luna Appliance Software 7.8.5 with the lnh_cluster-1.0.4 package, Luna HSM Firmware 7.8.4, and Luna HSM Client 10.7.2 to use clusters in production environments, or minimum Luna Appliance Software 7.9.0 with the lnh_cluster-1.0.5 package, Luna HSM Firmware 7.8.4, and Luna HSM Client 10.8.0 to migrate keys from Luna application partitions.

REST API: POST /api/clusters/{clusterID}/clients

User Privileges

Users with the following privileges can perform this command:

> Admin

Syntax

cluster client register -clusterid <string> **-label** <clientname> **-csr** <filename> [**-username** <username>]

Argument(s)	Shortcut	Description
-clusterid	**-cl**	Specifies the ID of the cluster you want to register the client to.
-csr	**-cs**	Specifies the filename of the client CSR you transferred to the appliance.
-label	**-l**	Specifies a label for the client.
-username	**-u**	Specifies a LunaSH username to associate with the client. This can be the default **monitor** role, or a custom user with the **monitor** role assigned (see Creating Custom Appliance User Accounts). The user must already exist on the appliance. This feature requires minimum Luna HSM Client 10.5.1 and Luna Network HSM 7 Appliance Software 7.8.1.

Example

```
lunash:>cluster client register -clusterid ac2a0f56-626e-4c91-a379-489b789a47e7 -label
myLunaClient -csr 1.2.3.4CSR.pem
```

```
Client Label:   myLunaClient
Client ID:      7ba8124c-05d3-412b-ac6b-fd2cbae6324a
Client signed certificate:
-----BEGIN CERTIFICATE-----
MIIChzCCAg2gAwIBAgIEAJocVjAKBggqhkjOPQQDAjBcMQswCQYDVQQGEwJDQTEQ
MA4GA1UECAwHT250YXJpbzEPMA0GA1UEBwwGT3R0YXdhMRQwEgYDVQQKDAtTYWZl
bmV0LUluYzEUMBIGA1UEAwwLSFNNLUNsdXN0ZXIwHhcNMjIwMzAzMDMyNjQ4WhcN
MjMwMzAzMDMyNjQ4WjBdMQswCQYDVQQGEwJDQTEQMA4GA1UECAwHT250YXJpbzEP
MA0GA1UEBwwGT3R0YXdhMRMwEQYDVQQKDApNeSBjb21wYW55MRYwFAYDVQQDDA0x
MC4xMjQuMTQzLjU2MIGbMBAGByqGSM49AgEGBSuBBAAjA4GGAAQACYFTirt0bzYo
TzAtL4akSwRU6i4V4owF5Y1hKdri589GAapX1YskfXEAWtlNRwA7RqPFT2VZdw0g
jIe+8b+taJEBhhVXZwuyqRf7NiPBnJ9IEniNs8HKWoUQltY0bwjhc0kQik9m9+55
ebT1lbnsnmKoG+ieCEj/nChzgey7v+xySHyjeTB3MAkGA1UdEwQCMAAwHQYDVR0O
BBYEFOlXxVmtRBoIye9qh1T/0oBobRPSMAsGA1UdDwQEAwIFoDAdBgNVHSUEFjAU
BggrBgEFBQcDAQYIKwYBBQUHAwIwHwYDVR0jBBgwFoAUMNwG/GbTdwN0mu8SHf/b
/ukbi34wCgYIKoZIzj0EAwIDaAAwZQIxAMjANbx2j67ykXjyE+aNuHYrCFMB9A6s
tG/mLbXdOM+aYFLI9nEiUQTZSpntG/61TgIwIwuTBWo02ZV+A8tpfEgT6mMZzt+7
9YDUB7ftlAQieByvrv6qrgTTkaviv24F0Fp7
-----END CERTIFICATE-----

Command Result : 0 (Success)
```

cluster client show

Display information about a registered cluster client, including the OUIDs of keyrings assigned to the client.

> **NOTE** This command requires minimum Luna Appliance Software 7.9.0 with the lnh_cluster-1.0.5 package installed.
>
> Thales requires minimum Luna Appliance Software 7.8.5 with the lnh_cluster-1.0.4 package, Luna HSM Firmware 7.8.4, and Luna HSM Client 10.7.2 to use clusters in production environments, or minimum Luna Appliance Software 7.9.0 with the lnh_cluster-1.0.5 package, Luna HSM Firmware 7.8.4, and Luna HSM Client 10.8.0 to migrate keys from Luna application partitions.

REST API: GET /api/clusters/{clusterID}/clients/{clientID}

User Privileges

Users with the following privileges can perform this command:

> Admin

Syntax

cluster client show -clusterid <UUID> **-clientid** <UUID> [**-detail**]

Argument(s)	Shortcut	Description
-clientid	**-cli**	Specifies the UUID of the client.

Argument(s)	Shortcut	Description
-clusterid	**-clu**	Specifies the UUID of the cluster.
-detail	**-d**	Include this option to display a list of UUIDs for all keyrings assigned to the specified client. When the list of keyrings is too long to appear on-screen, use commands for the Linux tool **less** to navigate the list, including: > **Down arrow**, **Enter**, **e**, or **j**: forward one line > **Up arrow**, **y** or **k**: backward one line > **Space bar** or **f**: forward one page > **b**: backward one page > **q**: exit > **h**: help

Example

```
lunash:>cluster client show -clusterid 9a168a8d-3a9e-4514-bb5d-c45a94f99830 -clientid 5cb213f6-
1465-4afa-96d3-ccafb233a95e -detail

Client name: myLunaClient
Client ID:   5cb213f6-1465-4afa-96d3-ccafb233a95e
User name:   N/A
Certificate:
    Fingerprint SHA256: 2a6d9313697feda219f1dffd7848233e225e7454de0d9281d1e9672ecf7d7d9d
    Start Date:         Mon, 11 Nov 2024 19:54:48 GMT
    End Date:           Thu, 09 Nov 2034 19:54:48 GMT
Assigned keyrings count: 5
Assigned keyrings:
    bab7bb14-4952-43a7-982c-1d619b866623
    72c2accf-eb14-4f84-a3b0-bc1e1579d024
    d1347267-b5b1-4546-a84c-1a4875c246f7
    3148a9d2-d2fd-43a4-8cf1-9b2d15ea0b62
    8c8668dc-8adc-45c6-ab85-fa52afad5197
```

cluster client unassign

Unassign a list of keyrings from a specified client. This client will no longer be able to access the keyring in LunaCM or crypto applications. Ensure that none of this client's applications are running operations on the keyring(s) you unassign. Client requests will be interrupted.

> **NOTE** This command requires minimum Luna Appliance Software 7.9.0 with the lnh_cluster-1.0.5 package installed.
>
> Thales requires minimum Luna Appliance Software 7.8.5 with the lnh_cluster-1.0.4 package, Luna HSM Firmware 7.8.4, and Luna HSM Client 10.7.2 to use clusters in production environments, or minimum Luna Appliance Software 7.9.0 with the lnh_cluster-1.0.5 package, Luna HSM Firmware 7.8.4, and Luna HSM Client 10.8.0 to migrate keys from Luna application partitions.

REST API: PATCH /api/cluster/client/{clientID}

User Privileges

Users with the following privileges can perform this command:

> Admin

Syntax

cluster client unassign -clientid <UUID> **-keyringlist** <string>

Argument(s)	Shortcut	Description
-clientid	**-c**	Specifies the UUID of the client.
-keyringlist	**-k**	Specifies a colon-separated list of up to 6 keyring UUIDs to be unassigned from this client. **NOTE** To assign or unassign more than 6 keyrings at a time, use the cluster REST API (see PATCH /api/cluster/client/{clientID}).

Example

```
lunash:>cluster client unassign -clientid 53a323fe-9528-4d24-87bf-69a614ab9bae -keyringlist
27aac110-f185-4f58-a5e4-929a68fda572:44f8d5f5-db53-4e0c-892b-3167f0648960:56271eb0-8a0d-4d7c-
b739-02cd65ff6c42

Success

Command Result : 0 (Success)
```

cluster config

Access commands that allow you to configure or display the cluster configuration settings, including the identity mode, client assignment mode, and core traffic IP.

> **NOTE** Thales requires minimum Luna Appliance Software 7.8.5 with the lnh_cluster-1.0.4 package, Luna HSM Firmware 7.8.4, and Luna HSM Client 10.7.2 to use clusters in production environments, or minimum Luna Appliance Software 7.9.0 with the lnh_cluster-1.0.5 package, Luna HSM Firmware 7.8.4, and Luna HSM Client 10.8.0 to migrate keys from Luna application partitions.

REST API: PUT /api/cluster/config

Using lnh_cluster-1.0.5 or newer

Syntax

cluster config

set
show

Argument(s)	Shortcut	Description
set	**se**	Using lnh_cluster-1.0.5 or newer, set the configuration for the cluster. See "cluster config set" on the next page.
show	**sh**	Display the configured settings for the cluster. See "cluster config show" on page 135.

Using lnh_cluster-1.0.4 or older

User Privileges

Users with the following privileges can perform this command:

- Admin
- Operator

Syntax

cluster config -service <service> [**-ipaddress** <ipaddress>] [**-interface** <netdevice>] [**-port** <port>]

Argument(s)	Shortcut	Description
-interface <netdevice>	**-in**	Specifies the network device to bind **admin** or **crypto** network traffic to. Valid values: **eth0**, **eth1**, **eth2**, **eth3**, **bond0**, **bond1**, **all**
-ipaddress <ipaddress>	**-ip**	Specifies the IP address to use for the core cluster traffic. The IP specified for the **core** traffic must be the same IP address as one of the appliance's network interfaces.

Argument(s)	Shortcut	Description
-port <port>	**-p**	Specifies the port to use for this type of traffic. Valid values: > **admin** service (default: **50070**): **50075-50079** > **crypto** service (default: **50052**): **50055-50059** **CAUTION!** In this release, changing the default port used for crypto operations on the cluster (**50052**) can cause communication problems between cluster members. Refer to known issue LUNA-26485.
-service <service>	**-s**	Specifies the type of network traffic to configure. Valid values: **core**, **admin**, **crypto**

Example

```
lunash:>cluster config -service core -ipaddress 1.2.3.4


Command Result : 0 (Success)
```

cluster config set

Configure the cluster network settings. This allows you to direct the cluster network traffic (**admin** or **crypto**) through one or another of the appliance's interfaces. The IP specified for the **core** service must be the same IP address as one of the appliance's network interfaces. This command also allows you to set the identity mode and client assignment mode on the cluster. Refer to Keyring Roles and Identity Modes and Client Assignment Modes for important information about these modes.

> **NOTE** This command requires minimum Luna Appliance Software 7.9.0 with the lnh_cluster-1.0.5 package installed. For older versions, see "cluster config" on page 131.
>
> Thales requires minimum Luna Appliance Software 7.8.5 with the lnh_cluster-1.0.4 package, Luna HSM Firmware 7.8.4, and Luna HSM Client 10.7.2 to use clusters in production environments, or minimum Luna Appliance Software 7.9.0 with the lnh_cluster-1.0.5 package, Luna HSM Firmware 7.8.4, and Luna HSM Client 10.8.0 to migrate keys from Luna application partitions.

> **TIP** Use lunash:> "cluster status" on page 162 to ensure that the **cluster** service is in either the `not running` or `running` state before setting or changing the cluster configuration. Using this command while the **cluster** service is `starting` or `stopping` can interrupt the operation and result in a `failed` state, requiring lunash:> "service restart" on page 467 **cluster**.

REST API: PUT /api/cluster/config

User Privileges

Users with the following privileges can perform this command:

> Admin

Syntax

cluster config set -service <service> [**-identity** <mode>] [**-clientAssignment** <mode>] [**-ipaddress** <ipaddress>] [**-interface** <netdevice>] [**-port** <port>]

Argument(s)	Shortcut	Description
-clientAssignment <mode>	**-c**	Specifies the client assignment mode to use for the cluster. Valid values: **auto**, **manual** > **Auto-Assignment Mode** (default): In this mode, keyrings are automatically assigned to all registered clients; all keyrings on the cluster are visible in LunaCM on any registered client. > **Manual Assignment Mode**: In this mode, keyrings must be manually assigned to or unassigned from registered clients. Clients are only able to see keyrings which have been assigned to them. Keyrings can be assigned to multiple clients.
-interface <netdevice>	**-in**	Specifies the network device to bind **admin** or **crypto** network traffic to. Valid values: **eth0**, **eth1**, **eth2**, **eth3**, **bond0**, **bond1**, **all**
-identity <mode>	**-id**	Specifies the identity mode to use for the cluster. Valid Values: **single**, **dual** > **Single-Identity Mode** (default): In this mode, the KRSO and KRCO roles on each keyring are intended to be held by the same individual, and use the same password. When the password for one role is changed, the change is applied to the other role as well. > **Dual-Identity Mode**: In this mode, the KRSO and KRCO roles on each keyring use separate passwords, and this separation is enforced using the same rules as standard Luna application partitions. This mode is required if you are migrating keys from standard Luna partitions to keyrings.
-ipaddress <ipaddress>	**-ip**	Specifies the IP address to use for the core cluster traffic. The IP specified for the **core** traffic must be the same IP address as one of the appliance's network interfaces.

Argument(s)	Shortcut	Description
-port <port>	**-p**	Specifies the port to use for this type of traffic. Valid values: > **admin** service (default: **50070**): **50075-50079** > **crypto** service (default: **50052**): **50055-50059** **CAUTION!** In this release, changing the default port used for crypto operations on the cluster (**50052**) can cause communication problems between cluster members. Refer to known issue LUNA-26485.
-service <service>	**-s**	Specifies the type of network traffic to configure. Valid values: **core**, **admin**, **crypto**

Example

```
lunash:>cluster config set -service core -ipaddress 1.2.3.4 -identity dual -clientAssignment
manual


Command Result : 0 (Success)
```

cluster config show

Display the configured settings for the cluster.

> **NOTE** Thales requires minimum Luna Appliance Software 7.8.5 with the lnh_cluster-1.0.4 package, Luna HSM Firmware 7.8.4, and Luna HSM Client 10.7.2 to use clusters in production environments, or minimum Luna Appliance Software 7.9.0 with the lnh_cluster-1.0.5 package, Luna HSM Firmware 7.8.4, and Luna HSM Client 10.8.0 to migrate keys from Luna application partitions.

REST API: GET /api/cluster/config

User Privileges

Users with the following privileges can perform this command:

- Admin
- Operator
- Monitor

Syntax

cluster config show

Example

```
lunash:>cluster config show


core service
               IP address: 1.2.3.4
            Identity Mode: dual
   Client Assignment Mode: auto
crypto service
       interface:  all
            port:  50052
admin service
       interface:  all
            port:  50070

Command Result : 0 (Success)
```

cluster create

Create a new cluster on the appliance. Do not create more than one cluster.

> **NOTE** Thales requires minimum Luna Appliance Software 7.8.5 with the lnh_cluster-1.0.4 package, Luna HSM Firmware 7.8.4, and Luna HSM Client 10.7.2 to use clusters in production environments, or minimum Luna Appliance Software 7.9.0 with the lnh_cluster-1.0.5 package, Luna HSM Firmware 7.8.4, and Luna HSM Client 10.8.0 to migrate keys from Luna application partitions.

REST API: POST /api/clusters

User Privileges

Users with the following privileges can perform this command:

> Admin

Syntax

cluster create -label <label> [**-password** <password>]

Argument(s)	Shortcut	Description
-label	**-l**	Specifies the label to assign to the cluster.
-password	**-p**	The HSM SO password. If this option is omitted on a password-authenticated HSM, LunaSH prompts for the password. If this option is included on a multifactor quorum-authenticated HSM, it is ignored.

Example

```
lunash:>cluster create -label cluster01 -password iamtheHSMSO

Cluster was created with UUID: ac2a0f56-626e-4c91-a379-489b789a47e7

Command Result : 0 (Success)
```

cluster delete

Delete the cluster on the appliance.

> **NOTE** Thales requires minimum Luna Appliance Software 7.8.5 with the lnh_cluster-1.0.4 package, Luna HSM Firmware 7.8.4, and Luna HSM Client 10.7.2 to use clusters in production environments, or minimum Luna Appliance Software 7.9.0 with the lnh_cluster-1.0.5 package, Luna HSM Firmware 7.8.4, and Luna HSM Client 10.8.0 to migrate keys from Luna application partitions.

> **CAUTION!** If the cluster being deleted is registered to any clients, you must also delete the cluster's information from the client's configuration file (see Removing a Cluster From the Luna HSM Client).

REST API: DELETE /api/clusters/{clusterID}

User Privileges

Users with the following privileges can perform this command:

> Admin

Syntax

cluster delete -clusterid <string> [**-password** <password>] [**-reset**] [**-force**]

Argument(s)	Shortcut	Description
-clusterid	**-c**	Specifies the UUID for the cluster to be deleted.
-force	**-f**	Delete the cluster without asking for confirmation.
-password	**-p**	The HSM SO password. If this option is omitted on a password-authenticated HSM, LunaSH prompts for the password. If this option is included on a multifactor quorum-authenticated HSM, it is ignored.

Argument(s)	Shortcut	Description
-reset	**-r**	Also delete the **cluster** service core IP address and the cluster certificate. If this option is specified, you must complete the procedure for Configuring the Luna Network HSM 7 for Clustering again on this appliance. If **-reset** is not specified, you can create a new cluster or join an existing one after starting the **cluster** service.

Example

```
lunash:>cluster delete -clusterid ac2a0f56-626e-4c91-a379-489b789a47e7 -password iamtheHSMSO

WARNING: This operation will delete the Cluster !!!

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

proceed
Proceeding...

Cluster ac2a0f56-626e-4c91-a379-489b789a47e7 was sucessfully deleted.

Command Result : 0 (Success)
```

cluster disable

Stop and disable the **cluster** service. If the service is disabled, it will not restart automatically.

> **NOTE** Thales requires minimum Luna Appliance Software 7.8.5 with the lnh_cluster-1.0.4 package, Luna HSM Firmware 7.8.4, and Luna HSM Client 10.7.2 to use clusters in production environments, or minimum Luna Appliance Software 7.9.0 with the lnh_cluster-1.0.5 package, Luna HSM Firmware 7.8.4, and Luna HSM Client 10.8.0 to migrate keys from Luna application partitions.

REST API: PATCH /api/lunasa/services/{serviceid}

User Privileges

Users with the following privileges can perform this command:

- Admin
- Operator

Syntax

cluster disable [**-force**]

Argument(s)	Shortcut	Description
-force	**-f**	Disable the **cluster** service without asking for confirmation.

Example

```
lunash:>cluster disable

WARNING: This operation will stop and disable Cluster Service!!!

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

> proceed
Proceeding...


Command Result : 0 (Success)
```

cluster enable

Enables and starts the **cluster** service. When enabled, the service will restart automatically if it is interrupted.

> **NOTE** Thales requires minimum Luna Appliance Software 7.8.5 with the lnh_cluster-1.0.4 package, Luna HSM Firmware 7.8.4, and Luna HSM Client 10.7.2 to use clusters in production environments, or minimum Luna Appliance Software 7.9.0 with the lnh_cluster-1.0.5 package, Luna HSM Firmware 7.8.4, and Luna HSM Client 10.8.0 to migrate keys from Luna application partitions.

REST API: PATCH /api/lunasa/services/{serviceid}

User Privileges

Users with the following privileges can perform this command:

- Admin
- Operator

REST API Equivalent

To perform this operation with the Luna REST API, use the following endpoint(s):

Syntax

cluster enable [**-force**]

Argument(s)	Shortcut	Description
-force	**-f**	Enable the **cluster** service without asking for confirmation.

Example

```
lunash:>cluster enable

WARNING: This operation will enable Cluster Service!!!

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

> proceed
Proceeding...


Command Result : 0 (Success)
```

cluster group list

Display a list of affinity groups that have been created within the cluster.

> **NOTE** Thales requires minimum Luna Appliance Software 7.8.5 with the lnh_cluster-1.0.4 package, Luna HSM Firmware 7.8.4, and Luna HSM Client 10.7.2 to use clusters in production environments, or minimum Luna Appliance Software 7.9.0 with the lnh_cluster-1.0.5 package, Luna HSM Firmware 7.8.4, and Luna HSM Client 10.8.0 to migrate keys from Luna application partitions.

REST API: GET /api/clusters/{clusterID}/groups

User Privileges

Users with the following privileges can perform this command:

- Admin
- Operator
- Monitor

Syntax

cluster group list

Argument(s)	Shortcut	Description
-clusterid <UUID>	**-c**	Specifies the UUID of the cluster to display affinity groups for.

Example

```
cluster group list -clusterid ac2a0f56-626e-4c91-a379-489b789a47e7


Group Name                        Group ID
----------------------------------------------------------------------
```

```
local                           0e9c2511-582b-4127-81dc-c2d332c83e31
remote1                         915e7272-6d02-43c4-abeb-89493a215fa2
remote2                         b23209c7-4b86-4ffa-8a7b-927e58cad664
```

cluster join

Join an existing cluster created on another Luna Network HSM 7. Both appliances must be configured with the same identity mode (**single** or **dual**; see Keyring Roles and Identity Modes) and client assignment mode (**auto** or **manual**; see Client Assignment Modes).

> **NOTE** Thales requires minimum Luna Appliance Software 7.8.5 with the lnh_cluster-1.0.4 package, Luna HSM Firmware 7.8.4, and Luna HSM Client 10.7.2 to use clusters in production environments, or minimum Luna Appliance Software 7.9.0 with the lnh_cluster-1.0.5 package, Luna HSM Firmware 7.8.4, and Luna HSM Client 10.8.0 to migrate keys from Luna application partitions.

> **CAUTION!** If the join process is interrupted due to a network disruption, an incomplete join state can result. If this happens, contact Thales Customer Support for recovery procedures.

REST API: PUT /api/clusters/{clusterID}

User Privileges

Users with the following privileges can perform this command:

> Admin

Syntax

cluster join -clusterid <string> **-clusteripaddress** <ipaddress> **-remotepassword** <password> **-partition** <label> [**-copassword** <password>] [**-force**]

Argument(s)	Shortcut	Description
-clusterid		Specifies the ID of the cluster to join.
-clusteripaddress	**-clusterip**	Specifies the IP address of the appliance whose cluster will be joined.
-copassword	**-co**	Specifies the Crypto Officer password for the cluster partition. If this option is omitted on a password-authenticated HSM, LunaSH prompts for the password. If this option is included on a multifactor quorum-authenticated HSM and the partition is not activated, it is ignored.
-force	**-f**	Join the cluster without asking for confirmation.

Argument(s)	Shortcut	Description
-partition	**-p**	Specifies the label of the cluster partition.
-remotepassword	**-r**	Specifies the **admin** user password for the appliance whose cluster will be joined.

Example

```
lunash:>cluster join -clusterid ac2a0f56-626e-4c91-a379-489b789a47e7 -clusterip 1.2.3.4 -
remotepassword IamtheAdmin -partition localpar -co IamtheCO -force

Step 1/2: Executing initial 'join Cluster' request...
Step 2/2: Setting cluster data and restarting service

Command Result : 0 (Success)
```

cluster leave

Remove a Luna Network HSM 7 appliance from a cluster. This action must be performed on the local member and it is not possible to remove a non-local member from the cluster. If the member you want to remove is unreachable, use "cluster member delete" on page 147.

> **NOTE** Thales requires minimum Luna Appliance Software 7.8.5 with the lnh_cluster-1.0.4 package, Luna HSM Firmware 7.8.4, and Luna HSM Client 10.7.2 to use clusters in production environments, or minimum Luna Appliance Software 7.9.0 with the lnh_cluster-1.0.5 package, Luna HSM Firmware 7.8.4, and Luna HSM Client 10.8.0 to migrate keys from Luna application partitions.

REST API: PATCH /api/clusters/{clusterID}/members/{memberID}

User Privileges

Users with the following privileges can perform this command:

> Admin

Syntax

cluster leave -memberid <string> **-partition** <label> [**-copassword** <password>] [**-force**]

Argument(s)	Shortcut	Description
-memberid	**-m**	Specifies the ID of the member leaving the cluster.

Argument(s)	Shortcut	Description
-copassword	**-co**	Specifies the Crypto Officer password for the cluster partition. If this option is omitted on a password-authenticated HSM, LunaSH prompts for the password. If this option is included on a multifactor quorum-authenticated HSM and the partition is not activated, it is ignored.
-force	**-f**	Leave the cluster without asking for confirmation.
-partition	**-p**	Specifies the label of the cluster partition.

Example

```
lunash:>cluster leave -memberid ecb8f151-8184-412d-840a-6cd15e8ffb36 -partition localpar -co
IamtheCO -force

Step 1/2: Executing initial 'leave Cluster' request...
Step 2/2: Clearing cluster data and restarting service

Command Result : 0 (Success)
```

cluster list

Display the name and ID of the cluster.

> **NOTE** Thales requires minimum Luna Appliance Software 7.8.5 with the lnh_cluster-1.0.4 package, Luna HSM Firmware 7.8.4, and Luna HSM Client 10.7.2 to use clusters in production environments, or minimum Luna Appliance Software 7.9.0 with the lnh_cluster-1.0.5 package, Luna HSM Firmware 7.8.4, and Luna HSM Client 10.8.0 to migrate keys from Luna application partitions.

REST API: GET /api/clusters

User Privileges

Users with the following privileges can perform this command:

- Admin
- Operator
- Monitor

Syntax

cluster list

Example

```
lunash:>cluster list

Name                              ID
--------------------------------------------------------------------------------
cluster00                         ac2a0f56-626e-4c91-a379-489b789a47e7

Command Result : 0 (Success)
```

cluster member

Access commands to get information about the members of a cluster, or manually authorize the local member to create keyrings and objects on the cluster.

> **NOTE** Thales requires minimum Luna Appliance Software 7.8.5 with the lnh_cluster-1.0.4 package, Luna HSM Firmware 7.8.4, and Luna HSM Client 10.7.2 to use clusters in production environments, or minimum Luna Appliance Software 7.9.0 with the lnh_cluster-1.0.5 package, Luna HSM Firmware 7.8.4, and Luna HSM Client 10.8.0 to migrate keys from Luna application partitions.

Syntax

cluster member

authorize
config
delete
list
partition
show

Argument(s)	Shortcut	Description
authorize	**a**	Authorize the specified cluster member to create objects on the cluster's keyrings. See "cluster member authorize" on the next page.
config	**c**	Move the specified member to a different affinity group, or promote it to the primary cluster member. See "cluster member config" on page 146.
delete	**d**	Delete an unrecoverable member from the cluster. This command can be run on any member of the cluster. See "cluster member delete" on page 147.
list	**l**	Display a list of members on the cluster and their member IDs. See "cluster member list" on page 148.

Argument(s)	Shortcut	Description
show	**s**	Display information about a specified cluster member. See "cluster member show" on page 156.

cluster member authorize

Authorize the specified cluster member to create objects on the cluster's keyrings.

> **NOTE** Thales requires minimum Luna Appliance Software 7.8.5 with the lnh_cluster-1.0.4 package, Luna HSM Firmware 7.8.4, and Luna HSM Client 10.7.2 to use clusters in production environments, or minimum Luna Appliance Software 7.9.0 with the lnh_cluster-1.0.5 package, Luna HSM Firmware 7.8.4, and Luna HSM Client 10.8.0 to migrate keys from Luna application partitions.

Manual member authorization is required only:

- to authorize the first member of a new cluster
- to authorize the only member of a single-member cluster that has rebooted or recovered
- to authorize the first member of a cluster where *all* members rebooted or recovered

In a cluster where at least one member remains active and connected, new and rejoining members automatically take their authorization from that member, and manual re-authorization is not required.

REST API: PUT /api/clusters/{clusterID}/members/{memberID}

User Privileges

Users with the following privileges can perform this command:

- Admin

Syntax

cluster member authorize -partition <name> [**-copassword** <password>] [**-memberid** <string>]

Argument(s)	Shortcut	Description
-copassword	**-c**	The cluster partition Crypto Officer password. If this option is omitted on a password-authenticated HSM, LunaSH prompts for the password. If this option is included on a multifactor quorum-authenticated HSM and the partition is not activated, it is ignored.
-memberid	**-m**	Specifies the member ID to be authorized. See "cluster member list" on page 148.
-partition	**-p**	Specifies the label of the cluster partition.

Example

```
lunash:>>cluster member authorize -memberid ecb8f151-8184-412d-840a-6cd15e8ffb36 -partition
clusterpar -copassword IamtheCO

Success

Command Result : 0 (Success)
```

cluster member config

Move the specified member to a different affinity group, or promote it to the primary cluster member.

> **NOTE** Thales requires minimum Luna Appliance Software 7.8.5 with the lnh_cluster-1.0.4 package, Luna HSM Firmware 7.8.4, and Luna HSM Client 10.7.2 to use clusters in production environments, or minimum Luna Appliance Software 7.9.0 with the lnh_cluster-1.0.5 package, Luna HSM Firmware 7.8.4, and Luna HSM Client 10.8.0 to migrate keys from Luna application partitions.

REST API: PUT /api/clusters/{clusterID}/members/{memberID}

User Privileges

Users with the following privileges can perform this command:

> Admin

Syntax

cluster member config -memberid <string> {**-group** <name> | **-primary**}

Argument(s)	Shortcut	Description
-group <name>	**-g**	Move the specified member from its current affinity group to the specified group. If the group does not already exist, a new group is created with the specified name.
-memberid <UUID>	**-m**	Specifies the member ID to be switched. See "cluster member list" on page 148.
-primary	**-p**	Promote the specified member to be the primary cluster member.

Example

```
lunash:>cluster member config -memberid ecb8f151-8184-412d-840a-6cd15e8ffb36 -primary

Success

Command Result : 0 (Success)
```

cluster member delete

Delete an unrecoverable member from the cluster. This command can be run on any member of the cluster. After running this command, you must factory reset the **cluster** service on the deleted member before attempting to rejoin the cluster (see "sysconf config factoryReset" on page 543).

> **NOTE** Thales requires minimum Luna Appliance Software 7.8.5 with the lnh_cluster-1.0.4 package, Luna HSM Firmware 7.8.4, and Luna HSM Client 10.7.2 to use clusters in production environments, or minimum Luna Appliance Software 7.9.0 with the lnh_cluster-1.0.5 package, Luna HSM Firmware 7.8.4, and Luna HSM Client 10.8.0 to migrate keys from Luna application partitions.

REST API: DELETE /api/clusters/{clusterID}/members/{memberID}

User Privileges

Users with the following privileges can perform this command:

> Admin

Syntax

cluster member delete -memberid <UUID> [**-copassword** <password>] [**-force**]

Argument(s)	Shortcut	Description
-copassword	**-c**	The local member's cluster partition Crypto Officer password. If this option is omitted on a password-authenticated HSM, LunaSH prompts for the password. If this option is included on a multifactor quorum-authenticated HSM and the partition is not activated, it is ignored.
-force	**-f**	Delete the specified member without asking for confirmation.
-memberid	**-m**	Specifies the member ID to be deleted. See "cluster member list" on the next page.

Example

```
lunash:>cluster member delete -memberid ecb8f151-8184-412d-840a-6cd15e8ffb36 -copassword
IamtheCO -f

Success

Command Result : 0 (Success)
```

cluster member list

Display a list of members on the cluster and their member IDs. The following flags indicate each member's status in the cluster:

> *****: The local member, where you have logged in to LunaSH

> **P**: The primary member of the cluster (see The Primary Member)

> **R**: The **cluster** service on this member has been flagged for automatic recovery and will soon restart.

> **x**: This member is not visible to the local member. There may be a network disruption or another issue.

> **A**: This member is authorized (lnh_cluster-1.0.4 or newer).

> **NOTE** Thales requires minimum Luna Appliance Software 7.8.5 with the lnh_cluster-1.0.4 package, Luna HSM Firmware 7.8.4, and Luna HSM Client 10.7.2 to use clusters in production environments, or minimum Luna Appliance Software 7.9.0 with the lnh_cluster-1.0.5 package, Luna HSM Firmware 7.8.4, and Luna HSM Client 10.8.0 to migrate keys from Luna application partitions.

REST API: GET /api/clusters/{clusterID}/members

User Privileges

Users with the following privileges can perform this command:

> Admin

> Operator

> Monitor

Syntax

cluster member list -clusterid <UUID>

Argument(s)	Shortcut	Description
-clusterid <UUID>	**-c**	Specifies the UUID of the cluster to display members for.

Example -- lnh_cluster 1.0.4 or Newer

```
lunash:>cluster member list -clusterid c41d1483-c4a4-4b20-9f5c-0867871641af


State Name                            ID                                   Group

------------------------------------------------------------------------------------------------
-------------
*P  A LNH-599477                      18de8f48-1c5e-4e3f-a899-a0e48c5d2ccb local

    A LNH-532018                      91ae1281-8cc6-489e-97a5-8b2885057a72 local
```

Example -- lnh_cluster 1.0.3 or Older

```
lunash:>cluster member list -clusterid ac2a0f56-626e-4c91-a379-489b789a47e7


     Name                            Authorized Group      ID
-----------------------------------------------------------------------------------------------
*    LNH-532018                      Yes        local      91ae1281-8cc6-489e-97a5-
8b2885057a72
 P   LNH-66331                       Yes        local      7d5b53d9-57fb-41de-b97c-
95cc6ab41a3c

Command Result : 0 (Success)
```

cluster member partition migration

Access commands that allow you to migrate keys from Luna application partitions to Luna keyrings on the cluster.

> **NOTE** These commands require minimum Luna Appliance Software 7.9.0 with the lnh_cluster-1.0.5 package installed.
>
> Thales requires minimum Luna Appliance Software 7.8.5 with the lnh_cluster-1.0.4 package, Luna HSM Firmware 7.8.4, and Luna HSM Client 10.7.2 to use clusters in production environments, or minimum Luna Appliance Software 7.9.0 with the lnh_cluster-1.0.5 package, Luna HSM Firmware 7.8.4, and Luna HSM Client 10.8.0 to migrate keys from Luna application partitions.

Syntax

cluster member partition migration

begin
end

Argument(s)	Shortcut	Description
begin	**b**	Begin the process of migrating keys from Luna application partitions to Luna keyrings. See "cluster member partition migration begin" below.
end	**e**	End the migration progress. See "cluster member partition migration end" on page 151.

cluster member partition migration begin

This command begins the process of migrating keys from Luna application partitions to Luna keyrings.

CAUTION! This overwrites the existing SMK on the migrating partition. If any important key material is backed up/encrypted using the old SMK, it will be unrecoverable unless you have a backup of the SMK. This includes cryptographic blobs backed up to a Luna Backup HSM. Refer to Partition Backup and Restore for more information.

NOTE This command requires minimum Luna Appliance Software 7.9.0 with the lnh_cluster-1.0.5 package installed.

Thales requires minimum Luna Appliance Software 7.8.5 with the lnh_cluster-1.0.4 package, Luna HSM Firmware 7.8.4, and Luna HSM Client 10.7.2 to use clusters in production environments, or minimum Luna Appliance Software 7.9.0 with the lnh_cluster-1.0.5 package, Luna HSM Firmware 7.8.4, and Luna HSM Client 10.8.0 to migrate keys from Luna application partitions.

REST API: PUT /api/clusters/{clusterID}/member/partitions/{partitionID}/migration

User Privileges

Users with the following privileges can perform this command:

> Admin

Syntax

cluster member partition migration begin -partitionid <UUID> [**-copassword** <password>] [**-popassword** <password>] [**-clusterco** <password>] [**-clusterpo** <password>] [**-force**]

Argument(s)	Shortcut	Description
-clusterco <password>	**-clusterc**	Specifies the Crypto Officer password for the cluster partition. If this option is not included, LunaSH prompts you to enter it.
-clusterpo <password>	**-clusterp**	Specifies the Partition SO password for the cluster partition. If this option is not included, LunaSH prompts you to enter it.
-copassword <password>	**-co**	Specifies the Crypto Officer password for the migrating partition. If this option is not included, LunaSH prompts you to enter it.
-force	**-f**	Begin the migration process without prompting for confirmation.
-partitionid <UUID>	**-pa**	Specifies the UUID of the migrating partition. See cluster member partition list.
-popassword <password>	**-po**	Specifies the Partition SO password for the migrating partition. If this option is not included, LunaSH prompts you to enter it.

Example

```
lunash:>cluster member partition migration begin -partitionid f66b649a-af1e-402b-8408-
8acfb21e06f5

Please enter the Migrating Partition CO password:
  > ********

Please enter the Migrating Partition PO password:
  > ********

Please enter the Cluster Partition CO password:
  > ********

Please enter the Cluster Partition PO password:
  > ********

WARNING !!  This operation will result in the migrating partition's current SMK to
            be overwritten. It will not be recoverable. Please ensure it has been
            backed up before proceeding.
If you are sure that you wish to proceed, then type 'proceed', otherwise type 'quit'

> proceed
Proceeding...

Success

Command Result : 0 (Success)
```

cluster member partition migration end

This command ends the migration process from Luna application partitions to Luna keyrings on the cluster.

> **NOTE** This command requires minimum Luna Appliance Software 7.9.0 with the lnh_cluster-1.0.5 package installed.
>
> Thales requires minimum Luna Appliance Software 7.8.5 with the lnh_cluster-1.0.4 package, Luna HSM Firmware 7.8.4, and Luna HSM Client 10.7.2 to use clusters in production environments, or minimum Luna Appliance Software 7.9.0 with the lnh_cluster-1.0.5 package, Luna HSM Firmware 7.8.4, and Luna HSM Client 10.8.0 to migrate keys from Luna application partitions.

REST API: PUT /api/clusters/{clusterID}/member/partitions/{partitionID}/migration

User Privileges

Users with the following privileges can perform this command:

> Admin

Syntax

cluster member partition migration end-partitionid <UUID> [**-copassword** <password>] [**-force**]

Argument(s)	Shortcut	Description
-copassword <password>	**-co**	Specifies the Crypto Officer password for the migrating partition.
-force	**-f**	End the migration process without prompting for confirmation.
-partitionid <UUID>	**-pa**	Specifies the UUID of the partition that was migrated. See cluster member partition list.

Example

```
lunash:>cluster member partition migration end -partitionid 50ef5563-eacd-4118-8486-
d52f38c8389a

Please enter the Migrating Partition CO password:
  > ********

WARNING !!  This operation will end the migration process for the migrating partition by
            removing the cluster SMK from it.
If you are sure that you wish to proceed, then type 'proceed', otherwise type 'quit'

> proceed
Proceeding...

Success

Command Result : 0 (Success)
```

cluster member partition object

Access commands to list objects on an eligible application partition, or migrate objects from that partition to a Luna keyring.

> **NOTE** These commands require minimum Luna Appliance Software 7.9.0 with the lnh_cluster-1.0.5 package installed.
>
> Thales requires minimum Luna Appliance Software 7.8.5 with the lnh_cluster-1.0.4 package, Luna HSM Firmware 7.8.4, and Luna HSM Client 10.7.2 to use clusters in production environments, or minimum Luna Appliance Software 7.9.0 with the lnh_cluster-1.0.5 package, Luna HSM Firmware 7.8.4, and Luna HSM Client 10.8.0 to migrate keys from Luna application partitions.

Syntax

cluster member partition object

assign
list

Argument(s)	Shortcut	Description
assign	**a**	This command allows you to select objects to migrate from an eligible Luna application partition to a Luna keyring. See "cluster member partition object assign" below.
list	**l**	This command displays a list of objects on an eligible application partition that are ready to migrate to a Luna keyring. See "cluster member partition object list" on the next page.

cluster member partition object assign

This command allows you to select objects to migrate from an eligible Luna application partition to a Luna keyring.

> **NOTE** This command requires minimum Luna Appliance Software 7.9.0 with the lnh_cluster-1.0.5 package installed.
>
> Thales requires minimum Luna Appliance Software 7.8.5 with the lnh_cluster-1.0.4 package, Luna HSM Firmware 7.8.4, and Luna HSM Client 10.7.2 to use clusters in production environments, or minimum Luna Appliance Software 7.9.0 with the lnh_cluster-1.0.5 package, Luna HSM Firmware 7.8.4, and Luna HSM Client 10.8.0 to migrate keys from Luna application partitions.

REST API: PUT /api/cluster/member/partitions/{partitionID}/objects

User Privileges

Users with the following privileges can perform this command:

> Admin

Syntax

cluster member partition object assign -partitionid <UUID> **-keyringrid** <UUID> {**-objectid** <OUID(s)> | **-filename** <filename>} [**-copassword** <password>] [**-keyringcopassword** <password>]

Argument(s)	Shortcut	Description
-copassword <password>	**-c**	Specifies the Crypto Officer password for the migrating partition.
-filename <filename>	**-f**	Specifies the name of the file containing the list of object OUIDs to be migrated. The file must be stored in the LunaSH user's files on the appliance (see lunash:> "my file list" on page 306).
-keyringcopassword <password>	**-keyringc**	Specifies the Keyring Crypto Officer password for the target keyring.

Argument(s)	Shortcut	Description
-keyringid <UUID>	**-keyringi**	Specifies the UUID of the target keyring.
-objectID <OUID>	**-o**	A colon-separated (**:**) list of object OUIDs to migrate to the keyring. You can specify up to 10 OUIDs with this option.
-partitionid <UUID>	**-p**	Specifies the UUID of the migrating partition.

Example

```
lunash:>cluster member partition object assign -partitionid 50ef5563-eacd-4118-8486-
d52f38c8389a -keyringid 14feaa24-53df-43d9-9457-2d53519e3f46 -filename migrate_keys

Please enter the Partition CO password:
  > ********

Please enter the Keyring CO password:
  > ********

Success

Command Result : 0 (Success)
```

cluster member partition object list

This command displays a list of objects on an eligible application partition that are ready to migrate to a Luna keyring.

> **NOTE** This command requires minimum Luna Appliance Software 7.9.0 with the lnh_cluster-1.0.5 package installed.
>
> Thales requires minimum Luna Appliance Software 7.8.5 with the lnh_cluster-1.0.4 package, Luna HSM Firmware 7.8.4, and Luna HSM Client 10.7.2 to use clusters in production environments, or minimum Luna Appliance Software 7.9.0 with the lnh_cluster-1.0.5 package, Luna HSM Firmware 7.8.4, and Luna HSM Client 10.8.0 to migrate keys from Luna application partitions.

REST API: GET /api/cluster/member/partitions/{partitionID}/objects

User Privileges

Users with the following privileges can perform this command:

- Admin
- Operator
- Monitor

Syntax

cluster member partition object list -partitionid <string> [**-memberid** <string>] [**-copassword** <password>] [**-startIndex** <number>] [**-maxEntries** <number>]

Argument(s)	Shortcut	Description
-copassword <password>	**-c**	Specifies the Crypto Officer password for the migrating partition.
-maxEntries <number>	**-ma**	Specifies the number of objects to include in the list. If this option is not included, all objects on the partition are listed. Valid Values: **1-4294967295**
-memberid <UUID>	**-me**	Specifies the UUID of the member that hosts the partition to be migrated. If this option is not included, the partition must be hosted on the local member appliance.
-partitionid <UUID>	**-p**	Specifies the UUID of the partition to be migrated.
-startIndex <number>	**-s**	Specifies the index position of the object to begin listing from. If this option is not included, the list begins with the object in position 0. Valid Values: **1-4294967295**

Example

```
lunash:>cluster member partition object list -partitionid db7e4518-8ed7-4750-b5d1-cb2baecaa22a

Please enter the Partition CO password:
  > ********

Starting index: 0 Maximum Entries Requested: ALL Total Entries Returned: 8 Total Objects in
Partition: 8

Label                            OUID                                Object Type
       Keyring Label
-------------------------------------------------------------------------------------------------
----------------------------------------
MT RSA 256-bit Private KeyGen    b40000001d0000011b030100            Private Key
       N/A
MT RSA 256-bit Public KeyGen     b30000001d0000011b030100            Public Key
       N/A
MT RSA 256-bit Private KeyGen    b20000001d0000011b030100            Private Key
       N/A
MT RSA 256-bit Public KeyGen     b10000001d0000011b030100            Public Key
       N/A
MT RSA 4096-bit Private KeyGen   5e1a00001d0000011b030100            Private Key
       myLunaKeyring
MT RSA 4096-bit Public KeyGen    5d1a00001d0000011b030100            Public Key
       myLunaKeyring
MT RSA 4096-bit Private KeyGen   5c1a00001d0000011b030100            Private Key
       myLunaKeyring
MT RSA 4096-bit Public KeyGen    5b1a00001d0000011b030100            Public Key
       myLunaKeyring
```

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

> **NOTE** Under the **Keyring Label** column, **N/A** indicates that the object has not yet been migrated to a keyring. Otherwise, the label of the keyring that received this migrated object is displayed.

cluster member show

Display information about a specified cluster member.

> **NOTE** Thales requires minimum Luna Appliance Software 7.8.5 with the lnh_cluster-1.0.4 package, Luna HSM Firmware 7.8.4, and Luna HSM Client 10.7.2 to use clusters in production environments, or minimum Luna Appliance Software 7.9.0 with the lnh_cluster-1.0.5 package, Luna HSM Firmware 7.8.4, and Luna HSM Client 10.8.0 to migrate keys from Luna application partitions.

REST API: GET /api/clusters/{clusterID}/members/{memberID}

User Privileges

Users with the following privileges can perform this command:

- Admin
- Operator
- Monitor

Syntax

cluster member show -memberid <string> [**-detail**]

Argument(s)	Shortcut	Description
-detail	**-d**	Include this option to display details of the certificates associated with the cluster. This option requires Luna Appliance Software 7.9.0 or newer with lnh_cluster-1.0.5 or newer installed.
-memberid <string>	**-m**	Specifies the ID of the member to display information about.

Examples

```
lunash:>cluster member show -memberid ecb8f151-8184-412d-840a-6cd15e8ffb36

Member Label:   LNH-999999

Member ID:      ecb8f151-8184-412d-840a-6cd15e8ffb36
```

```
IP:             1.2.3.4
Member Group:   local
SW Version:
Status:
             Authorized: True
                Primary: True
                  Local: True
                Visible: True
                   Mode: Read-Write
Restart Cluster service: False

Command Result : 0 (Success)


lunash:>cluster member show -memberid 0343262c-1dac-4426-9af1-22070426aa07 -detail

Member Label:   LNH-999999
Member ID:      0343262c-1dac-4426-9af1-22070426aa07
IP:             1.2.3.4
Service IP:     1.2.3.4
Member Group:   local
SW Version:
                Cluster: 1.0.5-166869
           IS Migration: not installed
Status:
             Authorized: True
                Primary: True
                  Local: True
                Visible: True
                   Mode: Read-Write
Restart Cluster service: False

Certificate:
service: grpc
    Fingerprint SHA256:
27:BB:94:B4:89:3D:46:75:C4:E4:7D:75:F9:71:06:FB:87:A3:23:98:CE:54:B9:5B:06:F0:B9:89:5A:5D:73:8A
    Start Date: Feb  8 03:24:05 2025 GMT
    End Date: Feb  6 03:24:05 2035 GMT
    Ciphers: TLS_AES_256_GCM_SHA384, TLS_CHACHA20_POLY1305_SHA256, TLS_AES_128_GCM_SHA256
service: database
    Fingerprint SHA256:
05:F9:42:9E:E4:88:51:22:2C:40:E3:89:E3:D2:23:8B:36:93:43:32:10:14:F9:97:2D:BD:28:AD:42:61:DA:3D
    Start Date: Feb  8 03:24:07 2025 GMT
    End Date: Feb  6 03:24:07 2035 GMT
    Ciphers: ECDHE-ECDSA-AES256-GCM-SHA384, ECDHE-ECDSA-CHACHA20-POLY1305, ECDHE-ECDSA-AES128-
GCM-SHA256, ECDHE-ECDSA-AES256-SHA384, ECDHE-ECDSA-AES128-SHA256, ECDHE-ECDSA-AES256-SHA,
ECDHE-ECDSA-AES128-SHA, TLS_AES_256_GCM_SHA384, TLS_CHACHA20_POLY1305_SHA256, TLS_AES_128_GCM_
SHA256
service: rest
    Fingerprint SHA256:
B1:B5:5F:D1:A6:BB:61:DD:A9:17:BA:C1:64:70:2B:BC:CE:AA:9A:8B:5A:D9:38:4F:A7:33:3A:88:98:0F:C8:BE
    Start Date: Feb  8 03:24:08 2025 GMT
    End Date: Feb  6 03:24:08 2035 GMT
    Ciphers: ECDHE-ECDSA-AES256-GCM-SHA384, ECDHE-ECDSA-AES128-GCM-SHA256, TLS_AES_256_GCM_
SHA384, TLS_CHACHA20_POLY1305_SHA256, TLS_AES_128_GCM_SHA256
service: messaging
    Fingerprint SHA256:
7C:A5:0C:67:5C:4A:60:1E:69:F8:5B:A2:9C:A0:18:68:E1:F3:5F:79:07:24:45:5C:A8:BA:5D:DD:C0:B0:BB:D8
    Start Date: Feb  8 03:24:03 2025 GMT
```

```
    End Date: Feb  6 03:24:03 2035 GMT
    Ciphers: TLS_AES_256_GCM_SHA384, TLS_CHACHA20_POLY1305_SHA256, TLS_AES_128_GCM_SHA256

Command Result : 0 (Success)
```

cluster restore

Access commands to restore keyrings to a cluster from backup.

> **NOTE** Thales requires minimum Luna Appliance Software 7.8.5 with the lnh_cluster-1.0.4 package, Luna HSM Firmware 7.8.4, and Luna HSM Client 10.7.2 to use clusters in production environments, or minimum Luna Appliance Software 7.9.0 with the lnh_cluster-1.0.5 package, Luna HSM Firmware 7.8.4, and Luna HSM Client 10.8.0 to migrate keys from Luna application partitions.

Syntax

cluster restore

run
show

Argument(s)	Shortcut	Description
run	**r**	Run a cluster or keyring restore operation on demand. See "cluster restore run" below.
show	**s**	Display the status of a restore operation, and the restore history. See "cluster restore show" on page 160.

cluster restore run

Run a cluster restore operation on demand. This command does not restore the cluster SMK (see The Cluster Partition). Refer to Backing Up/Restoring the Partition SMK for this procedure.

> **NOTE** Thales requires minimum Luna Appliance Software 7.8.5 with the lnh_cluster-1.0.4 package, Luna HSM Firmware 7.8.4, and Luna HSM Client 10.7.2 to use clusters in production environments, or minimum Luna Appliance Software 7.9.0 with the lnh_cluster-1.0.5 package, Luna HSM Firmware 7.8.4, and Luna HSM Client 10.8.0 to migrate keys from Luna application partitions.

Backup and restore operations can only be done on the primary member of the cluster. Stop the **cluster** service on all non-primary members of the cluster before you begin the restore operation:

lunash:> **"service stop" on page 471 cluster**

NOTE

> Using lnh_cluster-1.0.5 and newer, backups can be restored only to a cluster configured in the same identity mode as the backup (see Keyring Roles and Identity Modes). Attempts to restore a backup taken from a single-identity cluster to a dual-identity cluster, or vice-versa, will fail. If you have configured the cluster in dual-identity mode, it is therefore impossible to restore a backup made from an earlier **lnh_cluster** version.

> Using lnh_cluster-1.0.5 and newer, you may restore keyrings to a cluster configured in a different client assignment mode than the backup (see Client Assignment Modes). Client assignment information is not included in the backup file, so if you restore to a new or factory-reset cluster in **manual** assignment mode, you must assign keyrings to clients again. If you are restoring to a cluster that already has keyrings assigned to clients, those assignments are preserved when the keyrings are restored.

> Keyrings on the target cluster have their configuration (roles, passwords, lock status) restored to their backup state. Objects stored on keyrings are overwritten by their backup versions. Keyrings and objects that do not have a backup version are left unchanged by the restore operation.

REST API: PUT /api/cluster/restore

User Privileges

Users with the following privileges can perform this command:

> Admin

Syntax

cluster restore run -filename <filename> **-restorepassword** <password> **-type keyring**

Argument(s)	Shortcut	Description
-filename <filename>	**-f**	Specifies the backup filename to restore from.
-restorepassword <password>	**-r**	Specifies the password that was set on the backup file.
-type <string>	**-t**	Restores keyring data from a backup file. You must specify **keyring** as the data type.

Example

```
lunash:>cluster restore run -filename myBackup.tar.gz -type keyring -restorePassword
myBUpassword

Successfully started job with ID 6

Command Result : 0 (Success)
```

cluster restore show

Display the status of a restore operation, and the restore history.

> **NOTE** Thales requires minimum Luna Appliance Software 7.8.5 with the lnh_cluster-1.0.4 package, Luna HSM Firmware 7.8.4, and Luna HSM Client 10.7.2 to use clusters in production environments, or minimum Luna Appliance Software 7.9.0 with the lnh_cluster-1.0.5 package, Luna HSM Firmware 7.8.4, and Luna HSM Client 10.8.0 to migrate keys from Luna application partitions.

REST API: GET /api/cluster/restore

User Privileges

Users with the following privileges can perform this command:

- Admin
- Operator
- Monitor

Syntax

cluster restore show

Example

```
lunash:>cluster restore show

Restore requests:

Job ID          Status       Time                 Description
9               Finished     2025-05-02 08:37:34
10              Finished     2025-05-02 08:38:06
11              Finished     2025-05-02 08:39:15
18              Finished     2025-05-02 12:44:01
19              Finished     2025-05-02 12:51:32
20              Finished     2025-05-02 13:03:06
21              Finished     2025-05-02 13:14:18
23              Started      2025-05-02 13:38:36

Command Result : 0 (Success)
```

cluster show

Display information about the specified cluster, including the number of keyrings and keys created, number of authorized members, number of sessions and a breakdown of some crypto operations performed by the cluster.

> **NOTE** Thales requires minimum Luna Appliance Software 7.8.5 with the lnh_cluster-1.0.4 package, Luna HSM Firmware 7.8.4, and Luna HSM Client 10.7.2 to use clusters in production environments, or minimum Luna Appliance Software 7.9.0 with the lnh_cluster-1.0.5 package, Luna HSM Firmware 7.8.4, and Luna HSM Client 10.8.0 to migrate keys from Luna application partitions.
>
> The operation counts from all members are collated when **cluster show** runs. If a member's **cluster** service restarts, the operation counts on that member since the last **cluster show** command are reset to zero. This can result in counts that appear lower than the total number of operations run since the application was started. They do not indicate that assigned operations have not been completed.

REST API: GET /api/clusters/{clusterID}

User Privileges

Users with the following privileges can perform this command:

- Admin
- Operator
- Monitor

Syntax

cluster show -clusterid <string>

Argument(s)	Shortcut	Description
-clusterid	**-c**	Specifies the UUID for the cluster to be displayed.

Example

```
lunash:>cluster show -clusterid ac2a0f56-626e-4c91-a379-489b789a47e7

Cluster Label:  cluster00
Cluster ID:     ac2a0f56-626e-4c91-a379-489b789a47e7
CA certificate:
       SHA1 Fingerprint: 2A:D2:1E:D9:44:82:64:7C:5E:A3:3C:0C:3C:95:68:10:22:70:C3:4E
     SHA256 Fingerprint:
37:F2:67:58:DF:8E:08:C9:DE:FC:25:91:48:64:9B:7A:20:C6:97:4C:86:CA:96:4F:4F:B1:E0:7A:AA:2F:ED:A5
        Expiration Date: Jul 23 21:10:40 2032 GMT
Member:         2 out of 2 authorized
KeyRingCount:   249        KeyCount:           380
Session:        11 out of 11 authenticated
Crypto operations:
    sign/verify    encrypt/decrypt    wrap/unwrap    key generation
    1009              3                 12             14

Command Result : 0 (Success)
```

cluster status

Display the status of the **cluster** service.

> **NOTE** Thales requires minimum Luna Appliance Software 7.8.5 with the lnh_cluster-1.0.4 package, Luna HSM Firmware 7.8.4, and Luna HSM Client 10.7.2 to use clusters in production environments, or minimum Luna Appliance Software 7.9.0 with the lnh_cluster-1.0.5 package, Luna HSM Firmware 7.8.4, and Luna HSM Client 10.8.0 to migrate keys from Luna application partitions.

REST API: GET /api/lunasa/services/{serviceid}

User Privileges

Users with the following privileges can perform this command:

- Admin
- Operator
- Monitor

Syntax

cluster status

Example

```
lunash:>cluster status

   Cluster Service:
   ==================
   Configuration:         enabled
   Status:                running
   Cluster attached to partition: clusterpar

Command Result : 0 (Success)
```

hsm

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

> **NOTE** HSM commands from LunaSH 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

- **changepolicy**
- **changepw**
- **checkcertificates**
- **displaylicenses**
- **factoryreset**
- **firmware**
- **fm**
- **generatedak**
- **information**
- **init**
- **loadcustomercert**
- **login**
- **logout**
- **ped**
- **selftest**
- **setlegacydomain**
- **show**
- **showpolicies**
- **stc**
- **stm**
- **supportinfo**
- **tamper**
- **time**
- **update**
- **zeroize**

Argument(s)	Shortcut	Description
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 167.
changepw	**changepw**	Changes the password or PED key contents for the HSM Admin. See "hsm changePw" on page 169.

Argument(s)	Shortcut	Description
checkcertificates	**che**	Checks the HSM for presence of MAC and DAC. See "hsm checkCertificates" on page 171.
displaylicenses	**d**	Display a list of all licenses on the HSM. See "hsm displayLicenses" on page 172.
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 173.
firmware	**fi**	Update or rollback the HSM firmware. See "hsm firmware" on page 176.
fm	**fm**	Manage Functionality Modules. See "hsm fm" on page 181.
generatedak	**g**	Generate a new DAK pair. See "hsm generateDAK" on page 187.
information	**inf**	Display HSM information, reset the HSM counters, or monitor HSM performance. see "hsm information" on page 188.
init	**ini**	Initialize the HSM. See "hsm init" on page 194.
loadcustomercert	**loa**	Load the customer-signed MAC and DAC. See "hsm loadCustomerCert" on page 197.
login	**logi**	Log in as the HSM Admin. See "hsm login" on page 198.
logout	**logo**	Log out the HSM Admin account. See "hsm logout" on page 199.
ped	**p**	Display or change the configuration of the PED. See "hsm ped" on page 200.
selftest	**sel**	Test the cryptographic capabilities of the HSM. See "hsm selfTest" on page 232.
setlegacydomain	**set**	Set the legacy cloning domain on an HSM. See "hsm setLegacyDomain" on page 233
show	**sh**	Display a list showing the current configuration of the HSM. See "hsm show" on page 234.

Argument(s)	Shortcut	Description
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 237.
stc	**stc**	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 243.
stm	**stm**	Show the current secure transport mode status, place the HSM in secure transport mode, or recover from secure transport mode. See "hsm stm" on page 275.
supportinfo	**su**	Get HSM support information. See "hsm supportInfo" on page 281.
tamper	**ta**	Show and clear HSM tamper state. See "hsm tamper" on page 282.
time	**ti**	Display the current HSM time and synchronize HSM time with appliance time. See "hsm time" on page 284.
update	**u**	Display or install any available capability or firmware updates. See "hsm update" on page 287.
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 291.

hsm backup

> **NOTE** This command was deprecated, and is no longer available in Luna Network HSM 7 Appliance Software 7.7.0 and newer. It should not be used in older software and firmware versions.

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, with **hsm changepolicy**, then **hsm showpolicies** 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 you are given the choice to proceed or quit. This means that you cannot inadvertently destroy the contents of your HSM - you must acknowledge that you know that will happen before you proceed. Once a policy is changed, the program reports back the new value of the policy.

User Privileges

Users with the following privileges can perform this command:

> Admin

Syntax

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

Argument(s)	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 <hsm_policy_number>	**-p**	Specifies the policy code of the policy to alter. Policy descriptions and codes are obtained with the **hsm showpolicies** command.
-value <hsm_policy_value>	**-v**	Specifies the value to assign to the specified policy. When specifying values for an on/off type policy, use '**1**' for on and '**0**' for off.

Example

```
lunash:>hsm changePolicy -policy 39 -value 1

    Enabling STC will terminate all existing NTLS connections.

    Type 'proceed' to enable STC on HSM, or 'quit'
    to quit now. > proceed


'hsm changePolicy' successful.

Policy Allow Secure Trusted Channel is now set to value: 1
```

```
Restarting NTLS and STC services... Done

Command Result : 0 (Success)



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! (HSM Admin, Domain, and M of N (where applicable)
          will not be modified.)

          Type 'proceed' to zeroize your HSM and change the policy,
          or 'quit' to quit now.
          > proceed
'hsm changePolicy' successful.

Policy Allow masking is now set to value: 0


Command Result : 0 (Success)
```

hsm changePw

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

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

- Regular credential rotation as part of your organization's security policy
- Compromise of a role or secret due to loss or theft of a PED key
- Personnel changes in your organization or changes to individual security clearances
- Changes to your security scheme (implementing/revoking M of N, PINs, or shared secrets)

User Privileges

Users with the following privileges can perform this command:

- Admin

Syntax

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

Argument(s)	Shortcut	Description

-newpw <password>	**-n**	Specifies the new password that is used as the HSM SO'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.
		Passwords and activation challenge secrets must be 8-255 characters in length. Spaces are allowed; to specify a password with spaces using command-line options, enclose the password in double quotation marks. The space character may not be used as the first character in a password.
		The following characters are allowed:
		`!#$%'`
		`()*+,-./0123456789:=? @ABCDEFGHIJKLMNOPQRSTUVWXYZ`
		`[]^_abcdefghijklmnopqrstuvwxyz{}~`
		This character set is enforced when using Luna Appliance Software 7.9.0 or Luna HSM Client 10.8.0 or newer, and recommended for all previous versions. Previously-set passwords and challenge secrets are unaffected, but the new character set is enforced when these passwords are changed.

-oldpw <password>	**-o**	Specifies the current password for the HSM SO. If the current password is not provided on the command line, the user is interactively prompted for the current password.

Example

```
lunash:>hsm changePw

  Please enter the HSM Administrators' current password:
  > ********

  Please enter a new password for the HSM Administrator:
  > ********

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

'hsm changePw' successful.


Command Result : 0 (Success)
```

hsm checkCertificates

> **NOTE** This command has been removed in Luna Network HSM 7 Appliance Software 7.7.0 and newer, and was deprecated in Luna 7 versions older than that.

Check the HSM for presence of MAC and DAC.

User Privileges

Users with the following privileges can perform this command:

- Admin
- Operator
- Monitor

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 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.

User Privileges

Users with the following privileges can perform this command:

- Admin
- Operator
- Monitor

Syntax

hsm displayLicenses

Example

```
lunash:>hsm displayLicenses


   HSM CAPABILITY LICENSES
   License ID          Description
   ================    ====================================
      621000153-000    K7 base configuration
      621010185-003    Key backup via cloning protocol
      621000046-002    Maximum 100 partitions
      621000135-002    Enable allow decommissioning
      621000021-002    Performance level 15


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 only via a local serial connection; it is not accepted via SSH.

> **CAUTION!** 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 are asked whether to “proceed” unless the **-force** switch is provided at the command line. See Comparison of Destruction/Denial Actions to view a table that compares and contrasts various "deny access" events or actions that are sometimes confused.

This command:

- Erases the currently-initialized Auditor role
- Resets HSM policies
- Erases the RPV (Remote PED Vector or orange PED key authentication data)

  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 erases the RPV as described above, and you previously established a remote PED connection (using "hsm ped connect" on page 201), you must tear down the remote PED connection (using "hsm ped disconnect" on page 206) 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.

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

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

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 543 affects appliance settings external to the HSM. To bring your entire Luna Network HSM 7 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 291 instead.

User Privileges

Users with the following privileges can perform this command:

> Admin

Syntax

hsm factoryReset [**-force**]

Argument(s)	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 : 65535 (Luna Shell execution)
```

Local attempt (firmware older than Luna HSM Firmware 7.7.0):

```
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)
```

Local attempt (Luna HSM Firmware 7.7.0 and newer)

```
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 not be changed.
Type 'proceed' to return the HSM to factory default, or
'quit' to quit now.
> proceed
Error: Unable to communicate with HSM.

Restarting HSM card in progress. Please wait...
RESET: Input/output error

Error: Unable to communicate with HSM.

HSM reset operation may take several minutes to complete.
Please DO NOT interrupt the operation or reboot the system while the reset is in progress.

....resetting device.
Current Boot Loader: Boot Loader Revision K7 1.1.1
HSM Recover command stored for Firmware!
HSM Recover will be done by Firmware after next card reset.
The HSM Recover may take a few minutes.
....resetting device 1 of 2 times
....resetting device.
Firmware performed HSM Recover command!
....resetting device 2 of 2 times
Firmware restarted without error.

'hsm factoryReset' successful.

Please wait while the HSM is reset to complete the process.

Command Result : 0 (Success)
```

hsm firmware

Upgrade to the version of HSM firmware that is currently on standby in the Luna Network HSM 7 appliance.

Rollback to the previous version of HSM firmware, retained in the Luna Network HSM 7 appliance.

Syntax

hsm firmware

rollback
upgrade
show

Argument(s)	Shortcut	Description
show	**s**	Show HSM firmware version info. See "hsm firmware show" on page 179.
upgrade	**u**	Update HSM firmware. See "hsm firmware upgrade" on page 180.
rollback	**r**	Rollback HSM firmware. See "hsm firmware rollback" on the next page.

 Copyright 2001-2025 Thales Group

hsm firmware rollback

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

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

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

After rollback is complete, the command "hsm show" on page 234 indicates that no further firmware rollback is available.

If you wish to reinstall the newer firmware, use command "hsm firmware upgrade" on page 180. The newer version remains on standby in the appliance, so there is no need to re-upload or to re-install appliance software.

> **CAUTION!** *Update any factory-fresh Luna Network HSM 7 to newer firmware before rolling back*. The firmware rollback feature is intended to return the firmware to the previously installed version. Attempting a firmware rollback on a new appliance received directly from Thales factory can result in RMA (return of your HSM to Thales).

User Privileges

Users with the following privileges can perform this command:

- Admin
- Operator

Syntax

hsm firmware rollback [**-force**]

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

Example

```
lunash:>hsm firmware rollback

   The HSM Administrator is logged in. Proceeding...

   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 might lose some capabilities.
```

```
         (4) You must re-initialize the HSM.
         (5) If the PED use is remote, you must re-connect it.

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

   > proceed
   Proceeding...

Rolling back firmware.  This may take several minutes.


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.

User Privileges

Users with the following privileges can perform this command:

- Admin
- Operator
- Monitor

Syntax

hsm firmware show

Example

```
lunash:>hsm firmware show

   Current Firmware:                  7.2.0
   Rollback Firmware:                 7.0.3
   Upgrade Firmware:                  7.3.0

Command Result : 0 (Success)
```

Example after upgrade

```
lunash:>hsm firmware show

   Current Firmware:                  7.7.0
   Rollback Firmware:                 7.4.1
   Upgrade Firmware:                  N/A

Command Result : 0 (Success)
```

hsm firmware upgrade

This command updates the HSM firmware by applying the Firmware Update File that was saved in the standby location by the factory, or by your most recent Luna Network HSM 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 177, to roll back to the previous firmware version.

> **NOTE** If you are updating the firmware to Luna HSM Firmware 7.7.0 or newer, objects and partitions must be re-sized to include additional object overhead associated with the new V1 partitions - this is included in the process, no additional action from you (see Behavior of Pre-Firmware 7.7, V0, and V1 Partitions). This conversion can take much longer than previous firmware updates, depending on the number of objects stored on the HSM (a few minutes to several hours). Ensure that you can leave the update operation uninterrupted for this amount of time. Do not interrupt the procedure even if the operation appears to have stalled.

User Privileges

Users with the following privileges can perform this command:

- Admin
- Operator

Syntax

hsm firmware upgrade [**-force**]

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

Example

```
lunash:>hsm firmware upgrade

   The HSM Administrator is logged in. Proceeding...

   WARNING: This operation will upgrade the firmware and restart NTLS/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.

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

   > proceed
   Proceeding...


   Uploading new FW to the HSM. This may take several minutes.
   Firmware has been successfully uploaded to the HSM. Resetting HSM.
   Firmware update:
```

```
   Object check started.
   Object check successfully completed.
   Object update started.
   Object update successfully completed.

   Firmware successfully updated.

   Object update successfully completed.
   Firmware successfully updated.
Update Result : 0 (Success)
Resetting HSM ...

Stopping ntls:[  OK  ]

Starting ntls:[  OK  ]
Stopping stcd:[  OK  ]

Starting stcd:[  OK  ]

Command Result : 0 (Success)
```

hsm fm

Manage Functionality Modules in the HSM.

> **NOTE** This feature requires minimum Luna Network HSM 7 Appliance Software 7.4.0, Luna HSM Firmware 7.4.0, and Luna HSM Client 7.4.0. Your Luna Network HSM 7 hardware must be FM-Ready (see Preparing the Luna Network HSM 7 to Use FMs).

Syntax

hsm fm

delete
load
recover
smfs activate
status

Argument(s)	Shortcut	Description
delete	**d**	Delete a specified Functionality Module. See "hsm fm delete" on the next page.
load	**l**	Load Functionality Module. See "hsm fm load" on page 183.
recover	**r**	Erase FMs, the SMFS, or both; this can restore HSM functions in case of an FM-related loss of service. See "hsm fm recover" on page 183.

Argument(s)	Shortcut	Description
smfs activate	**sm a**	Activate the Secure Memory File System. See "hsm fm smfs activate" on page 185.
status	**st**	Check Functionality Module status. See "hsm fm status" on page 186.

hsm fm delete

Delete the specified Functionality Module. You must be logged in as HSM SO to use this command.

> **NOTE** This feature requires minimum Luna Network HSM 7 Appliance Software 7.4.0, Luna HSM Firmware 7.4.0, and Luna HSM Client 7.4.0. Your Luna Network HSM 7 hardware must be FM-Ready (see Preparing the Luna Network HSM 7 to Use FMs).

User Privileges

Users with the following privileges can perform this command:

> Admin

Syntax

hsm fm delete -id <FM_ID> [**-force**]

Argument(s)	Shortcut	Description
-id <FM_ID>	**-i**	Specifies the FM ID of the FM to be deleted.
-force	**-f**	Force the action without prompting.

Example

```
lunash:>hsm fm delete -id a000


WARNING !!  This command will delete this FM.
If you are sure that you wish to proceed, then type 'proceed', otherwise type 'quit'

> proceed
Proceeding...
Deleting FM in progress. Please wait...

Disabling/Deleting FM 0xa000 on device 0

Functionality Module deleted.


Command Result : 0 (Success)
```

hsm fm load

Load a Functionality Module into the HSM firmware.

> **NOTE** This feature requires minimum Luna Network HSM 7 Appliance Software 7.4.0, Luna HSM Firmware 7.4.0, and Luna HSM Client 7.4.0. Your Luna Network HSM 7 hardware must be FM-Ready (see Preparing the Luna Network HSM 7 to Use FMs).

User Privileges

Users with the following privileges can perform this command:

> Admin

Syntax

hsm fm load -certfile <cert_file> **-fmfile** <FM_file>

Argument(s)	Shortcut	Description
-certfile <cert_file>	**-c**	Certificate file created from the key pair that signed the FM.
-fmfile <FM_file>	**-f**	Signed FM file.

Example

```
[myLuna] lunash:>hsm fm load -certFile FMsign.cert -fmFile skeleton.fm


Importing FM on device 0

Functionality Module download in progress, please wait...

Functionality Module downloaded successfully.

Command Result : 0 (Success)
```

hsm fm recover

Erase the SMFS, all currently-loaded FMs, or both from the HSM firmware. This command is intended for cases where the HSM has become unresponsive due to a buggy or incorrectly configured FM. If this is not the case, use **hsm fm delete** to remove an FM ("hsm fm delete" on the previous page). You must be logged in as HSM SO to use this command.

> **NOTE** This feature requires minimum Luna Network HSM 7 Appliance Software 7.4.0, Luna HSM Firmware 7.4.0, and Luna HSM Client 7.4.0. Your Luna Network HSM 7 hardware must be FM-Ready (see Preparing the Luna Network HSM 7 to Use FMs).

User Privileges

Users with the following privileges can perform this command:

> Admin

Syntax

hsm fm recover [**-erase** <options>] [**-force**]

Argument(s)	Shortcut	Description
-erase <option>	**-e**	Erase the SMFS, all currently-loaded FMs, or both. **Valid Values:** > **smfs**: Erase the SFMS. > **fm**: Erase the FMs. > **both**: Erase both the SMFS and FMs.
-force	**-f**	Force the action without prompting.

Examples

```
lunash:>hsm fm recover -erase smfs

WARNING !!  This command will erase SMFS.
 If you are sure that you wish to proceed, then type 'proceed',
otherwise type 'quit'
 > proceed

Proceeding...
HSM recover in progress. Please wait...

Command Result : 0 (Success)



lunash:>hsm fm recover -erase fm

WARNING !!  This command will erase all loaded FMs.
 If you are sure that you wish to proceed, then type 'proceed',
otherwise type 'quit'
 > proceed

Proceeding...
HSM recover in progress. Please wait...

Command Result : 0 (Success)



lunash:>hsm fm recover -erase both

WARNING !!  This command will erase SMFS and all FMs.
 If you are sure that you wish to proceed, then type 'proceed',
otherwise type 'quit'
```

```
 > proceed

Proceeding...
HSM recover in progress. Please wait...

Command Result : 0 (Success)
```

hsm fm smfs activate

Activate the Secure Memory File System. You must be logged in as HSM SO to use this command. This command activates the SMFS only – it does not activate new Functionality Modules. The HSM firmware must be reset after loading a new FM.

> **NOTE HSM Policy 51: Allow SMFS Auto Activation**
>
> With this policy enabled, the Secure Memory File System (SMFS) is automatically activated on startup, providing a secure, tamper-enabled location in the HSM memory where Functionality Modules can load keys and parameters. Auto-activation for SMFS, like auto-activation for multifactor quorum-authenticated partitions in general, persists through a power outage of up to 2 hours duration.
>
> Thales recommends setting HSM policy 51 to 1 (ON) to avoid having to manually re-activate the SMFS if you need to reboot the HSM. Changing this policy (OFF-to-ON or ON-to-OFF) will destroy all existing application partitions.
>
> This feature requires minimum Luna Network HSM 7 Appliance Software 7.4.0, Luna HSM Firmware 7.4.0, and Luna HSM Client 7.4.0. Your Luna Network HSM 7 hardware must be FM-Ready (see Preparing the Luna Network HSM 7 to Use FMs).

User Privileges

Users with the following privileges can perform this command:

- Admin

Syntax

hsm fm smfs activate

Example

```
[myLuna] lunash:>hsm fm smfs activate


Activating SMFS on device 0

SMFS successfully activated.

Command Result : 0 (Success)
```

hsm fm status

Check the status of Functionality Modules on the HSM.

> **NOTE** This feature requires minimum Luna Network HSM 7 Appliance Software 7.4.0, Luna HSM Firmware 7.4.0, and Luna HSM Client 7.4.0. Your Luna Network HSM 7 hardware must be FM-Ready (see Preparing the Luna Network HSM 7 to Use FMs).

User Privileges

Users with the following privileges can perform this command:

> Appliance admin

Syntax

hsm fm status

Example

```
lunash:>hsm fm status

Getting status of the FM on all available devices


Current Functionality Module Configuration for device 0:
Serial # : 66331
Model    : Luna K7
SMFS     : Activated

FM Label      : skeleton
FM ID         : a000
Version       : 1.01
Manufacturer  : Safenet Inc.
Build Time    : Wed Dec  5 14:44:47 2018 - EST
Fingerprint   : 78 7C E3 C2 01 54 B3 99 08 59
ROM size      : 7302
Status        : Enabled
Startup Status: OK


Command Result : 0 (Success)
```

hsm generateDAK

> **NOTE** This command has been removed in Luna Network HSM 7 Appliance Software 7.7.0 and newer, and was deprecated in Luna 7 versions older than that.

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 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.

User Privileges

Users with the following privileges can perform this command:

- Admin
- Operator

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.

Syntax

hsm information

monitor
reset
show

Argument(s)	Shortcut	Description
monitor	**m**	Monitors the HSM performance. See "hsm information monitor" on the next page.
reset	**r**	Resets the HSM counters. See "hsm information reset" on page 192.
show	**s**	Display HSM information. See "hsm information show" on page 193.

 Copyright 2001-2025 Thales Group

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

> 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 573 to precisely set the time, and then manage/prevent clock drift.

> **NOTE** For ongoing/continual collection of such HSM information, Thales recommends using SNMP.

See Performance Monitoring.

User Privileges

Users with the following privileges can perform this command:

> Admin

> Operator

> Monitor

Syntax

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

Argument(s)	Shortcut	Description
-interval <integer>	**-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.

Argument(s)	Shortcut	Description
-rounds <integer>	**-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_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 'sftp' to retrieve the file to a workstation for analysis.
-serial <integer>	**-se**	Specifies the serial number of HSM to monitor. The default is to use the embedded HSM. This parameter is optional if your Luna Network HSM does not have additional HSMs attached. If you have a USB-connected HSM, such as Luna USB HSM 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

In the examples below, "Average HSM Utilization" is calculated as (<period-uptime> - <period-idle-time>) / (<period-uptime> * 100).

With no arguments (output to terminal):

```
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       :  Mon Jul  4 14:43:20 2016
    HSM Has Been Up For  :  9 day(s), 22:30:40

Command Result : 0 (Success)
```

With arguments (output to file):

```
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
-------------------|----------------|---------------|----------------|---------------
           859,370 |     103,545,072 |           241 |           1.03 |          1.46
           859,376 |     103,545,569 |           497 |           1.03 |          0.46
           859,382 |     103,545,570 |             1 |           1.03 |          0.00
           859,388 |     103,545,571 |             1 |           1.03 |          0.01
           859,394 |     103,545,812 |           241 |           1.03 |          1.46
           859,400 |     103,545,813 |             1 |           1.03 |          0.00
-------------------|----------------|---------------|----------------|---------------

    Average HSM Utilization In This Period  :  0.57%

    HSM Last Reset       :  Mon Jul  4 14:43:21 2016
    HSM Has Been Up For  :  9 day(s), 22:43:20


The output has been saved to a file named `hsm_monitor_56726.txt`.
Output is appended if the file already exists.
Use `my file delete hsm_monitor_56726.txt` to remove the file.
Use `scp/sftp` to retrieve the file to an external workstation for further analysis.


Command Result : 0 (Success)
```

hsm information reset

Reset the HSM counters.

User Privileges

Users with the following privileges can perform this command:

- Admin
- Operator

Syntax

hsm information reset

Example

```
lunash:>hsm information reset

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

hsm information show

Display the contents of the HSM counters.

> **NOTE** The "Operation Requests" counter increments rapidly (often by 42 or 47 counts) because even relatively simple LunaSH 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.

User Privileges

Users with the following privileges can perform this command:

- Admin
- Operator
- Monitor

Syntax

hsm information show

Example

```
lunash:>hsm information show


HSM Event Counters:

Operation Requests:                       103560569
Operation Errors:                               199
Crypto Operation Requests:                 88292416
Crypto Operation Errors:                       60
Critical Events:                                0
Non-Critical Events:                            0



Command Result : 0 (Success)
```

hsm init

Initialize the HSM in the Luna Network HSM 7. Initialization assigns an HSM label, creates an HSM Security Officer (HSM SO), 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, including application partitions and their data. 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. 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 Initializing the HSM.

User Privileges

Users with the following privileges can perform this command:

> Admin

Syntax

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

Argument(s)	Shortcut	Description
-applytemplate <filename>	**-ap**	Apply an HSM policy template. This feature requires minimum Luna HSM Firmware 7.1.0 and Luna Network HSM 7 Appliance Software 7.1.0.
-authtimeconfig	**-a**	Specifies that the HSM SO role must be logged in to configure the time.
-defaultdomain	**-de**	This option is deprecated. It applies to password-authenticated HSMs only. It allows you to set a default domain that is compatible with certain legacy HSMs, instead of specifying a unique domain string with **-domain**.

 Copyright 2001-2025 Thales Group

Argument(s)	Shortcut	Description
-domain <hsm_domain>	**-do**	Specifies the key cloning domain string for the HSM Admin partition. It applies to password-authenticated HSMs only. This string is not required for any key cloning or crypto operations on application partitions. The HSM domain is a legacy feature that must be set, but has no practical function on Luna 7 HSMs. **NOTE** This is distinct from the domain on an application partition, which is a critical component required for key cloning, backup/restore, and high availability groups. Refer to Domain Planning for more information. The domain string must be 1-128 characters in length. The following characters are allowed: `abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789 ! @#$%^*-_=+[]{}()/:',.~` The following characters are problematic or invalid and must not be used in a domain string: `"&;<>?\`|` Spaces are allowed, as long as the leading character is not a space; to specify a domain string with spaces using the **-domain** option, enclose the string in double quotation marks. For password-authenticated HSMs, the domain string should match the complexity of the partition password.
-force	**-f**	Force the action without prompting.
-label <hsm_label>	**-l**	Specifies the label to assign to the HSM. The HSM label created during initialization must be 1-32 characters in length. If you specify a longer label, it will automatically be truncated to 32 characters. Only alphanumeric characters and the underscore are allowed: `abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789_`
-password <HSMSO_password>	**-p**	Specifies the password to be used as login credential by the HSM SO. For multifactor quorum-authenticated HSMs, the Luna PED is used for the HSM SO credential, and data input for this value is ignored. This parameter is required in password-authenticated HSMs. It is ignored in multifactor quorum-authenticated HSMs. Passwords and activation challenge secrets must be 8-255 characters in length. Spaces are allowed; to specify a password with spaces using command-line options, enclose the password in double quotation marks. The space character may not be used as the first character in a password. The following characters are allowed: `!#$%'()*+,-./0123456789:=? @ABCDEFGHIJKLMNOPQRSTUVWXYZ[]^_ abcdefghijklmnopqrstuvwxyz{}~` This character set is enforced when using Luna Appliance Software 7.9.0 or Luna HSM Client 10.8.0 or newer, and recommended for all previous versions. Previously-set passwords and challenge secrets are unaffected, but the new character set is enforced when these passwords are changed.

Example

Multifactor Quorum-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)
```

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

Warning:  This HSM is not in the factory reset (zeroized) state.
          You must present the current HSM Admin login credentials
          to clear the HSM contents.

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)
```

hsm loadCustomerCert

> **NOTE** This command has been removed in Luna Network HSM 7 Appliance Software 7.7.0 and newer, and was deprecated in Luna 7 versions older than that.

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

User Privileges

Users with the following privileges can perform this command:

- Admin
- Operator

Syntax

hsm loadcustomercert -certfilename <filename>

Argument(s)	Shortcut	Description
-certfilename <filename>	**-c**	The customer-signed certificate's filename.

hsm login

Log in as the HSM Security Officer (SO).

User Privileges

Users with the following privileges can perform this command:

> Admin

> Operator

Syntax

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

Argument(s)	Shortcut	Description
-password <password>	**-p**	Specify HSM SO password (for password-authenticated HSM only; ignored for multifactor quorum-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.

User Privileges

Users with the following privileges can perform this command:

- Admin
- Operator

Syntax

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 Luna PED.

Syntax

hsm ped

connect
deselect
disconnect
select
server
set
show
timeout
vector

Argument(s)	Shortcut	Description
connect	**c**	Connect to a Remote PED. See "hsm ped connect" on the next page.
deselect	**de**	Deselect the currently selected PEDserver. See "hsm ped deselect" on page 205.
disconnect	**di**	Disconnect a connected Remote PED. See "hsm ped disconnect" on page 206.
select	**sel**	Select a connected PEDserver from the list to provide Luna PED operations to the HSM. See "hsm ped select" on page 209.
server	**ser**	Display or configure PEDserver. See "hsm ped server" on page 210.
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 214.
show	**sh**	Display information for the current HSM PED connection. See "hsm ped show" on page 207.
timeout	**t**	Set or display the remote PED connection timeout. See "hsm ped timeout" on page 215.
vector	**v**	Initialize or erase a remote PED vector. See "hsm ped vector" on page 219.

 Copyright 2001-2025 Thales Group

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 214 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**.

Values set with hsm ped set	Parameters specified by hsm ped connect	IP address used	Port used
Port only	None	Error. You must use the **-ip** parameter to specify an IP address.	Port configured with **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 specify at least an IP address. If no port is specified, the default port (1503) is used.

> **NOTE** To set up or erase a Remote PED vector, or to make or break the Remote PED connection, on an HSM that is externally connected to the Luna Network HSM 7, use the "**-serial**" option to specify the target HSM. If "**-serial**" is not specified, then the command acts on the Luna Network HSM 7's internal HSM card.

User Privileges

Users with the following privileges can perform this command:

- Admin
- Operator

Syntax

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

Argument(s)	Shortcut	Description
-force	**-f**	Force the action without prompting.
-ip <ip_address>	**-i**	Specifies the IP Address of the remote Luna PED.

Argument(s)	Shortcut	Description
-password <optional_PIN>	**-pa**	Used to set up a one-time password-protected secure channel between an uninitialized HSM and the Luna PED, allowing you to securely initialize the orange (Remote PED Vector) key. Include **-password** alone to use a randomly-generated one-time PIN, or you can specify your own 8-digit numeric pin using **-password** <optional_PIN>. See Remote RPV Initialization for more information. **NOTE** This option is available only if you are using Luna HSM Firmware 7.7.0 or newer and Luna HSM Client 10.3.0 or newer. Using older firmware, you are prompted to enter an 8-digit numeric PIN.
-port <port>	**-po**	Network Port (0-65535). **Default:** 1503
-serial <serial_num>	**-s**	Token Serial Number.

Examples

Connecting to a remote PED on a Luna Network HSM 7 with zeroized HSM and non-initialized RPV

```
lunash:>hsm ped c -ip 172.20.9.24

Luna PED operation required to connect to Remote PED - use orange PED key(s).

Luna PED operation required to connect to remote PED - Enter PED password: 37749794.

Command Result : 0 (Success)
```

Connecting to a remote PED on a Luna Network HSM 7 with zeroized HSM, non-initialized RPV and provided manually defined password

```
lunash:>hsm ped c -ip 172.20.9.24 -password 12345678

Luna PED operation required to connect to Remote PED - use orange PED key(s).

Luna PED operation required to connect to remote PED - Enter PED password: 12345678.

Command Result : 0 (Success)
```

Connecting to a remote PED on a Luna Network HSM 7 with zeroized HSM, non-initialized RPV, and incorrect password was typed on PED

```
lunash:>hsm ped c -ip 172.20.9.24

Luna PED operation required to connect to Remote PED - use orange PED key(s).
```

```
Luna PED operation required to connect to remote PED - Enter PED password: 58592536.

Error connecting to remote PED with error code: LUNA_RET_PED_DEK_INVALID

Error for 'hsm ped connect': 0X300146 (LUNA_RET_PED_DEK_INVALID)
Failed to connect the remote PED

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

Connecting to a remote PED on a Luna Network HSM 7 with zeroized HSM and initialized RPV

```
lunash:>hsm ped c -ip 172.20.9.24

Luna PED operation required to connect to Remote PED - use orange PED key(s).

Command Result : 0 (Success)
```

Connecting to a remote PED on a Luna PED with zeroized HSM, initialized RPV and provided manual defined password:

```
lunash:>hsm ped c -ip 172.20.9.24 -password 12345678

Luna PED operation required to connect to Remote PED - use orange PED key(s).

Warning:  You provided "-password" option, but either
the Remote PED Vector has already been initialized or HSM is not zeroized.

"-password" option provided was ignored.

Command Result : 0 (Success)
```

Using incorrect number of digits for “-password” option

```
lunash:>hsm ped c -ip 172.20.9.24 -password 1234

Syntax Error: password parameter 1234 for option -password is shorter than minimum length 8

Command Result : 22 (Invalid argument)

Syntax:      hsm ped connect [-ip <ipaddress>] [-port <port>] [-serial <serialnum>] [-force]

Option(s)         Short     Parameter                Description
...............................................................................
-ip               -i        <ipaddress>              IP Address
-port             -po       <port>                   Network Port (0-65535)
-serial           -s        <serialnum>              Token Serial Number
-force            -f        .                        Force Action

Setup a remote PED connection.
```

hsm ped deselect

When a PEDserver is connected and selected to provide Luna PED operations to the HSM, use this command to deselect the currently selected PEDserver. The PEDserver remains connected and remains in the list of available PEDservers, but is no longer selected and can no longer provide PED operations for the HSM until it is selected again.

User Privileges

Users with the following privileges can perform this command:

> Admin

> Operator

Syntax

hsm ped deselect [**-host** <hostname>]

Argument(s)	Shortcut	Description
-host <hostname>	-h	The hostname of the PEDserver instance that you are deselecting, as shown in the output of the **hsm ped show** command. Required if multiple PEDservers have established connections; optional if only one PEDserver is available.

Example

```
lunash:>lunash:>hsm ped deselect -host WIN-1TFMAA8U4V7

  Host WIN-1TFMAA8U4V7 deselected.

Command Result : 0 (Success)
```

hsm ped disconnect

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

To disconnect the PED when using a peer-to-peer connection, you must first disconnect from peer mode and return to legacy mode.

> **NOTE** To set up or erase a Remote PED vector, or to make or break the Remote PED connection, on an HSM that is externally connected to the Luna Network HSM 7, use the "**-serial**" option to specify the target HSM. If "**-serial**" is not specified, then the command acts on the Luna Network HSM 7's internal HSM card.

User Privileges

Users with the following privileges can perform this command:

- Admin
- Operator

Syntax

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

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


Command Result : 0 (Success)
```

hsm ped show

Display information for the current HSM PED connection.

User Privileges

Users with the following privileges can perform this command:

- Admin
- Operator
- Monitor

Syntax

hsm ped show

Argument(s)	Shortcut	Description
<none>	<none>	With no argument, the command displays PED Client config and status information.
server	**s**	Displays PED Server config and status information.

Example

```
lunash:>hsm ped show


Configured Remote PED Server IP address: 192.20.11.64
Configured Remote PED Server Port: 1503

Ped Client Version 2.0.1 (20001)
Ped Client launched in status mode.
Callback Server is running..

   Callback Server Information:
         Hostname:                        sa7ped
         IP:                              192.20.11.40
         Software Version:                2.0.1 (20001)

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

      Callback Server Up Time:                     494832 (secs)
      Callback Server Current Idle Time:           3774 (secs)
      Callback Server Total Idle Time:             494098 (secs) (99%)
      Idle Timeout Value:                 1800 (secs)

   Number of PED ID Mappings:            1

   PED ID Mapping Table:
      PED ID:                             4
```

```
      Server Hostname:                    192.20.11.64
      Server Port:                        1503
      Status: Not Assigned


   Number of HSMs:                        1
   HSM List:
      Device Type:                        K7 HSM
      HSM Serial Number:                  532018
      HSM Firmware Version:               7.0.1
      HSM Cmd Protocol Version:           21
      HSM Callback IO Version:            1
      HSM Callback Protocol Version:      1
      HSM Up Time:                        423248 (secs)
      HSM Total Idle Time:                422514 (secs) (99%)
      HSM Current Idle Time:              3774 (secs)

   Number of Connected PED Server :      0

Show command passed.

Command Result : 0 (Success)
```

hsm ped select

When a PEDserver has established a connection to this Luna Network HSM 7 appliance in peer-to-peer mode, it could be one of many. Use this command to select one connected PEDserver from the list to provide Luna PED operations to the HSM.

User Privileges

Users with the following privileges can perform this command:

- Admin
- Operator

Syntax

hsm ped select [**-host**<hostname>] [**-serial** <serialnum>]

Argument(s)	Shortcut	Description
-host <hostname>	**-h**	The hostname of the PEDserver that you are selecting, as shown in the output of the **hsm ped show** command. Required if multiple PEDservers have established connections; optional if only one PEDserver is available.
-serial <serialnum>	**-s**	Specifies the serial number of the HSM that is to be served by Luna PED operations. Optional unless more than one HSM is present.

Example

```
lunash:>lunash:>hsm ped select -host WIN-1TFMAA8U4V7

Luna PED operation required to connect to Remote PED - use orange PED key(s).


Command Result : 0 (Success)
```

hsm ped server

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

Syntax

hsm ped server

delete
list
register

Argument(s)	Description
delete	Deregister a PEDserver. See "hsm ped server delete" on the next page.
list	List all remote PEDserver configurations. See "hsm ped server list" on page 212.
register	Register a PEDserver certificate with the appliance. See "hsm ped server register" on page 213.

 Copyright 2001-2025 Thales Group

hsm ped server delete

Delete a previously registered PEDserver. This command will prompt the user to continue the removal of the certificate before executing.

If the certificate common name input into the command does not exist, an error is returned.

User Privileges

Users with the following privileges can perform this command:

- Admin
- Operator

Syntax

hsm ped server revoke -commonname <certificate common name> [**-force**]

Argument(s)	Shortcut	Description
-commonname <certificate common name>	**-c**	The common name of the certificate. The name can be retrieved by running the **hsm ped server list** command.
-force	**-f**	Force the action without prompting.

Example

```
lunash:>hsm ped server revoke -commonname 192.20.11.64

CAUTION:  Are you sure you wish to delete PED server named:
           192.20.11.64
          Type 'proceed' to delete the PED server, or 'quit'
          to quit now. > proceed

'hsm ped server delete' successful.

Command Result : 0 (Success)
```

hsm ped server list

List all remote PEDserver configurations.

User Privileges

Users with the following privileges can perform this command:

- Admin
- Operator
- Monitor

Syntax

hsm ped server list

Example

```
lunash:>hsm ped server list

   Number of Registered PED Server :  1

      PED Server  1 : CN = 192.20.11.64

Command Result : 0 (Success)
```

hsm ped server register

Register a PEDserver certificate with the appliance. Once the certificate has been registered, the certificate file is removed from the user's LunaSH home directory.

This command will fail if the same certificate is being registered again.

User Privileges

Users with the following privileges can perform this command:

- Admin
- Operator

Syntax

hsm ped server register -certificate <filename> [**-force**]

Argument(s)	Description
-certificate <filename>	The name of the certificate file stored in the user's LunaSH home directory. The filename can be found by executing the **my file list** command.
-force	Force the action without prompting.

Example

```
lunash:>hsm ped server register -certificate 192.20.11.64.pem

'hsm ped server register' successful.

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 PEDserver. See "hsm ped connect" on page 201 for more information.

User Privileges

Users with the following privileges can perform this command:

> Admin

Syntax

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

Argument(s)	Shortcut	Description
-ip <ip_address>	**-i**	Specifies the default IP Address used by the **hsm ped connect** command.
-port <port>	**-p**	Specifies the default port used by the **hsm ped connect** command. **Range:** 0-65535 **Default:** 1503

Example

```
lunash:>hsm ped set -ip 192.20.11.64 -port 1503

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

Argument(s)	Shortcut	Description
set	**se**	Set the remote PED connection timeouts. See "hsm ped timeout set" on the next page.
show	**sh**	Display the currently configured remote PED connection timeout values. See "hsm ped timeout show" on page 218.

 Copyright 2001-2025 Thales Group

hsm ped timeout set

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

> **rped** - is the connection inactivity timeout. The default is 1800 seconds (30 minutes).

> **pedk** - is for PED key activities in particular. The default and minimum setting is 200 seconds. If you are using M of N for your HSM roles, it might be useful to increase this value so that there is time for each required user to present their PED key (maximum 600 seconds).

> **pedo** - is for the entire Luna PED operation. The default is 920 seconds. It should only be necessary to increase this if you are migrating a large number of orange PED keys for use with Luna HSM Firmware 7.7.0 or newer.

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.

User Privileges

Users with the following privileges can perform this command:

> Admin

> Operator

Syntax

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

Argument(s)	Shortcut	Description
-seconds <seconds*>	**-s**	Specifies the timeout value, in seconds, for the specified type, *except that type wdel is in microseconds. **Defaults:** 1800 (rped), 200 (pedk), 920 (pedo), none (wdel)

Argument(s)	Shortcut	Description
-type <type>	**-t**	Specifies the timeout type. **Valid values:** > **rped** - set the remote PED connection inactivity timeout. • [Range 1-to-99999] • [Default 1800 seconds (set the value of **-seconds** to zero to reset to default)] > **pedk** - set the PED key timeout. • [Range 200-to-600] • [Default 200 seconds (set the value of **-seconds** to zero to reset to default)] > **pedo** - set the total Luna PED operation timeout. [Range 920-to-99999] > **wdel** -set the PED write delay in *microseconds* • [Range 0-to-10000]; can be viewed if the string "server" is appended to "hsm ped show" on page 207 command. like **hsm ped show server** A PED write delay (-type wdel) of 0 s OFF... no default.

Example

```
lunash:>hsm ped timeout set -type pedk -seconds 500

Set the timeout value to 500 seconds.

Command Result : 0 (Success)
```

hsm ped timeout show

Display the currently configured remote PED connection timeout values.

User Privileges

Users with the following privileges can perform this command:

- Admin
- Operator
- Monitor

Syntax

hsm ped timeout show

Example

```
lunash:>hsm ped timeout show

The remote PED connection timeout value (seconds) =  1800
The PED key interaction timeout value (seconds)    = 200
The entire PED operation timeout value (seconds)  =  920

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 Remote PED vector, or to make or break the Remote PED connection, on an HSM that is externally connected to the Luna Network HSM 7, use the "**-serial**" option to specify the target HSM. If "**-serial**" is not specified, then the command acts on the Luna Network HSM 7's internal HSM card.

Syntax

hsm ped vector

erase
init

Argument(s)	Shortcut	Description
erase	**e**	Erase a remote PED vector. See "hsm ped vector erase" on the next page.
init	**i**	Initialize a remote PED vector. See "hsm ped vector init" on page 221.

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 Remote PED vector, or to make or break the Remote PED connection, on an HSM that is externally connected to the Luna Network HSM 7, use the "**-serial**" option to specify the target HSM. If "**-serial**" is not specified, then the command acts on the Luna Network HSM 7's internal HSM card.

User Privileges

Users with the following privileges can perform this command:

> Admin

Syntax

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

Argument(s)	Shortcut	Description
-force	**-f**	Force the action without prompting.
-serial <serialnum>	**-s**	Specifies the serial number of the external HSM 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 type 'proceed', otherwise
type 'quit'

> proceed
Proceeding...

The remote PED vector (RPV) has been erased on HSM.
Ped Client Version 2.0.1 (20001)
Ped Client launched in "Release ID" mode.
Callback Server is running..
ReleaseID command passed.
"Release ID" command passed.
Ped Client Version 2.0.1 (20001)
Ped Client launched in "Delete ID" mode.
Callback Server is running..
DeleteID command passed.
"Delete ID" command passed.

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.

- The orange PED key is kept with the Remote PED, when you set up a Remote PED workstation. The orange PED key allows a Luna Network HSM 7 with that RPV to connect to a Remote PED workstation where the attached PED provides the matching RPV, via the orange PED key.
- 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** If the HSM is initialized, you must be logged in as HSM SO (blue PED key) to initialize the RPV.
>
> If the HSM is uninitialized, you can:
>
> > initialize the RPV remotely by providing a one-time 8-digit PIN
>
> > initialize the RPV locally by connecting a Luna PED to the HSM
>
> To set up or erase a Remote PED vector, or to make or break the Remote PED connection, on an HSM that is externally connected to the Luna Network HSM 7, use the "**-serial**" option to specify the target HSM. If "**-serial**" is not specified, then the command acts on the Luna Network HSM 7's internal HSM card.

User Privileges

Users with the following privileges can perform this command:

> Admin

Syntax

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

Argument(s)	Shortcut	Description
-force	**-f**	Force the action without prompting.
-serial <serialnum>	**-s**	Specifies the serial number of the HSM for which you want to initialize 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',
```

```
otherwise type 'quit'.

> proceed
Proceeding...

Luna PED operation required to initialize remote PED key vector - use orange PED key(s).

Command Result : 0 (Success)
```

hsm qos metrics

Display Partition Utilization Metrics (counters) to terminal or save to a file, or reset the partition utilization counters.

To use the **hsm qos metrics** commands, HSM policy 49 must be enabled (see "hsm showPolicies" on page 237 and "hsm changePolicy" on page 167).

Syntax

hsm qos metrics

reset
show

Argument(s)	Shortcut	Description
reset	**r**	Reset the Partition Utilization Metrics. See "hsm qos metrics reset" below.
show	**s**	Display Partition Utilization Metrics. See "hsm qos metrics show" on page 225.

hsm qos metrics reset

Reset the partition utilization metrics, and optionally display the counts or save to a file.

> **NOTE** This feature requires minimum Luna HSM Firmware 7.3.0, Luna Network HSM 7 Appliance Software 7.3.0, and Luna HSM Client 7.3.0.

To use the **qos metrics** commands, HSM **Policy 49 Allow Partition Utilization Metrics** must be set to a value of 1 (see "hsm showPolicies" on page 237 and "hsm changePolicy" on page 167).

User Privileges

For HSM firmware older than version 7.9.0, this command requires that the HSM SO be logged in.

For HSM firmware at version 7.9.0 onward, this command ***can*** stil require that the HSM SO be logged in (default), but you can remove the SO login requirement by setting HSM **Policy 58 Allow Unrestricted Metrics Access** to a value of 1.

Appliance Users with the following privileges can perform this command:

> Admin

Syntax

hsm qos metrics reset [**-display**] [**-export** <filename>] [**-force**]

Argument(s)	Shortcut	Description
-display	**-d**	Display the utilization counts, up to the moment they are reset.
-export <filename>	**-e**	Export the utilization counts, up to the moment of reset, to the named file.
-force	**-f**	Force the action without prompting for confirmation.

Example

With no arguments (reset only - no display, no save)

```
lunash:>hsm qos metrics reset

CAUTION:  Are you sure you wish to reset the utlilization counters?
          All counters across all partitions will be zeroized.

          Type 'proceed' to reset the counters, or 'quit'
          to quit now.
          > proceed

Successfully reset all utilization counters and restarted count.

Command Result : 0 (Success)
```

With arguments (output to terminal)

```
lunash:>hsm qos metrics reset -display

CAUTION:  Are you sure you wish to reset the utlilization counters?
          All counters across all partitions will be zeroized.

          Type 'proceed' to reset the counters, or 'quit'
          to quit now.
          > proceed

Successfully reset all utilization counters and restarted count.

           Partition
-----------------------------------
Name            Serial          Operation       Action      Count
==============  ==============  ==============  ==========  ==============
test            1230463154880   SIGN            REQUESTS                 0
test            1230463154880   VERIFY          REQUESTS                 0
test            1230463154880   ENCRYPT         REQUESTS                 0
test            1230463154880   DECRYPT         REQUESTS                 0
```

```
test            1230463154880   KEY_GENERATION  REQUESTS                0
test            1230463154880   KEY_DERIVATION  REQUESTS                0

par1            1230463154886   SIGN            REQUESTS        4700342794
par1            1230463154886   VERIFY          REQUESTS        4700342747
par1            1230463154886   ENCRYPT         REQUESTS                0
par1            1230463154886   DECRYPT         REQUESTS                0
par1            1230463154886   KEY_GENERATION  REQUESTS                2
par1            1230463154886   KEY_DERIVATION  REQUESTS                0

Summary of metrics:

SIGN            :       4700342794
VERIFY          :       4700342747
ENCRYPT         :                0
DECRYPT         :                0
KEY_DERIVATION  :                0
KEY_GENERATION  :                2

Metrics valid since 19 December 2018 22:24:43

Command Result : 0 (Success)
```

With arguments (output to file)

```
lunash:>hsm qos metrics reset -export myparmetricsfile

CAUTION:  Are you sure you wish to reset the utlilization counters?
          All counters across all partitions will be zeroized.

          Type 'proceed' to reset the counters, or 'quit'
          to quit now.
          > proceed

Successfully reset all utilization counters and restarted count.
Successfully exported metrics to file.

Command Result : 0 (Success)
```

With arguments (display and output to file)

```
lunash:>hsm qos metrics reset -display -export todaysmetrics.cvs

CAUTION:  Are you sure you wish to reset the utilization counters?
          All counters across all partitions will be zeroized.

          Type 'proceed' to reset the counters, or 'quit'
          to quit now.
          > proceed

Successfully reset all utilization counters and restarted count.

Partition Name  Serial         Operation        Action      Count
==============  =============  ==========       ==========  =======
test            1230463154880  SIGN             REQUESTS              0
test            1230463154880  VERIFY           REQUESTS              0
test            1230463154880  ENCRYPT          REQUESTS              0
test            1230463154880  DECRYPT          REQUESTS              0
test            1230463154880  KEY_GENERATION   REQUESTS              0
```

```
test            1230463154880  KEY_DERIVATION   REQUESTS              0

par1            1230463154886   SIGN            REQUESTS           1000
par1            1230463154884   VERIFY          REQUESTS           1000
par1            1230463154884   ENCRYPT         REQUESTS              0
par1            1230463154884   DECRYPT         REQUESTS              0
par1            1230463154884   KEY_GENERATION  REQUESTS              0
par1            1230463154884   KEY_DERIVATION  REQUESTS              0

par2            1230463154887   SIGN            REQUESTS     4700342794
par2            1230463154887   VERIFY          REQUESTS     4700342747
par2            1230463154887   ENCRYPT         REQUESTS              0
par2            1230463154887   DECRYPT         REQUESTS              0
par2            1230463154887   KEY_GENERATION  REQUESTS              0
par2            1230463154887   KEY_DERIVATION  REQUESTS              0

Summary of metrics:

SIGN            :       4700343794
VERIFY          :       4700343747
ENCRYPT         :                0
DECRYPT         :                0
KEY_DERIVATION  :                0
KEY_GENERATION  :                0

Metrics valid since 18 December 2018 16:57:11

Successfully exported metrics to file.

Command Result : 0 (Success)
```

hsm qos metrics show

Display the partition utilization metrics, or optionally save to file.

> **NOTE** This feature requires minimum Luna HSM Firmware 7.3.0, Luna Network HSM 7 Appliance Software 7.3.0, and Luna HSM Client 7.3.0.

To use the **qos metrics** commands, HSM **Policy 49 Allow Partition Utilization Metrics** must be set to a value of 1 (see "hsm showPolicies" on page 237 and "hsm changePolicy" on page 167).

User Privileges

For HSM firmware older than version 7.9.0, this command requires that the HSM SO be logged in. For HSM firmware at version 7.9.0 onward, this command ***can*** stil require that the HSM SO be logged in (default), but you can remove the SO login requirement by setting HSM **Policy 58 Allow Unrestricted Metrics Access** to a value of 1.

Appliance Users with the following privileges can perform this command:

> Admin

Syntax

hsm qos metrics show [**-export** <filename>] [**-partition** <name/SN>]

Argument(s)	Shortcut	Description
-export <filename>	**-e**	File to receive the utilization data.
-partition <name/SN>	**-p**	A single partition name or serial number, or a comma-delimited list (the list can contain any combination of names and serial numbers). The command output: > displays utilization information for all valid partition names and numbers from the partition list > skips any invalid names or numbers > skips any duplicates > identifies any incorrect partition names or numbers to assist in correcting the error If the partition option is *not* specified, the command shows information for all partitions in the HSM, by default.

Example

With no arguments (output to terminal)

```
lunash:>hsm qos metrics show

Partition Name  Serial         Operation       Action      Count
==============  =============  ==========      ==========  =======
test            1230463154880  SIGN            REQUESTS               0
test            1230463154880  VERIFY          REQUESTS               0
test            1230463154880  ENCRYPT         REQUESTS               0
test            1230463154880  DECRYPT         REQUESTS               0
test            1230463154880  KEY_GENERATION  REQUESTS               0
test            1230463154880  KEY_DERIVATION  REQUESTS               0

par2            1230463154886   SIGN            REQUESTS      4700342794
par2            1230463154886   VERIFY          REQUESTS      4700342747
par2            1230463154886   ENCRYPT         REQUESTS               0
par2            1230463154886   DECRYPT         REQUESTS               0
par2            1230463154886   KEY_GENERATION  REQUESTS               0
par2            1230463154886   KEY_DERIVATION  REQUESTS               0

Summary of metrics:


SIGN            :       4700342794
VERIFY          :       4700342747
ENCRYPT         :                0
DECRYPT         :                0
KEY_DERIVATION  :                0
KEY_GENERATION  :                0
```

```
Metrics valid since 17 December 2018 11:14:47



Command Result : 0 (Success)
```

With arguments (output to file)

```
lunash:>hsm qos metrics show -export myparmetricsfile.cvs

Partition Name  Serial       Operation        Action      Count
==============  ============ ===============  =========  ============
sa7pwd78        154438865286 SIGN             REQUESTS              0
sa7pwd78        154438865286 VERIFY           REQUESTS              0
sa7pwd78        154438865286 ENCRYPT          REQUESTS              0
sa7pwd78        154438865286 DECRYPT          REQUESTS              0
sa7pwd78        154438865286 KEY_GENERATION   REQUESTS              0
sa7pwd78        154438865286 KEY_DERIVATION   REQUESTS              0

mypar01         154438865287 SIGN             REQUESTS            404
mypar01         154438865287 VERIFY           REQUESTS            404
mypar01         154438865287 ENCRYPT          REQUESTS              0
mypar01         154438865287 DECRYPT          REQUESTS              0
mypar01         154438865287 KEY_GENERATION   REQUESTS           4354
mypar01         154438865287 KEY_DERIVATION   REQUESTS              0

Summary of metrics:

SIGN            :              404
VERIFY          :              404
ENCRYPT         :                0
DECRYPT         :                0
KEY_GENERATION  :             4354
KEY_DERIVATION  :                0

Metrics valid since 17 December 2018 12:51:43

Successfully exported metrics to file.


Command Result : 0 (Success)
```

With partition names or numbers (output to terminal)

```
lunash:>hsm qos metrics show -partition test,par1,1230463154887,par2


Partition Name  Serial         Operation       Action      Count
==============  =============  ==========      ==========  =======
test            1230463154880  SIGN            REQUESTS                0
test            1230463154880  VERIFY          REQUESTS                0
test            1230463154880  ENCRYPT         REQUESTS                0
test            1230463154880  DECRYPT         REQUESTS                0
test            1230463154880  KEY_GENERATION  REQUESTS                0
test            1230463154880  KEY_DERIVATION  REQUESTS                0

par1            1230463154886   SIGN            REQUESTS            1000
par1            1230463154884   VERIFY          REQUESTS            1000
par1            1230463154884   ENCRYPT         REQUESTS               0
```

```
par1            1230463154884   DECRYPT         REQUESTS               0
par1            1230463154884   KEY_GENERATION  REQUESTS               0
par1            1230463154884   KEY_DERIVATION  REQUESTS               0

par2            1230463154887   SIGN            REQUESTS      4700342794
par2            1230463154887   VERIFY          REQUESTS      4700342747
par2            1230463154887   ENCRYPT         REQUESTS               0
par2            1230463154887   DECRYPT         REQUESTS               0
par2            1230463154887   KEY_GENERATION  REQUESTS               0
par2            1230463154887   KEY_DERIVATION  REQUESTS               0

Summary of metrics:


SIGN            :       4700343794
VERIFY          :       4700343747
ENCRYPT         :                0
DECRYPT         :                0
KEY_DERIVATION  :                0
KEY_GENERATION  :                0


Metrics valid since 17 December 2018 11:14:47

Command Result : 0 (Success)
```

> **NOTE** In the above example, "par2" is the name of the partition with serial number "1230463154887", so the duplicate designation is ignored.

With partition names or numbers with incorrect name (output to terminal)

```
lunash:>hsm qos metrics show -partition sa6pwd78,mypar01,154438865288

Error:  The following partitions are invalid and no metrics will be
        shown for them:
        sa6pwd78

        Use 'partition list' for a list of all partitions.

Partition Name  Serial         Operation       Action      Count
==============  =============  ==============  ========== =============
mypar01         154438865287   SIGN             REQUESTS            404
mypar01         154438865287   VERIFY           REQUESTS            404
mypar01         154438865287   ENCRYPT          REQUESTS              0
mypar01         154438865287   DECRYPT          REQUESTS              0
mypar01         154438865287   KEY_GENERATION   REQUESTS           4354
mypar01         154438865287   KEY_DERIVATION   REQUESTS              0

mypar02         154438865288   SIGN             REQUESTS              0
mypar02         154438865288   VERIFY           REQUESTS              0
mypar02         154438865288   ENCRYPT          REQUESTS              0
mypar02         154438865288   DECRYPT          REQUESTS              0
mypar02         154438865288   KEY_GENERATION   REQUESTS           1714
mypar02         154438865288   KEY_DERIVATION   REQUESTS              0

Summary of metrics:
SIGN            :              404
```

```
VERIFY          :              404
ENCRYPT         :                0
DECRYPT         :                0
KEY_GENERATION  :             6068
KEY_DERIVATION  :                0

Metrics valid since 17 December 2018 22:51:43

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

hsm restart

Restart the HSM without rebooting the appliance. This command closes out any login status and open sessions.

Syntax

hsm restart [**-force**]

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

Example

```
lunash:>hsm restart

WARNING !!  This command will restart the HSM card.

If you are sure that you wish to proceed, then type 'proceed', otherwise type 'quit'
> proceed
Proceeding...
Restarting HSM card in progress. Please wait...

Command Result : 0 (Success)
```

hsm restore

> **NOTE** This command was deprecated, and is no longer available in Luna Network HSM 7 Appliance Software 7.7.0 and newer. It should not be used in older software and firmware versions.

hsm selfTest

Test the cryptographic capabilities of the HSM.

User Privileges

Users with the following privileges can perform this command:

- Admin
- Operator
- Monitor

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 (Luna 4.x) cloning domain on a Luna 7 HSM for the purposes of key migration:

> 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 Network HSM.

> For multifactor quorum-authenticated HSMs, this is the cloning domain secret on the red Luna PED for the legacy multifactor quorum-authenticated token HSM whose contents are to be migrated to the Luna Network HSM 7.

Your target Luna Network HSM 7 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 Network HSM 7 is attached until the HSM is reinitialized.

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

You can now migrate objects between password-authenticated and multifactor quorum-authenticated HSMs by setting multiple cloning domains on a partition. See Universal Cloning.

See About the Key Migration Guide for information on the possible combinations of source (legacy) tokens/HSMs and target (modern) HSMs and the disposition of token objects from one to the other.

User Privileges

Users with the following privileges can perform this command:

> Admin

Syntax

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

Argument(s)	Shortcut	Description
-domain <domain>	**-d**	Specifies the Legacy Cloning Domain name. This parameter is required on password-authenticated HSMs. It is ignored on multifactor quorum-authenticated HSMs, which retrieve 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 Luna PED prompts for the legacy red domain PED key (notice mention of "raw data" in the PED message).

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

hsm show

Display a list showing the current configuration of the HSM.

User Privileges

Users with the following privileges can perform this command:

- Admin
- Operator
- Monitor

Syntax

hsm show

Example for Luna HSM Firmware 7.8.0

```
[docs_lab] lunash:>hsm show


   Appliance Details:
   ==================
   Software Version:                   7.7.2-651


   HSM Details:
   ============
   HSM Label:                          myLuna
   Serial #:                           532018
   Bootloader:                         1.1.5
   Firmware:                           7.8.0
   HSM Model:                          Luna K7
   HSM Part Number:                    808-000073-001
   Authentication Method:              Password
   HSM Admin login status:             Logged In
   HSM Admin login attempts left:      3 before HSM zeroization!
   RPV Initialized:                    No
   Audit Role Initialized:             No
   Remote Login Initialized:           No
   Manually Zeroized:                  No
   Secure Transport Mode:              No
   HSM Tamper State:                   No tamper(s)

   Partitions created on HSM:
   ==========================
   Partition:        1238700701509, Name: LNH_143.156_kpar01
   Partition:        1238700701510, Name: LNH_143.156_kpar02
   Partition:        1238700701512, Name: LNH_143.156_kpar-v0-03
   Partition:        1238700701513, Name: LNH_143.156_kpar-v1-04

   Number of partitions allowed:       100
   Number of partitions created:       4

   FIPS 140-2 Operation:
```

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

   System Times:
   =============
   HSM Time:                          Wed Jun 01 18:13:13 UTC 2022
   Host Time:                         Wed Jun 01 18:13:12 UTC 2022
   Difference:                        1 sec

   HSM Storage Information:
   ========================
   Maximum HSM Storage Space (Bytes):  67108864
   Space In Use (Bytes):               2000298
   Free Space Left (Bytes):            65108566

   Environmental Information on HSM:
   =================================
   Battery Voltage:                    3.093 V
   Battery Warning Threshold Voltage:  2.750 V
   System Temp:                        40 deg. C
   System Temp Warning Threshold:      75 deg. C


   Functionality Module HW:            FM Ready
   ========================

Command Result : 0 (Success)
```

> **NOTE** The **System Times** field does not appear until the HSM time has been synchronized with the appliance system using lunash:> "hsm time sync" on page 286.

Example for Luna HSM Firmware 7.7.0

```
lunash:>hsm show


   Appliance Details:
   ==================
   Software Version:                7.7.0


   HSM Details:
   ============
   HSM Label:                         myLuna
   Serial #:                          532018
   Bootloader:                        1.1.2
   Firmware:                          7.7.0
   HSM Model:                         Luna K7
   HSM Part Number:                   808-000066-001
   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
   Secure Transport Mode:             No
```

```
   HSM Tamper State:                    No tamper(s)

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


   Number of partitions allowed:        10
   Number of partitions created:        0

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

   HSM Storage Information:
   ========================
   Maximum HSM Storage Space (Bytes):   67108864
   Space In Use (Bytes):                671120
   Free Space Left (Bytes):             66437744

   Environmental Information on HSM:
   =================================
   Battery Voltage:                     3.093 V
   Battery Warning Threshold Voltage:   2.750 V
   System Temp:                         46 deg. C
   System Temp Warning Threshold:       75 deg. C


   Functionality Module HW:             FM Ready
   ========================

Command Result : 0 (Success)
```

> **NOTE** Starting with Luna HSM Firmware 7.7.0, this command reports "Space in Use" (example 671120) bytes of overhead, at the HSM Storage heading, after initialization.

hsm showPolicies

Display the current settings for all HSM capabilities and policies, or optionally restrict the listing to only the policies that are configurable. Include the **-exporttemplate** option to export the current state of all policies to a template file. For a complete list of HSM capabilities and policies, refer to HSM Capabilities and Policies.

User Privileges

Users with the following privileges can perform this command:

- Admin
- Operator
- Monitor

Syntax

hsm showPolicies [**-configonly**] [**-exporttemplate** <filename>]

Argument(s)	Shortcut	Description
-configonly	**-c**	Restrict the list to configurable policies only.
-exporttemplate <filename>	**-e**	Export the current state of all HSM policies to a template file. This feature requires minimum Luna HSM Firmware 7.1.0 and Luna Network HSM 7 Appliance Software 7.1.0.

Example with HSM firmware older than 7.7.0

```
lunash:>hsm showPolicies


   HSM Label:   myLunaHSM
   Serial #:    66331
   Firmware:    7.4.0

   The following capabilities describe this HSM, and cannot be altered
   except via firmware or capability updates.

   Description                              Value
   ===========                              =====
   Enable PIN-based authentication          Allowed
   Enable PED-based authentication          Disallowed
   Performance level                        15
   Enable domestic mechanisms & key sizes   Allowed
   Enable masking                           Disallowed
   Enable cloning                           Allowed
   Enable full (non-backup) functionality   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 forcing user PIN change            Allowed
Enable portable masking key               Allowed
Enable partition groups                   Disallowed
Enable remote PED usage                   Disallowed
HSM non-volatile storage space            33554432
Enable unmasking                          Allowed
Maximum number of partitions              100
Enable Single Domain                      Disallowed
Enable Unified PED Key                    Disallowed
Enable MofN                               Disallowed
Enable small form factor backup/restore   Disallowed
Enable Secure Trusted Channel             Allowed
Enable decommission on tamper             Allowed
Enable partition re-initialize            Disallowed
Enable low level math acceleration        Allowed
Enable Fast-Path                          Disallowed
Allow Disabling Decommission              Allowed
Enable Tunnel Slot                        Disallowed
Enable Controlled Tamper Recovery         Allowed
Enable Partition Utilization Metrics      Allowed
Enable Functionality Modules              Allowed
Enable SMFS Auto Activation               Allowed
Allow Restricting FM Privilege Level      Allowed
Allow encrypting of keys from FM to HSM   Allowed

The following policies are set due to current configuration of
this HSM and cannot be altered directly by the user.

Description                               Value
===========                               =====
PIN-based authentication                  True


The following policies describe the current configuration of
this HSM and may be changed by the HSM Administrator.

Changing policies marked "destructive" will erase all HSM partitions
on the HSM.

IMPORTANT NOTE: Changing policy 46 (Disable Decommission) will erase
all partitions AND zeroize your HSM.

Description                               Value        Code      Destructive
===========                               =====        ====      ===========
Allow cloning                             On           7         Yes
Allow non-FIPS algorithms                 On           12        Yes
SO can reset partition PIN                Off          15        Yes
Allow network replication                 On           16        No
Force user PIN change after set/reset     On           21        No
Allow offboard storage                    On           22        Yes
Allow unmasking                           On           30        No
Current maximum number of partitions      100          33        No
Allow Secure Trusted Channel              Off          39        No
Decommission on tamper                    Off          40        Yes
Allow low level math acceleration         On           43        No
Disable Decommission                      Off          46        Yes
Do Controlled Tamper Recovery             On           48        No
```

```
   Allow Partition Utilization Metrics      Off          49        No
   Allow Functionality Modules              Off          50        Yes
   Allow SMFS Auto Activation               Off          51        Yes
   Restrict FM Privilege Level              Off          52        Yes
   Encrypt keys passing from FM to HSM      Off          53        Yes


Command Result : 0 (Success)
```

Example with Luna HSM Firmware 7.7.0 or newer

```
lunash:>hsm showpolicies


   HSM Label:   myLunaPWD
   Serial #:    66331
   Firmware:    7.7.0

   The following capabilities describe this HSM, and cannot be altered
   except via firmware or capability updates.

   Description                              Value
   ===========                              =====
   Enable PIN-based authentication          Allowed
   Enable PED-based authentication          Disallowed
   Performance level                        15
   Enable domestic mechanisms & key sizes   Allowed
   Enable masking                           Allowed
   Enable cloning                           Allowed
   Enable full (non-backup) functionality   Allowed
   Enable non-FIPS algorithms               Allowed
   Enable SO reset of partition PIN         Allowed
   Enable network replication               Allowed
   Enable Korean Algorithms                 Disallowed
   FIPS evaluated                           Disallowed
   Manufacturing Token                      Disallowed
   Enable forcing user PIN change           Allowed
   Enable portable masking key              Allowed
   Enable partition groups                  Disallowed
   Enable remote PED usage                  Disallowed
   HSM non-volatile storage space           58720256
   Enable unmasking                         Allowed
   Maximum number of partitions             10
   Enable Single Domain                     Disallowed
   Enable Unified PED Key                   Disallowed
   Enable MofN                              Disallowed
   Enable small form factor backup/restore  Disallowed
   Enable decommission on tamper            Allowed
   Enable partition re-initialize           Disallowed
   Enable low level math acceleration       Allowed
   Enable Fast-Path                         Disallowed
   Allow Disabling Decommission             Allowed
   Enable Controlled Tamper Recovery        Allowed
   Enable Partition Utilization Metrics     Allowed
   Enable Functionality Modules             Allowed
   Enable SMFS Auto Activation              Allowed
   Allow Restricting FM Privilege Level     Allowed
   Allow encrypting of keys from FM to HSM  Allowed
```

```
   The following policies are set due to current configuration of
   this HSM and cannot be altered directly by the user.

   Description                              Value
   ===========                              =====
   PIN-based authentication                 True


   The following policies describe the current configuration of
   this HSM and may be changed by the HSM Administrator.

   Changing policies marked "destructive" will erase all HSM partitions
   on the HSM.

   IMPORTANT NOTE: Changing policy 46 (Disable Decommission) will erase
   all partitions AND zeroize your 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               Off          15        Yes
   Allow network replication                On           16        No
   Force user PIN change after set/reset    On           21        No
   Allow offboard storage                   On           22        Yes
   Allow unmasking                          On           30        No
   Current maximum number of partitions     10           33        No
   Decommission on tamper                   Off          40        Yes
   Allow low level math acceleration        On           43        No
   Disable Decommission                     Off          46        Yes
   Do Controlled Tamper Recovery            On           48        No
   Allow Partition Utilization Metrics      Off          49        No
   Allow Functionality Module               Off          50        Yes
   Allow SMFS Auto Activation               Off          51        Yes
   Restrict FM Privilege Level              Off          52        Yes
   Encrypt keys passing from FM to HSM      Off          53        Yes


Command Result : 0 (Success)
```

Example with Luna HSM Firmware 7.7.2 and newer

```
lunash:>hsm showpolicies


   HSM Label:   myLunaPWD
   Serial #:    66331
   Firmware:    7.7.0

   The following capabilities describe this HSM, and cannot be altered
   except via firmware or capability updates.

   Description                              Value
   ===========                              =====
   Enable PIN-based authentication          Allowed
```

```
Enable PED-based authentication          Disallowed
Performance level                        15
Enable domestic mechanisms & key sizes   Allowed
Enable masking                           Allowed
Enable cloning                           Allowed
Enable full (non-backup) functionality   Allowed
Enable non-FIPS algorithms               Allowed
Enable SO reset of partition PIN         Allowed
Enable network replication               Allowed
Enable Korean Algorithms                 Disallowed
FIPS evaluated                           Disallowed
Manufacturing Token                      Disallowed
Enable forcing user PIN change           Allowed
Enable portable masking key              Allowed
Enable partition groups                  Disallowed
Enable remote PED usage                  Disallowed
HSM non-volatile storage space           58720256
Enable unmasking                         Allowed
Maximum number of partitions             10
Enable Single Domain                     Disallowed
Enable Unified PED Key                   Disallowed
Enable MofN                              Disallowed
Enable small form factor backup/restore  Disallowed
Enable decommission on tamper            Allowed
Enable partition re-initialize           Disallowed
Enable low level math acceleration       Allowed
Enable Fast-Path                         Disallowed
Allow Disabling Decommission             Allowed
Enable Controlled Tamper Recovery        Allowed
Enable Partition Utilization Metrics     Allowed
Enable Functionality Modules             Allowed
Enable SMFS Auto Activation              Allowed
Allow Restricting FM Privilege Level     Allowed
Allow encrypting of keys from FM to HSM  Allowed
Enable User Defined ECC Curves           Allowed


The following policies are set due to current configuration of
this HSM and cannot be altered directly by the user.

Description                              Value
===========                              =====
PIN-based authentication                 True


The following policies describe the current configuration of
this HSM and may be changed by the HSM Administrator.

Changing policies marked "destructive" will erase all HSM partitions
on the HSM.

IMPORTANT NOTE: Changing policy 46 (Disable Decommission) will erase
all partitions AND zeroize your 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               Off         15        Yes
   Allow network replication                On          16        No
   Force user PIN change after set/reset    On          21        No
   Allow offboard storage                   On          22        Yes
   Allow unmasking                          On          30        No
   Current maximum number of partitions     10          33        No
   Decommission on tamper                   Off         40        Yes
   Allow low level math acceleration        On          43        No
   Disable Decommission                     Off         46        Yes
   Do Controlled Tamper Recovery            On          48        No
   Allow Partition Utilization Metrics      Off         49        No
   Allow Functionality Module               Off         50        Yes
   Allow SMFS Auto Activation               Off         51        Yes
   Restrict FM Privilege Level              Off         52        Yes
   Encrypt keys passing from FM to HSM      Off         53        Yes
   Allow User Defined ECC Curves            On          56        Yes


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.

> **NOTE** The STC admin channel is configurable using Luna Network HSM 7 Appliance Software 7.4.0 and older, and Luna HSM Firmware 7.4.2 and older. This feature is not available in Luna HSM Firmware 7.7.0 and newer.

Syntax

hsm stc

activationtimeout
cipher
disable
enable
hmac
identity
partition
rekeythreshold
status

Argument(s)	Shortcut	Description
activationtimeout	**a**	Set and display the activation timeout for an STC link. See "hsm stc activationtimeout" on page 245.
cipher	**ci**	Enable, disable, and show the use of a symmetric encryption cipher algorithm for data encryption on the link. See "hsm stc cipher" on page 248.
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 252.
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 253.
hmac	**h**	Enable, disable, and display 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" on page 254.

Argument(s)	Shortcut	Description
identity	**i**	Manage the HSM SO client identity for the LunaSH STC client token. See "hsm stc identity" on page 258.
partition	**p**	Export the specified partition's public key to a file, or display that public key. See "hsm stc partition" on page 268.
rekeythreshold	**rek**	Set or display the key life for the symmetric key used to encrypt data on the STC link for the specified partition. See "hsm stc rekeythreshold" on page 271.
status	**s**	Display status and configuration information for an STC link. See "hsm stc status" on page 274.

hsm stc activationtimeout

Display and set the activation timeout for STC.

> **NOTE** The STC admin channel is configurable using Luna Network HSM 7 Appliance Software 7.4.0 and older, and Luna HSM Firmware 7.4.2 and older. This feature is not available in Luna HSM Firmware 7.7.0 and newer.

Syntax

hsm stc activationtimeout

set
show

Argument(s)	Shortcut	Description
set	**se**	Set the activation timeout for an STC link. See "hsm stc activationTimeOut set" on the next page.
show	**sh**	Display the STC link activation timeout for the specified partition. See "hsm stc activationTimeOut show" on page 247.

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.

> **NOTE** The STC admin channel is configurable using Luna Network HSM 7 Appliance Software 7.4.0 and older, and Luna HSM Firmware 7.4.2 and older. This feature is not available in Luna HSM Firmware 7.7.0 and newer.

User Privileges

Users with the following privileges can perform this command:

- Admin
- Operator

Syntax

hsm stc activationTimeOut set -time <timeout>

Argument(s)	Shortcut	Description
-time <timeout>	**-t**	Specifies the activation timeout, in seconds. **Range:** 1 to 240 **Default:** 120

Example

```
lunash:>hsm stc activationTimeOut set -time 30

Successfully changed the activation timeout for HSM to 30 seconds.


Command Result : 0 (Success)
```

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.

> **NOTE** The STC admin channel is configurable using Luna Network HSM 7 Appliance Software 7.4.0 and older, and Luna HSM Firmware 7.4.2 and older. This feature is not available in Luna HSM Firmware 7.7.0 and newer.

User Privileges

Users with the following privileges can perform this command:

- Admin
- Operator

Syntax

hsm stc activationTimeOut show

Example

```
lunash:>hsm stc activationTimeOut show

The channel activation timeout for HSM is 120 seconds.


Command Result : 0 (Success)
```

hsm stc cipher

View, enable, and disable STC cipher algorithms.

> **NOTE** The STC admin channel is configurable using Luna Network HSM 7 Appliance Software 7.4.0 and older, and Luna HSM Firmware 7.4.2 and older. This feature is not available in Luna HSM Firmware 7.7.0 and newer.

Syntax

hsm stc cipher

disable
enable
show

Argument(s)	Shortcut	Description
disable	**d**	Disable the use of a symmetric encryption cipher algorithm for data encryption on the link. See "hsm stc cipher disable" on the next page.
enable	**e**	Enable the use of a symmetric encryption cipher algorithm for data encryption on the link. See "hsm stc cipher enable" on page 250.
show	**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 251.

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.

> **NOTE** The STC admin channel is configurable using Luna Network HSM 7 Appliance Software 7.4.0 and older, and Luna HSM Firmware 7.4.2 and older. This feature is not available in Luna HSM Firmware 7.7.0 and newer.

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 251 to show which ciphers are currently enabled/disabled.

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

User Privileges

Users with the following privileges can perform this command:

- Admin
- Operator

Syntax

hsm stc cipher disable {**-all** | **-id** <cipher_id>} [**-force**]

Argument(s)	Shortcut	Description
-all	**-a**	Disable all ciphers.
-id <cipher_id>	**-i**	Specifies the numerical identifier of the cipher you want to disable, as listed using the command "hsm stc cipher show" on page 251.
-force	**-f**	Force the action without prompting.

Example

```
lunash:>hsm stc cipher disable -id 3

AES 256 Bit with Cipher Block Chaining is now disabled.


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.

> **NOTE** The STC admin channel is configurable using Luna Network HSM 7 Appliance Software 7.4.0 and older, and Luna HSM Firmware 7.4.2 and older. This feature is not available in Luna HSM Firmware 7.7.0 and newer.

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 the next page to show which ciphers are currently enabled/disabled.

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

User Privileges

Users with the following privileges can perform this command:

- Admin
- Operator

Syntax

hsm stc cipher enable {**-all** | **-id** <cipher_id>}

Argument(s)	Shortcut	Description
-all	**-a**	Enable all ciphers.
-id <cipher_id>	**-i**	Specifies the numerical identifier of the cipher you want to use, as listed using the command "hsm stc cipher show" on the next page.

Example

```
lunash:>hsm stc cipher enable -id  3

AES 256 Bit with Cipher Block Chaining is now enabled.


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.

> **NOTE** The STC admin channel is configurable using Luna Network HSM 7 Appliance Software 7.4.0 and older, and Luna HSM Firmware 7.4.2 and older. This feature is not available in Luna HSM Firmware 7.7.0 and newer.

User Privileges

Users with the following privileges can perform this command:

- Admin
- Operator

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 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.

> **NOTE** The STC admin channel is configurable using Luna Network HSM 7 Appliance Software 7.4.0 and older, and Luna HSM Firmware 7.4.2 and older. This feature is not available in Luna HSM Firmware 7.7.0 and newer.

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.

User Privileges

Users with the following privileges can perform this command:

- Admin
- Operator

Syntax

hsm stc disable [**-force**]

Argument(s)	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** The STC admin channel is configurable using Luna Network HSM 7 Appliance Software 7.4.0 and older, and Luna HSM Firmware 7.4.2 and older. This feature is not available in Luna HSM Firmware 7.7.0 and newer.
>
> 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.

User Privileges

Users with the following privileges can perform this command:

- Admin
- Operator

Syntax

hsm stc enable [**-force**]

Argument(s)	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

Enable, disable, and show STC HMAC algorithms.

> **NOTE** The STC admin channel is configurable using Luna Network HSM 7 Appliance Software 7.4.0 and older, and Luna HSM Firmware 7.4.2 and older. This feature is not available in Luna HSM Firmware 7.7.0 and newer.

Syntax

hsm stc hmac

disable
enable
show

Argument(s)	Shortcut	Description
disable	**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 the next page.
enable	**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 256.
show	**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 257.

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.

> **NOTE** The STC admin channel is configurable using Luna Network HSM 7 Appliance Software 7.4.0 and older, and Luna HSM Firmware 7.4.2 and older. This feature is not available in Luna HSM Firmware 7.7.0 and newer.

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 257 to show which HMAC message digest algorithms are currently enabled/disabled.

> **NOTE** You cannot disable all HMAC message digest algorithms.

User Privileges

Users with the following privileges can perform this command:

- Admin
- Operator

Syntax

hsm stc hmac disable -id <hmac_id>

Argument(s)	Shortcut	Description
-id <hmac_id>	**-i**	Specifies the numerical identifier of the HMAC algorithm you want to disable, as listed using the command "hsm stc hmac show" on page 257.

Example

```
lunash:>hsm stc hmac disable -id 0

HMAC with SHA 256 Bit is now disabled.


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.

> **NOTE** The STC admin channel is configurable using Luna Network HSM 7 Appliance Software 7.4.0 and older, and Luna HSM Firmware 7.4.2 and older. This feature is not available in Luna HSM Firmware 7.7.0 and newer.

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 the next page to show which HMAC message digest algorithms are currently enabled/disabled.

> **NOTE** You must enable at least one HMAC message digest algorithm.

User Privileges

Users with the following privileges can perform this command:

- Admin
- Operator

Syntax

hsm stc hmac enable -id <hmac_id>

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

Example

```
lunash:>hsm stc hmac enable -id 0

HMAC with SHA 256 Bit is now enabled.


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.

> **NOTE** The STC admin channel is configurable using Luna Network HSM 7 Appliance Software 7.4.0 and older, and Luna HSM Firmware 7.4.2 and older. This feature is not available in Luna HSM Firmware 7.7.0 and newer.

User Privileges

Users with the following privileges can perform this command:

- Admin
- Operator

Syntax

hsm stc hmac show

Example

```
lunash:>hsm stc hmac show

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


 HMAC ID      HMAC Name                                  Enabled
_____________________________________________________________________

 0            HMAC with SHA 256 Bit                      Yes

 1            HMAC with SHA 512 Bit                      Yes


Command Result : 0 (Success)
```

hsm stc identity

Create and manage client identities for STC.

> **NOTE** The STC admin channel is configurable using Luna Network HSM 7 Appliance Software 7.4.0 and older, and Luna HSM Firmware 7.4.2 and older. This feature is not available in Luna HSM Firmware 7.7.0 and newer.

Syntax

hsm stc identity

create
delete
initialize
partition
show

Argument(s)	Shortcut	Description
create	**c**	Create a STC client identity for the LunaSH client. See "hsm stc identity create" on the next page.
delete	**d**	Delete the LunaSH STC client identity. See "hsm stc identity delete" on page 260.
initialize	**i**	Initialize the LunaSH STC client token. See "hsm stc identity initialize" on page 262.
partition	**p**	Commands allowing you to register or de-register the HSM SO partition identity public key with the LunaSH STC client token. See "hsm stc identity partition" on page 264.
show	**s**	Display the client name, public key hash, and registered partitions for the LunaSH STC client token. See "hsm stc identity show" on page 267.

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**.

> **NOTE** To protect the integrity of any existing STC links, you cannot execute this command if HSM policy 39: Allow Secure Trusted Channel is enabled.

User Privileges

Users with the following privileges can perform this command:

- Admin
- Operator

Syntax

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

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

Example

```
lunash:>hsm stc identity create

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


Command Result : 0 (Success)
```

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.

> **NOTE** The STC admin channel is configurable using Luna Network HSM 7 Appliance Software 7.4.0 and older, and Luna HSM Firmware 7.4.2 and older. This feature is not available in Luna HSM Firmware 7.7.0 and newer.

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

This command does the following, in the order specified:

1. Deletes the 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.

> **NOTE** To protect the integrity of any existing STC links, you cannot execute this command if **HSM policy 39: Allow Secure Trusted Channel** is enabled.

User Privileges

Users with the following privileges can perform this command:

> Admin

> Operator

Syntax

stc identity delete [**-force**]

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

Example

```
lunash:>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.

Command Result : 0 (Success)
```

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.

> **NOTE** The STC admin channel is configurable using Luna Network HSM 7 Appliance Software 7.4.0 and older, and Luna HSM Firmware 7.4.2 and older. This feature is not available in Luna HSM Firmware 7.7.0 and newer.

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.

> **NOTE** To protect the integrity of any existing STC links, you cannot execute this command if **HSM policy 39: Allow Secure Trusted Channel** is enabled.

User Privileges

Users with the following privileges can perform this command:

- Admin
- Operator

Syntax

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

Argument(s)	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:              71e31e3c6366caf62327225587c4c69cfe080112
Registered Partition:              No


Re-initialization will delete the client identity.

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

Successfully re-initialized the client token.
```

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

hsm stc identity partition

Register and deregister HSM SO partition identities for STC.

> **NOTE** The STC admin channel is configurable using Luna Network HSM 7 Appliance Software 7.4.0 and older, and Luna HSM Firmware 7.4.2 and older. This feature is not available in Luna HSM Firmware 7.7.0 and newer.

Syntax

hsm stc identity partition

deregister
register

Argument(s)	Shortcut	Description
deregister	**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 the next page.
register	**r**	Register the HSM SO partition identity public key with the LunaSH STC client token. See "hsm stc identity partition register" on page 266.

 Copyright 2001-2025 Thales Group

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.

> **NOTE** The STC admin channel is configurable using Luna Network HSM 7 Appliance Software 7.4.0 and older, and Luna HSM Firmware 7.4.2 and older. This feature is not available in Luna HSM Firmware 7.7.0 and newer.

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.

> **NOTE** To protect the integrity of any existing STC links, you cannot execute this command if **HSM policy 39: Allow Secure Trusted Channel** is enabled.

User Privileges

Users with the following privileges can perform this command:

- Admin
- Operator

Syntax

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

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

Example

```
lunash:>hsm stc identity partition deregister


Are you sure you want to deregister the partition identity?

          Type 'proceed' to continue, or 'quit"
          to quit now.
          > proceed
Successfully deregistered the partition identity from the client token.

Command Result : 0 (Success)
```

hsm stc identity partition register

Register the HSM SO partition 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.

> **NOTE** The STC admin channel is configurable using Luna Network HSM 7 Appliance Software 7.4.0 and older, and Luna HSM Firmware 7.4.2 and older. This feature is not available in Luna HSM Firmware 7.7.0 and newer.

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.

User Privileges

Users with the following privileges can perform this command:

- Admin
- Operator

Syntax

hsm stc identity partition register -file <filename>

Argument(s)	Shortcut	Description
-file <filename>	**-f**	Specifies the partition public key file.

Example

```
lunash:>hsm stc identity partition register -file 66331.pid

Successfully registered the partition identity to the client token.


Command Result : 0 (Success)
```

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.

> **NOTE** The STC admin channel is configurable using Luna Network HSM 7 Appliance Software 7.4.0 and older, and Luna HSM Firmware 7.4.2 and older. This feature is not available in Luna HSM Firmware 7.7.0 and newer.

User Privileges

Users with the following privileges can perform this command:

> Admin

> Operator

Syntax

hsm stc identity show

Example

```
lunash:>hsm stc identity show

Public Key SHA1 Hash:              b28a5876e839715fc62eb3fde264f6f612ef9841
Registered Partition Identity:
   Partition Serial Number:        66331
   Partition Public Key SHA1 Hash: 71a453e3aecf4938b2a04b5096c329645eb5a322


Command Result : 0 (Success)
```

hsm stc partition

View the public key for the HSM SO partition, and export that public key to a file.

> **NOTE** The STC admin channel is configurable using Luna Network HSM 7 Appliance Software 7.4.0 and older, and Luna HSM Firmware 7.4.2 and older. This feature is not available in Luna HSM Firmware 7.7.0 and newer.

Syntax

hsm stc partition

export
show

Argument(s)	Shortcut	Description
export	**e**	Export the specified partition's public key to a file. See "hsm stc partition export" on the next page.
show	**s**	Display the public key and serial number for the current partition. See "hsm stc partition show" on page 270.

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.

> **NOTE** The STC admin channel is configurable using Luna Network HSM 7 Appliance Software 7.4.0 and older, and Luna HSM Firmware 7.4.2 and older. This feature is not available in Luna HSM Firmware 7.7.0 and newer.

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

User Privileges

Users with the following privileges can perform this command:

- Admin
- Operator

Syntax

hsm stc partition export

Example

```
lunash:>hsm stc partition export

Successfully exported partition identity for HSM to file: 66331.pid


Command Result : 0 (Success)
```

hsm stc partition show

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

> **NOTE** The STC admin channel is configurable using Luna Network HSM 7 Appliance Software 7.4.0 and older, and Luna HSM Firmware 7.4.2 and older. This feature is not available in Luna HSM Firmware 7.7.0 and newer.

User Privileges

Users with the following privileges can perform this command:

- Admin
- Operator

Syntax

hsm stc partition show

Example

```
lunash:>hsm stc partition show

Partition Serial Number:                 66331
Partition Identity Public Key SHA1 Hash: 71a453e3aecf4938b2a04b5096c329645eb5a322


Command Result : 0 (Success)
```

hsm stc rekeythreshold

Display and set the rekey threshold for the symmetric key used to encrypt data on the STC admin channel.

> **NOTE** The STC admin channel is configurable using Luna Network HSM 7 Appliance Software 7.4.0 and older, and Luna HSM Firmware 7.4.2 and older. This feature is not available in Luna HSM Firmware 7.7.0 and newer.

Syntax

hsm stc rekeythreshold

set
show

Argument(s)	Shortcut	Description
set	**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 the next page.
show	**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 273.

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.

> **NOTE** The STC admin channel is configurable using Luna Network HSM 7 Appliance Software 7.4.0 and older, and Luna HSM Firmware 7.4.2 and older. This feature is not available in Luna HSM Firmware 7.7.0 and newer.

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.

User Privileges

Users with the following privileges can perform this command:

- Admin
- Operator

Syntax

hsm stc rekeyThreshold set -value <threshold>

Argument(s)	Shortcut	Description
-value <key_life>	**-v**	An integer that specifies the key life for the STC symmetric key, in millions of messages. **Range:** 0 - 4000 **Default:** 400

Example

```
lunash:>hsm stc rekeyThreshold set -value 500

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


Command Result : 0 (Success)
```

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.

> **NOTE** The STC admin channel is configurable using Luna Network HSM 7 Appliance Software 7.4.0 and older, and Luna HSM Firmware 7.4.2 and older. This feature is not available in Luna HSM Firmware 7.7.0 and newer.

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.

User Privileges

Users with the following privileges can perform this command:

- Admin
- Operator

Syntax

hsm stc rekeyThreshold show

Example

```
lunash:>hsm stc rekeyThreshold show

Current rekey threshold for HSM is 400 million messages.


Command Result : 0 (Success)
```

hsm stc status

View the current STC policy activated on the HSM.

> **NOTE** The STC admin channel is configurable using Luna Network HSM 7 Appliance Software 7.4.0 and older, and Luna HSM Firmware 7.4.2 and older. This feature is not available in Luna HSM Firmware 7.7.0 and newer.

User Privileges

Users with the following privileges can perform this command:

- Admin
- Operator
- Monitor

Syntax

hsm stc status

Example

```
lunash:>hsm stc status

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


Command Result : 0 (Success)
```

hsm stm

Configure, or display information about Secure Transport Mode (STM).

STM allows you to verify that an HSM has not been tampered while in transit or storage. STM is optional. When invoked, STM provides comparison strings that you can visually verify, and imposes a pause during the STM recover operation where you indicate that you have seen the command output and decided to resume using the HSM, or to leave the HSM in Secure Transport Mode. For more information, see Secure Transport Mode.

Syntax

hsm stm

recover
show
transport

Argument(s)	Shortcut	Description
recover	**r**	Recover an HSM that has been placed in STM. See "hsm stm recover" on the next page.
show	**s**	Displays the current STM state. See "hsm stm show" on page 278.
transport	**t**	Place the HSM in STM. See "hsm stm transport" on page 279.

 Copyright 2001-2025 Thales Group

hsm stm recover

Recover the HSM from Secure Transport Mode (STM). If the HSM is in initialized state, you must be logged in as HSM SO to recover from STM; if the HSM is zeroized, no login is required.

When you enter this command, enter the random user string that was generated when the HSM was put into STM. A verification string will be displayed:

> If the verification string generated matches the string that was displayed when the HSM was put into STM (see "hsm stm transport" on page 279), the HSM was not interfered with or tampered while in STM.

> If the verification string generated does not match the verification string generated when you placed the HSM in STM, this might indicate that the HSM has been interfered with or tampered while in STM, or that an incorrect random user string has been entered.

> **NOTE** The random user string is for verification purposes only. Entering a different string will not prevent you from recovering the HSM from STM.

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

> **CAUTION!** Use the LunaCM command role deactivate from a connected client, to deactivate *each role*, by name, for *each partition* on the HSM, before issuing command "hsm stm transport" on page 279.
>
> Failure to do so can result in mismatch when the generated strings are later compared during Secure Transport Mode recovery.

User Privileges

Users with the following privileges can perform this command:

> Admin

> Operator

Syntax

hsm stm recover -randomuserstring <string>

Argument(s)	Shortcut	Description
-randomuserstring <string>	**-r**	To confirm that the HSM was not tampered with while in STM, enter the random user string generated when it was placed in STM, in the format XXXX-XXXX-XXXX-XXXX.

Example

```
lunash:>hsm stm recover -randomuserstring 4CEd-4HX7-J/YW-pCX6

        Attempting to recover from Secure Transport Mode...
        Calculating the verification string (may take a few seconds)...
```

```
        Verification String: 59bt-3CXF-7/Tt-qKTx

CAUTION: You are attempting to recover the HSM from Secure Transport Mode. If the Verification
         string does not match the one you were provided out-of-band, there may be an issue
         with the HSM. Type 'quit' at the prompt to remain in Secure Transport Mode.

          If the verification strings match, or if you wish to bypass this check,
          type 'proceed' to recover from Secure Transport Mode.

          Type 'proceed' to continue, or 'quit' to quit now.
          > proceed
        Successfully recovered from Secure Transport Mode.

Command Result : 0 (Success)
```

hsm stm show

Display the current Secure Transport Mode (STM) state. The state is NO or YES, as follows:

NO	The HSM is not in STM, and is ready for use.
YES	The HSM is in STM. You must use the command "hsm stm recover" on page 276 to exit STM before you can use the HSM.

User Privileges

Users with the following privileges can perform this command:

> Admin

> Operator

> Monitor

Syntax

hsm stm show

Example

```
lunash:>hsm stm show

   Secure Transport Mode: NO


Command Result : No Error
```

hsm stm transport

Place the HSM in Secure Transport Mode (STM). You need to be logged in as the HSM SO to issue this command.

When you enter this command, two strings are displayed: a verification string and a random user string. Record both of these to confirm later that the HSM was not tampered with while in STM. When you recover from STM, enter the random user string and compare the generated verification string to the original one you received. If the strings match, the HSM has not been tampered while in STM (see "hsm stm recover" on page 276).

> **CAUTION!** Using a multifactor quorum-authenticated HSM with Luna HSM Firmware 7.7.1-20 or older, ensure that CO, LCO and CU roles are deactivated *on all partitions* before placing the HSM in Secure Transport Mode (see Deactivating a Role). If any roles are still activated when STM is set, this can result in mismatched verification strings during STM recovery.
>
> This is not necessary using Luna HSM Firmware 7.7.2 or newer; placing the HSM in STM automatically logs out and deactivates these roles.
>
> The roles can be logged in and reactivated manually after STM recovery.

User Privileges

Users with the following privileges can perform this command:

- Admin
- Operator

Syntax

hsm stm transport

Example

```
lunash:>hsm stm transport


WARNING !!  You are about to configure the HSM in secure transport mode.
            If you proceed, the HSM will be inoperable until it is recovered with hsm stm
recover command.
            If you are sure that you wish to proceed, then type 'proceed', otherwise type
'quit'.

> proceed
Proceeding...

Configuring the HSM for secure transport mode...

Record the displayed verification & random user strings. These are required to recover from
Secure Transport Mode.


        Verification String: 59bt-3CXF-7/Tt-qKTx
```

```
        Random User  String: 4CEd-4HX7-J/YW-pCX6

HSM is now in Secure Transport Mode.


Command Result : 0 (Success)
```

hsm supportInfo

Generate the **supportInfo.txt** file. The **supportInfo.txt** file includes detailed information about the state and settings of the HSM, as well as other important appliance information, such as the network settings and negotiated link status. You must transfer the file from the Luna appliance to your client using **pscp** or **sftp**, and send it to Customer Support.

The file **supportInfo.txt** is generated by executing any of the following commands:

- hsm supportInfo
- sysconf appliance reboot
- sysconf appliance poweroff

User Privileges

Users with the following privileges can perform this command:

- Admin
- Operator
- Monitor

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 tamper

Show and clear the HSM tamper state.

Syntax

hsm tamper

show
clear

Argument(s)	Shortcut	Description
show	**s**	Display the HSM tamper state. See "hsm tamper show" on page 284.
clear	**c**	Clear the HSM tamper state. See "hsm tamper clear" on the next page.

hsm tamper clear

Clear HSM tamper state. The HSM Security Officer (SO) must be logged in, or an error is returned.

User Privileges

Users with the following privileges can perform this command:

> Admin

Syntax

hsm tamper clear

Example

```
lunash:>hsm tamper clear


WARNING !!  You are about to clear the HSM Tamper State..
            If you are sure that you wish to proceed, then type 'proceed', otherwise type
'quit'.

> proceed
Proceeding...

HSM Tamper State was successfully cleared.



Command Result : 0 (Success)
```

hsm tamper show

Show HSM tamper state.

User Privileges

Users with the following privileges can perform this command:

- Admin
- Operator
- Monitor

Syntax

hsm tamper show

Example

HSM is in a tamper state

```
lunash:>hsm tamper show

        WARNING - Tamper(s) Detected:
        Chassis intrusion

Command Result : 0 (Success)
```

HSM is not in a tamper state

```
lunash:>hsm tamper show

        No active tampers.

Command Result : 0 (Success)
```

hsm time

Display the current HSM time, and synchronize the HSM time to the appliance (host) time.

Syntax

hsm time

get
sync

Argument(s)	Shortcut	Description
get	**g**	Display the current HSM time. See "hsm time get" below.

Argument(s)	Shortcut	Description
sync	**s**	Synchronize the HSM time with the appliance (host) time. See "hsm time sync" on the next page.

hsm time get

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

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

> lunash:> "hsm show" on page 234

> lunacm:> partition showinfo

> **NOTE** The "hsm time" on the previous page commands are available for HSMs with Luna Appliance Software 7.8.0 or newer and Luna HSM Firmware 7.8.0 or newer.
>
> This command returns an error (`LUNA_RET_TIME_NOT_INITIALIZED`) until lunash:> "hsm time sync" on the next page has been executed for the first time.

User Privileges

Users with the following privileges can perform this command:

> Admin

> Operator

> Monitor

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

Syntax

hsm time get

Example

```
lunash:>hsm time get

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



Command Result : 0 (Success)
```

hsm time sync

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

Automatic HSM time synchronization depends on **HSM policy 57:** Allow Sync with Host Time being set, and requires the HSM and Host clocks being no more than 3 seconds out-of-sync in the first 24 hours since the clock was last updated (for every 24 hours beyond the first 24, the HSM allows for 0.328 seconds). If the difference is greater, you can use this command to manually synchronize the two, after which daily automatic synchronization can carry on.

> **NOTE** The "hsm time" on page 284 commands are available for HSMs with Luna Appliance Software 7.8.0 or newer and Luna HSM Firmware 7.8.0 or newer.
>
> Once "hsm time sync" above has been executed, the **System Times** information also appears in the command output for:
>
> - lunash:> "hsm show" on page 234
> - lunacm:> partition showinfo

User Privileges

Users with the following privileges can perform this command:

- Admin
- Operator

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

Syntax

hsm time sync

Example

```
lunash:>hsm time sync

HSM time was synchronized to Host

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

Argument(s)	Shortcut	Description
capability	**c**	Apply a capability update. See "hsm update capability" on the next page.
show	**s**	Display a list of the available HSM updates. See "hsm update show" on page 290.

hsm update capability

Apply a capability update. You must use **sftp** to transfer the capability update from your Luna HSM 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.

User Privileges

Users with the following privileges can perform this command:

- Admin
- Operator

Syntax

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

Argument(s)	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 newcapability


CAUTION:  This command updates the HSM Capability.
          This process cannot be reversed.
          Any connected clients will have their
          connections closed.
          All clients should disconnect and the
          NTLS should be stopped before proceeding.

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

CAUTION:  This capability update is destructive.

          All keys and partitions on the HSM or token will be destroyed.
          This process cannot be reversed.
```

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


SafeNet Firmware/Capability Update Utility

Enter slot number (0 for the first slot found) : 0

Success
Capability "newcapability" updated.


Command Result : 0 (Success)
```

hsm update show

Display the HSM capability update packages that have been transferred onto the Luna Network HSM 7 appliance; shows both capability packages that have not yet been applied using the **hsm update capability** command, and packages that have been applied.

Firmware rollback 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.

User Privileges

Users with the following privileges can perform this command:

- Admin
- Operator

Syntax

hsm update show

Example

```
lunash:>hsm update show

Capability Updates:

        newcapability


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 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 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 Creating a Client-Partition STC Connection.
- 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, see "hsm factoryReset" on page 173.

User Privileges

Users with the following privileges can perform this command:

- Admin

Syntax

hsm zeroize [**-force**]

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

Example

```
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)
```

keyring

Access commands that allow you to manage keyrings on a cluster. See also the "cluster" on page 112 commands.

> **NOTE** Thales requires minimum Luna Appliance Software 7.8.5 with the lnh_cluster-1.0.4 package, Luna HSM Firmware 7.8.4, and Luna HSM Client 10.7.2 to use clusters in production environments, or minimum Luna Appliance Software 7.9.0 with the lnh_cluster-1.0.5 package, Luna HSM Firmware 7.8.4, and Luna HSM Client 10.8.0 to migrate keys from Luna application partitions.

Syntax

keyring

create
delete
disable
enable
list
reset
show
unlock

Argument(s)	Shortcut	Description
create	**c**	Create up to 100 keyrings at a time on the specified cluster. See "keyring create" on the next page.
delete	**de**	Delete a specified keyring. See "keyring delete" on page 294.
disable	**di**	Disable a specified keyring. See "keyring disable" on page 295.
enable	**e**	Enable a specified keyring. See "keyring enable" on page 296.
list	**l**	Display a list of available keyrings, their UUIDs, and whether they are locked or enabled. See "keyring list" on page 297.

Argument(s)	Shortcut	Description
reset	**r**	Reset a keyring to its initial conditions (erase all objects, reset label and password). See "keyring reset" on page 298.
show	**s**	Displays information about a keyring, specified by UUID. See "keyring show" on page 299.
unlock	**u**	Unlock a specified keyring that has been locked due to reaching the consecutive failed login limit. See "keyring unlock" on page 300.

keyring create

Create up to 100 keyrings at a time on the specified cluster. In this release, you can create up to 3000 keyrings on the cluster in total.

> **NOTE** Thales requires minimum Luna Appliance Software 7.8.5 with the lnh_cluster-1.0.4 package, Luna HSM Firmware 7.8.4, and Luna HSM Client 10.7.2 to use clusters in production environments, or minimum Luna Appliance Software 7.9.0 with the lnh_cluster-1.0.5 package, Luna HSM Firmware 7.8.4, and Luna HSM Client 10.8.0 to migrate keys from Luna application partitions.

REST API: POST /api/keyrings

User Privileges

Users with the following privileges can perform this command:

> Admin

Syntax

keyring create -label <label> **-password** <password> **-partition** <label> [**-total** <number>] [**-index** <number>] [**-copassword** <password>]

Argument(s)	Shortcut	Description
-copassword	**-c**	Specifies the Crypto Officer password for the cluster partition. If this option is omitted on a password-authenticated HSM, LunaSH prompts for the password. If this option is included on a multifactor quorum-authenticated HSM and the partition is not activated, it is ignored.

Argument(s)	Shortcut	Description
-index	**-i**	Starting index number to be appended to the label when creating multiple keyrings at a time. Valid values: **1-10000**
-label	**-l**	Set a label for the new keyring.
-partition	**-par**	Specifies the label of the cluster partition. Use lunash:> cluster member partition list to display the partitions available on the HSM. The cluster partition is displayed with a **C** flag.
-password	**-pas**	Set a password for the Partition Security Officer (PO) role on the new keyring(s).
-total	**-t**	Specifies the number of keyrings to be created. Valid values: **1-100**

Example

```
lunash:>keyring create -label keyring01 -password iamtheCO -partition clusterpar -copassword
password

KeyRing was created

Command Result : 0 (Success)
```

keyring delete

Delete a specified keyring.

> **NOTE** Thales requires minimum Luna Appliance Software 7.8.5 with the lnh_cluster-1.0.4 package, Luna HSM Firmware 7.8.4, and Luna HSM Client 10.7.2 to use clusters in production environments, or minimum Luna Appliance Software 7.9.0 with the lnh_cluster-1.0.5 package, Luna HSM Firmware 7.8.4, and Luna HSM Client 10.8.0 to migrate keys from Luna application partitions.

REST API: DELETE /api/keyrings/{keyringID}

User Privileges

Users with the following privileges can perform this command:

> Admin

Syntax

keyring delete {**-keyringid** <string> | **-label** <name>} [**-copassword** <password>] [**-force**]

Argument(s)	Shortcut	Description
-copassword	**-c**	Specifies the Crypto Officer password for the cluster partition. If this option is omitted on a password-authenticated HSM, LunaSH prompts for the password. If this option is included on a multifactor quorum-authenticated HSM and the partition is not activated, it is ignored.
-keyringid	**-k**	Specifies the UUID of the keyring to be deleted. Use lunash:> **keyring list** to display a list of available keyrings and their UUIDs.
-label	**-l**	Specifies the label of the keyring to be deleted.
-force	**-f**	Delete the keyring without asking for confirmation.

Example

```
lunash:>keyring delete -copassword iamtheCO -keyringid e921c334-3d11-4797-a10f-e98bc9ed5621

WARNING !!  This command will delete keyring e921c334-3d11-4797-a10f-e98bc9ed5621.
If you are sure that you wish to proceed, then type 'proceed', otherwise type 'quit'

> proceed
Proceeding...

Keyring e921c334-3d11-4797-a10f-e98bc9ed5621 was sucessfully deleted.

Command Result : 0 (Success)
```

keyring disable

Disable a specified keyring. A disabled keyring is still visible to clients, but no cryptographic operations are permitted.

> **NOTE** Thales requires minimum Luna Appliance Software 7.8.5 with the lnh_cluster-1.0.4 package, Luna HSM Firmware 7.8.4, and Luna HSM Client 10.7.2 to use clusters in production environments, or minimum Luna Appliance Software 7.9.0 with the lnh_cluster-1.0.5 package, Luna HSM Firmware 7.8.4, and Luna HSM Client 10.8.0 to migrate keys from Luna application partitions.

REST API: PATCH /api/keyrings/{keyringID}

User Privileges

Users with the following privileges can perform this command:

> Admin

Syntax

keyring disable {**-keyringid** <string> | **-label** <name>} [**-copassword** <password>]

Argument(s)	Shortcut	Description
-copassword	**-c**	Specifies the Crypto Officer password for the cluster partition. If this option is omitted on a password-authenticated HSM, LunaSH prompts for the password. If this option is included on a multifactor quorum-authenticated HSM and the partition is not activated, it is ignored.
-keyringid	**-k**	Specifies the UUID of the keyring to be disabled. Use lunash:> **keyring list** to display a list of available keyrings and their UUIDs.
-label	**-l**	Specifies the label of the keyring to be disabled.

Example

```
lunash:>keyring disable -copassword iamtheCO -keyringid e921c334-3d11-4797-a10f-e98bc9ed5621


Success

Command Result : 0 (Success)
```

keyring enable

Enable a specified keyring that has been disabled. A disabled keyring is still visible to clients, but no cryptographic operations are permitted.

> **NOTE** Thales requires minimum Luna Appliance Software 7.8.5 with the lnh_cluster-1.0.4 package, Luna HSM Firmware 7.8.4, and Luna HSM Client 10.7.2 to use clusters in production environments, or minimum Luna Appliance Software 7.9.0 with the lnh_cluster-1.0.5 package, Luna HSM Firmware 7.8.4, and Luna HSM Client 10.8.0 to migrate keys from Luna application partitions.

REST API: PATCH /api/keyrings/{keyringID}

User Privileges

Users with the following privileges can perform this command:

> Admin

Syntax

keyring enable {**-keyringid** <string> | **-label** <name>} [**-copassword**] <password>

Argument(s)	Shortcut	Description
-copassword	**-c**	Specifies the Crypto Officer password for the cluster partition. If this option is omitted on a password-authenticated HSM, LunaSH prompts for the password. If this option is included on a multifactor quorum-authenticated HSM and the partition is not activated, it is ignored.
-keyringid	**-k**	Specifies the UUID of the keyring to be enabled. Use lunash:> **"keyring list" below** to display a list of available keyrings and their UUIDs.
-label	**-l**	Specifies the label of the keyring to be enabled.

Example

```
lunash:>keyring enable -copassword iamtheCO -keyringid e921c334-3d11-4797-a10f-e98bc9ed5621

Success

Command Result : 0 (Success)
```

keyring list

Display a list of available keyrings, their UUIDs, and whether they are locked or enabled.

> **NOTE** Thales requires minimum Luna Appliance Software 7.8.5 with the lnh_cluster-1.0.4 package, Luna HSM Firmware 7.8.4, and Luna HSM Client 10.7.2 to use clusters in production environments, or minimum Luna Appliance Software 7.9.0 with the lnh_cluster-1.0.5 package, Luna HSM Firmware 7.8.4, and Luna HSM Client 10.8.0 to migrate keys from Luna application partitions.

REST API: GET /api/keyrings

User Privileges

Users with the following privileges can perform this command:

- Admin
- Operator
- Monitor

Syntax

keyring list

Example

```
lunash:>keyring list

Label                              Locked  Enabled  ID
-------------------------------------------------------------------------------------
keyring02                          No      Yes      7e8b55dd-fc16-4119-93fd-0654763104b7
keyring00                          No      Yes      728e8b21-81d5-49fc-ba77-2ebb22e7e25e
keyring03                          No      Yes      cf97fbfc-6afb-40cc-ae3c-6966670b7439
keyring01                          No      Yes      dffff62c-835c-4686-ace6-7fb45605fb28

Command Result : 0 (Success)
```

keyring reset

Reset a keyring to its initial conditions (erase all objects, reset label, initial password set to `PASSWORD`). You must then re-initialize the keyring and set a new KRCO password.

> **NOTE**
> - Thales requires minimum Luna Appliance Software 7.8.5 with the lnh_cluster-1.0.4 package, Luna HSM Firmware 7.8.4, and Luna HSM Client 10.7.2 to use clusters in production environments, or minimum Luna Appliance Software 7.9.0 with the lnh_cluster-1.0.5 package, Luna HSM Firmware 7.8.4, and Luna HSM Client 10.8.0 to migrate keys from Luna application partitions.
> - This operation is not supported for clusters in dual-identity mode.

REST API: PATCH /api/keyrings/{keyringID}

User Privileges

Users with the following privileges can perform this command:

- Admin

Syntax

keyring reset [**-copassword** <password>] [**-keyringid** <string>] [**-label** <name>] [**-force**]

Argument(s)	Shortcut	Description
-copassword	**-c**	Specifies the keyring CO password. If this option is omitted on a password-authenticated HSM, LunaSH prompts for the password. If this option is included on a multifactor quorum-authenticated HSM and the partition is not activated, it is ignored.
-force	**-f**	Reset the keyring without asking for confirmation.

Argument(s)	Shortcut	Description
-keyringid	**-k**	Specifies the UUID of the keyring to be reset. Use lunash:> **"keyring list" on page 297** to display a list of available keyrings and their UUIDs.
-label	**-l**	Specifies the label of the keyring to be reset.

Example

```
lunash:>keyring reset -label keyring00 -co IamtheKRCO

WARNING !! This command will reset keyring keyring00.
This will delete all objects belonging to the keyring.
If you are sure that you wish to proceed, then type 'proceed', otherwise type 'quit'

proceed
Proceeding...

Keyring 728e8b21-81d5-49fc-ba77-2ebb22e7e25e was successfully reset.

Command Result : 0 (Success)
```

keyring show

Displays information about a keyring, specified by label or UUID.

> **NOTE** Thales requires minimum Luna Appliance Software 7.8.5 with the lnh_cluster-1.0.4 package, Luna HSM Firmware 7.8.4, and Luna HSM Client 10.7.2 to use clusters in production environments, or minimum Luna Appliance Software 7.9.0 with the lnh_cluster-1.0.5 package, Luna HSM Firmware 7.8.4, and Luna HSM Client 10.8.0 to migrate keys from Luna application partitions.

REST API: GET /api/keyrings/{keyringID}

User Privileges

Users with the following privileges can perform this command:

- Admin
- Operator
- Monitor

Syntax

keyring show -keyringid <string> [**-detail**]

Argument(s)	Shortcut	Description
-detail	**-d**	Provide detailed keyring information.
-keyringid <string>	**-k**	Specifies the UUID for the keyring.
-label <label>	**-l**	Specifies the label for the keyring.

Examples

```
lunash:>keyring show -label keyring00

Name:            keyring00
Original Label:  keyring00
ID:              728e8b21-81d5-49fc-ba77-2ebb22e7e25e
Serial Number:   6616622530168
Key count:       15
Mutex acquired:  No
Enabled:         Yes              Locked:          No

Command Result : 0 (Success)


lunash:>keyring show -keyringid 728e8b21-81d5-49fc-ba77-2ebb22e7e25e -detail

Name:            keyring00
Original Label:  keyring00
ID:              728e8b21-81d5-49fc-ba77-2ebb22e7e25e
Serial Number:   6616622530168
Key count:       15
Mutex acquired:  No
Enabled:         Yes              Locked:          No
Partition Label: clusterpar
Partition UUID:  1b9214ae-dcb9-4f5f-896d-c708a7808955
Created:          Thu May  5 18:06:32 2022 Modified:    Thu May  5 18:06:32 2022
Policy:
 Ignore Lockout: No

Command Result : 0 (Success)
```

keyring unlock

Unlock a specified keyring that has been locked due to reaching the consecutive failed login limit (10 attempts). The Crypto Officer for the cluster partition (see The Cluster Partition) must provide authentication.

> **NOTE** Thales requires minimum Luna Appliance Software 7.8.5 with the lnh_cluster-1.0.4 package, Luna HSM Firmware 7.8.4, and Luna HSM Client 10.7.2 to use clusters in production environments, or minimum Luna Appliance Software 7.9.0 with the lnh_cluster-1.0.5 package, Luna HSM Firmware 7.8.4, and Luna HSM Client 10.8.0 to migrate keys from Luna application partitions.

> **NOTE** The KRCO password is what your applications will specify to access the keyring and create and use objects. Thales recommends that you always use the most secure password possible. The length of your KRSO/KRCO password affects the behavior of the keyring as follows:
>
> > If the KRCO password is 16 characters or shorter, the keyring is locked after 10 failed login attempts and must be unlocked before it can be used again:
> >
> > PATCH /api/keyrings/{keyringID}
> >
> > lunash:> **"keyring unlock" on the previous page** {**-keyringid** <string> | **-label** <name>} [**-copassword** <password>]
> >
> > If the KRCO password is 17 characters or longer, the lockout counter is not incremented.
>
> Failed login attempts using 6 characters or less never increment the counter.

REST API: PATCH /api/keyrings/{keyringID}

User Privileges

Users with the following privileges can perform this command:

> Admin

Syntax

keyring unlock {**-keyringid** <string> | **-label** <name>} [**-copassword** <password>]

Argument(s)	Shortcut	Description
-copassword	**-c**	Specifies the Crypto Officer password for the cluster partition. If this option is omitted on a password-authenticated HSM, LunaSH prompts for the password. If this option is included on a multifactor quorum-authenticated HSM and the partition is not activated, it is ignored.
-keyringid	**-k**	Specifies the UUID of the keyring to be unlocked. Use lunash:> **"keyring list" on page 297** to display a list of available keyrings and their UUIDs.
-label	**-l**	Specifies the label of the keyring to be unlocked.

Example

```
lunash:>keyring unlock -copassword iamtheCO -keyringid e921c334-3d11-4797-a10f-e98bc9ed5621

Success

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

Argument(s)	Shortcut	Description
file	**f**	Access commands that allow the currently logged in user to manage their files. See "my file" on the next page.
password	**pa**	Access commands that allow the currently logged in user to manage their password. See "my password" on page 307.
public-key	**pu**	Access commands that allow the currently logged in user to manage their public keys. See "my public-key" on page 310.

my file

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

Syntax

my file

clear
delete
list

Argument(s)	Shortcut	Description
clear	**c**	Delete all of the files owned by the currently logged in user. See "my file clear" on the next page.
delete	**d**	Delete a file owned by the currently logged in user. See "my file delete" on page 305.
list	**l**	List the files owned by the currently logged in user. See "my file list" on page 306.

my file clear

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

User Privileges

Users with the following privileges can perform this command:

- Admin
- Operator
- Monitor

Syntax

my file clear [**-force**]

Argument(s)	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.

User Privileges

Users with the following privileges can perform this command:

- Admin
- Operator
- Monitor

Syntax

my file delete <filename>

Argument(s)	Shortcut	Description
<filename>		Specifies the name of the file to delete.

Example

```
lunash:>my file delete supportInfo.txt


Command Result : 0 (Success)
```

my file list

List the files owned by the currently logged in user.

User Privileges

Users with the following privileges can perform this command:

- Admin
- Operator
- Monitor

Syntax

my file list

Example

```
lunash:>my file list

217811 Feb 27 15:28 supportInfo.txt
   681 Feb 27 12:03 DAKCertRequest.bin
   515 Feb 24 13:41 154438865323.pid
   515 Feb 24 13:41 154438865322.pid
   515 Feb 24 13:41 154438865321.pid
   515 Feb 23 10:01 154438865316.pid
   515 Feb 23 10:01 154438865315.pid
   515 Feb 23 10:01 154438865314.pid
   515 Feb 23 10:01 154438865313.pid
   4330 Feb 21 10:21 firstboot.log

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

Argument(s)	Shortcut	Description
expiry show	**e s**	Displays password expiry information for the currently logged in user. See "my password expiry show" on the next page.
set	**s**	Change the password for the currently logged in user. See "my password set" on page 309.

my password expiry show

Display password expiry information for the currently logged in user.

User Privileges

Users with the following privileges can perform this command:

- Admin
- Operator
- Monitor

Syntax

my password expiry show

Example

```
lunash:>my password expiry show


Last password change                                    : Feb 27, 2017
Password expires                                        : never


Command Result : 0 (Success)
```

my password set

Change the password for the currently logged-in user.

Using Luna Appliance Software 7.9.0 or newer, LunaSH passwords must be at least eight characters in length, and include characters from each of the following four categories. Previous versions require characters from three categories:

> lowercase alphabetic: `abcdefghijklmnopqrstuvwxyz`

> uppercase alphabetic: `ABCDEFGHIJKLMNOPQRSTUVWXYZ`

> numeric: `0123456789`

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

User Privileges

Users with the following privileges can perform this command:

> Admin

> Operator

> Monitor

Syntax

my password set

Example

```
lunash:>my password set

Changing password for user admin.

You can now choose the new password.

The password must be at least 8 characters long.
The password must contain characters from at least 3 of the following 4 categories:
    - Uppercase letters (A through Z)
    - Lowercase letters (a through z)
    - Numbers (0 through 9)
    - Non-alphanumeric characters (such as !, $, #, %)

New password:
Retype 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 Network HSM 7 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" on the next page command.

> **NOTE** The **my public-key** commands manage public keys for use by ssh sessions, but the commands to enable and disable their use on Luna Network HSM 7 are still "sysconf ssh publickey enable" on page 710 and "sysconf ssh publickey disable" on page 709.

Syntax

my public-key

add
clear
delete
list

Argument(s)	Shortcut	Description
add	**a**	Adds an SSH public key for the currently logged in user. See "my public-key add" on the next page.
clear	**c**	Deletes all SSH public keys for the currently logged in user. See "my public-key clear" on page 312.
delete	**d**	Deletes an SSH public key for the currently logged in user. See "my public-key delete" on page 313.
list	**l**	Lists the SSH public keys owned by the currently logged in user. See "my public-key list" on page 314.

my public-key add

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

> **NOTE** The **my public-key** commands manage public keys for use by ssh sessions, but the commands to enable and disable their use on Luna Network HSM 7 are still "sysconf ssh publickey enable" on page 710 and "sysconf ssh publickey disable" on page 709.

User Privileges

Users with the following privileges can perform this command:

- Admin
- Operator
- Monitor

Syntax

my public-key add <lunash_user_public_key>

Argument(s)	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 public keys for use by ssh sessions, but the commands to enable and disable their use on Luna Network HSM 7 are still "sysconf ssh publickey enable" on page 710 and "sysconf ssh publickey disable" on page 709.

User Privileges

Users with the following privileges can perform this command:

- Admin
- Operator
- Monitor

Syntax

my public-key clear [**-force**]

Argument(s)	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 public keys for use by ssh sessions, but the commands to enable and disable their use on Luna Network HSM 7 are still "sysconf ssh publickey enable" on page 710 and "sysconf ssh publickey disable" on page 709.

User Privileges

Users with the following privileges can perform this command:

- Admin
- Operator
- Monitor

Syntax

my public-key delete <lunash_user_public_key>

Argument(s)	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 public keys for use by ssh sessions, but the commands to enable and disable their use on Luna Network HSM 7 are still "sysconf ssh publickey enable" on page 710 and "sysconf ssh publickey disable" on page 709.

User Privileges

Users with the following privileges can perform this command:

- Admin
- Operator
- Monitor

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.

> **NOTE** If the network service has been stopped using the **service stop network** command, all network commands will fail.

Syntax

network

dns
hostname
interface
ping
route
show

Argument(s)	Shortcut	Description
dns	**d**	Access commands that allow you to configure the appliance DNS settings. See "network dns" on the next page.
hostname	**h**	Set the network host name. See "network hostname" on page 325.
interface	**i**	Configure the network interfaces. See "network interface" on page 327.
ping	**p**	Test the network connectivity. See "network ping" on page 358.
route	**r**	Access commands that allow you to configure the network routes for the appliance. See "network route" on page 359.
show	**s**	Display the current network configuration. See "network show" on page 369.

network dns

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

> **NOTE** If the network service has been stopped using the **service stop network** command, all network commands will fail.

Syntax

network dns

add
delete

Argument(s)	Shortcut	Description
add	**a**	Add domain name servers and search domains to the network configuration. See "network dns add" on the next page.
delete	**d**	Delete domain name servers and search domains from the network configuration. See "network dns delete" on page 322.

network dns add

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

You 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
searchdomain

Argument(s)	Shortcut	Description
nameserver	**n**	Add the specified name server to the DNS table. See "network dns add nameserver" on the next page.
searchdomain	**s**	Add the specified search domain to the DNS table. See "network dns add searchdomain" on page 320.

network dns add nameserver

Add a domain name server to the network configuration for the appliance. The name server is added to the appliance DNS table. You can add up to three different DNS nameservers to the appliance DNS table. There is one DNS table that applies to all network devices (ports) on the appliance.

When you add a DNS server, you add it to a specific network device on the appliance (eth0, eth1, eth2, eth3, bond0, bond1). When you add a DNS server to a device, it is added to the DNS table for the appliance and becomes available to all devices on the appliance, provided the device you added it to is connected to the network. For example, if you add a DNS server to eth0, all devices will be able to access the DNS server if eth0 is connected to the network. If eth0 is disconnected from the network, access to the DNS server is lost for any devices to which you did not add the DNS server. To ensure that any DNS server you add is available in the event of a network or port failure, it is recommended that you add it to all devices you will use to connect the appliance to the network.

> **NOTE** Although you can use this command to add more than three different DNS nameservers, only the first three that you add are used. Any additional nameservers that you add are ignored.

To display the current DNS settings for the appliance, use the command "network show" on page 369.

> **NOTE** Running this command changes the interface state and causes the **ctc** service to restart (see Crypto Traffic Controller for QoS).
>
> You must restart the **ntls** service (lunash:> "service restart" on page 467 **ntls**) for DNS changes to take effect.

User Privileges

Users with the following privileges can perform this command:

- Admin
- Operator

Syntax

network dns add nameserver <ip_address> **-device**<net_device>

Argument(s)	Shortcut	Description
<ip_address>		Specifies the IP address of the DNS server you want to add to the DNS table on the appliance.
-device <net_device>	**-d**	Add the specified network device to the DNS table. **Valid values:** eth0, eth1, eth2, eth3, bond0, bond1

Example

```
lunash:>network dns add nameserver 192.16.0.2 -device eth0


Command Result : 0 (Success)
```

network dns add searchdomain

Add a search domain to the network configuration for the appliance. Search domains allow you to avoid typing the complete address of frequently used Internet domains by automatically appending the search domain to an internet address you specify in LunaSH. For example, if you add the search domain **mycompany.com**, entering the command **network ping hsm1** would search for the domain **hsm1.mycompany.com**. If the domain resolves, it would ping the device with that host name.

The search domain is added to the appliance DNS table.

When you add a DNS search domain, you add it to a specific network device on the appliance (eth0, eth1, eth2, eth3, bond0, bond1). When you add a search domain to a device, it is added to the DNS table for the appliance and becomes available to all devices on the appliance, provided the device you added it to is connected to the network. For example, if you add a search domain to eth0, all devices will use the search domain if eth0 is connected to the network. If eth0 is disconnected from the network, the search domain is not used by any devices to which you did not add the search domain. To ensure that any search domain you add is available in the event of a network or port failure, it is recommended that you add it to all devices you will use to connect the appliance to the network.

> **NOTE** These settings apply to static network configurations only. If you are using DHCP, the DNS search domains configured on the DHCP server are used.

To display the current DNS settings for the appliance, including the search domains, use the command "network show" on page 369

> **NOTE** Running this command changes the interface state and causes the **ctc** service to restart (see Crypto Traffic Controller for QoS).
>
> You must restart the **ntls** service (lunash:> "service restart" on page 467 **ntls**) for DNS changes to take effect.

User Privileges

Users with the following privileges can perform this command:

- Admin
- Operator

Syntax

network dns add searchdomain <domain> **-device**<net_device>

Argument(s)	Shortcut	Description
<domain>		Add the specified search domain to the DNS table.
-device <net_device>	**-d**	Add the search domain to the specified network device. **Valid values:** eth0, eth1, eth2, eth3, bond0, bond1

Example

```
lunash:>network dns add searchdomain thales.com -device eth0


Command Result: 0 (Success)
```

network dns delete

Delete a DNS name server or search domain from the appliance network configuration.

To display the current DNS settings for the appliance, use the command "network show" on page 369.

Syntax

network dns delete

nameserver
searchdomain

Argument(s)	Shortcut	Description
nameserver	**-n**	Delete the specified name server from the DNS table. See "network dns delete nameserver" on the next page.
searchdomain	**-s**	Delete the specified search domain from the DNS table. See "network dns delete searchdomain" on page 324.

network dns delete nameserver

Delete a domain name server from the network configuration for the appliance.

When you delete a DNS server, you delete it from a specific network device on the appliance (eth0, eth1, eth2, eth3, bond0, bond1). When you delete a DNS server from a device, it is deleted from the DNS table for the appliance only if it is not configured on any other network devices on the appliance. To completely remove a DNS name server from the DNS table for the appliance, you must delete the DNS name server from each device to which it was added. If you do not delete the the DNS name server from each device to which it was added, it will continue to be listed in the DNS table for the appliance and will be available to all devices on the appliance, provided the device it is added it to is connected to the network.

To display the current DNS settings for the appliance, including the name servers, use the command "network show" on page 369

> **NOTE** Running this command changes the interface state and causes the **ctc** service to restart (see Crypto Traffic Controller for QoS).
>
> You must restart the **ntls** service (lunash:> "service restart" on page 467 **ntls**) for DNS changes to take effect.

User Privileges

Users with the following privileges can perform this command:

- Admin
- Operator

Syntax

network dns delete nameserver <ip_address> **-device**<net_device>

Argument(s)	Shortcut	Description
<ip_address>		Delete the specified name server from the DNS table.
-device<net_device>	**-d**	Delete the specified network device from the DNS table. **Valid values:** eth0, eth1, eth2, eth3, bond0, bond1

Example

```
lunash:>network dns delete nameserver 11.22.33.44 -device eth0


Command Result : 0 (Success)
```

network dns delete searchdomain

Delete a DNS search domain from the network configuration for the appliance.

When you delete a DNS search domain, you delete it from a specific network device on the appliance (eth0, eth1, eth2, eth3, bond0, bond1). When you delete a DNS search domain from a device, it is deleted from the DNS table for the appliance only if it is not configured on any other network devices on the appliance. To completely remove a DNS search domain from the DNS table for the appliance, you must delete the DNS search domain from each device to which it was added. If you do not delete the DNS search domain from each device to which it was added, it will continue to be listed in the DNS table for the appliance and will be available to all devices on the appliance, provided the device it is added it to is connected to the network.

To display the current DNS settings for the appliance, including the search domains, use the command "network show" on page 369.

> **NOTE** Running this command changes the interface state and causes the **ctc** service to restart (see Crypto Traffic Controller for QoS).
>
> You must restart the **ntls** service (lunash:> "service restart" on page 467 **ntls**) for DNS changes to take effect.

User Privileges

Users with the following privileges can perform this command:

- Admin
- Operator

Syntax

network dns delete searchdomain <ip_address> **-device**<net_device>

Argument(s)	Shortcut	Description
<ip_address>		Delete the specified search domain from the DNS table.
-device<net_device>	**-d**	Delete the specified network device from the DNS table. **Valid values:** eth0, eth1, eth2, eth3, bond0, bond1

Example

```
lunash:>network dns delete searchdomain thales.com -device eth0


Command Result : 0 (Success)
```

network hostname

Configure a host name for the appliance. You can use this command to specify a fully-qualified domain name (FQDN) for the appliance, in the format <hostname>.<domainname>, if necessary.

> **NOTE** This command replaces the **network domain** command from Luna 5/6.

The host name must adhere to the following rules:

- Have a maximum length of 64 characters
- Contain only the following characters: a-z, A-Z, 0 -9 , - , , and .(the underscore is not allowed* in Luna Network HSM 7appliance software version 7.9.0 onward; pre-existing hostnames that include underscores will have the underscore removed, but otherwise remain unchanged)
- Not begin or end in a dot (period)
- Not begin or end in a - (dash)
- Not have two dots (periods) immediately following each other

> **TIP** *If the appliance hostname changes due to appliance software update, the DNS entry in the configuration file must be updated as in ServerName in this example:
>
> ```
> LunaSA Client = {
>  ReceiveTimeout = 20000;
>  SSLConfigFile = /usr/safenet/lunaclient/bin/openssl.cnf;
>  ClientPrivKeyFile =
> /usr/safenet/lunaclient/cert/client/10.124.79.4Key.pem;
>  ClientCertFile = /usr/safenet/lunaclient/cert/client/10.124.79.4.pem;
>  ServerCAFile = /usr/safenet/lunaclient/cert/server/CAFile.pem;
>  NetClient = 1;
>  TCPKeepAlive = 1;
>  ServerName00 = random.lab.hsm;
>  ServerPort00 = 1792;
>  ServerHtl00 = 0;
> }
> ```

If the network service has been stopped using the **service stop network** command, all network commands will fail.

User Privileges

Users with the following privileges can perform this command:

- Admin
- Operator

Syntax

network hostname <hostname>

Argument(s)	Description
<hostname>	Specifies the host name for the appliance. You can specify a simple host name, or a fully-qualified domain name (FQDN), in the format <hostname>.<domainname>.

Example

```
[local_host] lunash:>network hostname mylunasa

Success: Hostname mylunasa set.


Command Result : 0 (Success)

[mylunasa] lunash:>
```

network interface

Access sub-commands that allow you to configure the appliance network interface ports.

> **NOTE** If the network service has been stopped using the **service stop network** command, all network commands will fail.

Syntax

network interface

bonding
delete
dhcp
slaac
speed
static

Argument(s)	Shortcut	Description
bonding	**b**	Configure the network interface port bonding. See "network interface bonding" on page 329.
delete	**del**	Delete the network configuration for a network interface port. See " network interface delete" on page 345.
dhcp	**dh**	Set dynamic IP configuration. See "network interface dhcp" on page 346.
slaac	**sl**	Set SLAAC IPv6 Configuration. See "network interface slaac" on page 349.
speed	**sp**	Set the speed/duplex mode on a network interface. See "network interface speed" on page 351.
static	**st**	Set static IP configuration. See "network interface static" on page 355. This is the default. If you do not specify an interface type, static is assumed.

network interface -device <netdevice> **-ip** <IP_address> **-netmask** <IP_or_prefixlength> [**-gateway** <IP_address>] [**-ipv6**] [**-force**]

Argument(s)	Shortcut	Description
-device <netdevice>	**-d**	Specifies the network device you want to configure. **Valid values**: eth0, eth1, eth2, eth3

Argument(s)	Shortcut	Description
-force	**-f**	Force the action without prompting.
-gateway <IP_address>	**-g**	Specifies the address of the network gateway. > If you are configuring an IPv4 address, you must provide an IPv4 address for the gateway. > If you are configuring an IPv6 address, you must provide an IPv6 address for the gateway.
-ip <IP_address>	**-i**	Specifies the IP address you want to assign to the device. You can specify an IPv4 or IPv6 address. If you are configuring an IPv6 address, you must also include the **-ipv6** flag in the command. When entering an IPv6 address, you can use full or shorthand syntax. For example, the following notations are equivalent: > 2001:0db3:8ba3:0000:0000:8a5e:03f0:7384 > 2001:db3:8ba3::8a5e:3f0:7384
-ipv6	**-ipv**	Specifies that the address specified using the **-ip** parameter is an IPv6 address.
-netmask <IP_or_prefixlength>	**-n**	Specifies the network mask for the interface. > If you are configuring an IPv4 address, you must specify the network mask in dotted-decimal format (for example, 255.255.255.0) > If you are configuring an IPv6 address, you must specify the prefix length (for example, 64).

network interface bonding

Access commands that allow you to bond two network interfaces into a single virtual device. Creating a bonded interface provides redundant failover in the event of a port failure. You can create bond0 between eth0 and eth1, and bond1 between eth2 and eth3. Bonded interfaces must use static addressing.

Syntax

network interface bonding

config
disable
enable
show

Argument(s)	Shortcut	Description
config	**c**	Add a network bonding interface. See "network interface bonding config" on the next page.
disable	**d**	Disable network interface bonding. See "network interface bonding disable" on page 338.
enable	**e**	Enable network interface bonding. See "network interface bonding enable" on page 340.
show	**s**	Display the current network interface bonding configuration. See "network interface bonding show" on page 342.

 Copyright 2001-2025 Thales Group

network interface bonding config

Configures network bonding interfaces. A bonded interface provides redundancy in the event of a physical port failure or network connection failure. You can create bond0 between eth0 and eth1, and bond1 between eth2 and eth3. Bonded interfaces must use static addressing.

The bonded port is not active unless port bonding is enabled. To enable port bonding, use the command "network interface bonding enable" on page 340.

Changing the configuration for a bonded interface
If the bonded interface you configure has already been configured, the existing configuration is deleted and is replaced by the new configuration, regardless of whether the existing bonded interface is enabled or not.

User Privileges

Users with the following privileges can perform this command:

- Admin
- Operator

Syntax

network interface bonding config -ip <IP_address> **-netmask** <netmask> **-name** {**bond0** | **bond1**} [**-gateway** <IP_address>] [**-mode** <bondmode>] [**-ipv6**]

Argument(s)	Shortcut	Description
-ip <ipaddress>	**-i**	Specifies the IP address of the bonded virtual network device.
-gateway <ipaddress>	**-g**	Specifies the gateway/router IP address.
-ipv6	**-ipv**	Applied to IPv6. This option requires Luna Appliance Software 7.8.4 or newer.

Argument(s)	Shortcut	Description
-mode <bondmode>	**-m**	Bond Interface Mode options: > Mode 1- Active-Backup Mode (default) > Mode 3 - Broadcast Mode > Mode 4 - LACP Mode (IEEE 802.3ad) Valid Values: **broadcast**, **lacp** **NOTE** The **-mode** option requires Luna Appliance Software 7.8.4 or newer. > Using Luna Appliance Software 7.8.3 or older, **Mode 1 - Active-Backup Mode** is the only bonding mode available, and it is selected by default; do not include the **-mode** option to select Active Backup. > Using Luna Appliance Software 7.8.4 or newer, **Mode 3 - Broadcast Mode** is also available. > Using Luna Appliance Software 7.8.5 or newer, **Mode 4 - LACP Mode (IEEE 802.3ad)** is also available. If you choose this mode, the relevant switch(es) on your network ***must*** be configured to support IEEE 802.3ad dynamic link.
-name {**bond0** | **bond1**}	**-na**	Specifies the network bond you want to configure: > **bond0** bonds eth0 and eth1 > **bond1** bonds eth2 and eth3
-netmask <string>	**-ne**	Specifies the network mask for the interface. You can specify the network mask in IP address format (for example, 255.255.255.0) or in CIDR format, without the leading slash (for example, 24).

Example

```
[local_host] lunash:>network interface bonding config -name bond0 -ip 192.168.143.184 -netmask
255.255.252.0 -mode broadcast -gateway 192.168.140.1


Command Result : 0 (Success)
[local_host] lunash:>network interface bonding config -name bond1 -ip 192.168.142.20 -netmask
255.255.252.0 -mode broadcast -gateway 192.168.140.1


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

   Hostname         : local_host
```

```
   Name Server(s)   : 192.168.105.6      192.121.120.23
   Search Domain(s) : lab.hsm

Interface settings and status

ne   HW Address (eth0)    : 00:15:B2:AD:40:7C
   IP Address (eth0)    : 192.168.143.184/22
   Mask (eth0)          : 255.255.252.0
   Gateway (eth0)       : 192.168.140.1
   DNS (eth0)           :
   DNS Search (eth0)    :
   IP Protocol (eth0)   : IPv4
   Protocol (eth0)      : DHCP
   Auto Connect (eth0)  : Yes
   Activated (eth0)     : Yes
   Link detected (eth0) : Yes
   Default Route (eth0) : Yes


   HW Address (eth1)    : 00:15:B2:AD:40:7D
   IP Address (eth1)    : 192.168.143.1/22
   Mask (eth1)          : 255.255.252.0
   Gateway (eth1)       : --
   DNS (eth1)           :
   DNS Search (eth1)    :
   IP Protocol (eth1)   : IPv4
   Protocol (eth1)      : DHCP
   Auto Connect (eth1)  : Yes
   Activated (eth1)     : Yes
   Link detected (eth1) : Yes
   Default Route (eth1) : No

   HW Address (eth2)    : 00:15:B2:AD:40:7E
   IP Address (eth2)    : 192.168.142.20/22
   Mask (eth2)          : 255.255.252.0
   Gateway (eth2)       : --
   DNS (eth2)           :
   DNS Search (eth2)    :
   IP Protocol (eth2)   : IPv4
   Protocol (eth2)      : DHCP
   Auto Connect (eth2)  : Yes
   Activated (eth2)     : Yes
   Link detected (eth2) : Yes
   Default Route (eth2) : No


ne   HW Address (eth3)    : 00:15:B2:AD:40:7F
   IP Address (eth3)    : 192.168.142.21/22
   Mask (eth3)          : 255.255.252.0
   Gateway (eth3)       : --
   DNS (eth3)           :
   DNS Search (eth3)    :
   IP Protocol (eth3)   : IPv4
   Protocol (eth3)      : DHCP
   Auto Connect (eth3)  : Yes
   Activated (eth3)     : Yes
   Link detected (eth3) : Yes
   Default Route (eth3) : No
```

```
t   HW Address (bond0)    :
   IP Address (bond0)    : 192.168.143.184
   Mask (bond0)          : 255.255.252.0
   Gateway (bond0)       : 192.168.140.1
   DNS (bond0)           :
   DNS Search (bond0)    :
   IP Protocol (bond0)   : IPv4
   Protocol (bond0)      : Static
   Auto Connect (bond0)  : No
   Activated (bond0)     : No
   Link detected (bond0) : No
   Default Route (bond0) : Yes
   Active Slaves (bond0) :

   HW Address (bond1)    :
   IP Address (bond1)    : 192.168.142.20
   Mask (bond1)          : 255.255.252.0
   Gateway (bond1)       : 192.168.140.1
   DNS (bond1)           :
   DNS Search (bond1)    :
   IP Protocol (bond1)   : IPv4
   Protocol (bond1)      : Static
   Auto Connect (bond1)  : No
   Activated (bond1)     : No
   Link detected (bond1) : No
   Default Route (bond1) : Yes
   Active Slaves (bond1) :


Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
0.0.0.0         192.168.140.1    0.0.0.0         UG    108    0        0 eth0
192.168.140.0    0.0.0.0         255.255.252.0   U     105    0        0 eth1
192.168.140.0    0.0.0.0         255.255.252.0   U     106    0        0 eth2
192.168.140.0    0.0.0.0         255.255.252.0   U     107    0        0 eth3
192.168.140.0    0.0.0.0         255.255.252.0   U     108    0        0 eth0


Command Result : 0 (Success)
[local_host] lunash:>network interface bonding show


bond0:
bond0 is configured, but not enabled.

Bonding Interface: bond0
IPADDR=192.168.143.184
PREFIX=22
GATEWAY=192.168.140.1
Slave devices: eth0 eth1
------------------------------------------------------------

bond1:
bond1 is configured, but not enabled.

Bonding Interface: bond1
```

```
IPADDR=192.168.142.20
PREFIX=22
GATEWAY=192.168.140.1
Slave devices: eth2 eth3
------------------------------------------------------------

Command Result : 0 (Success)

[local_host] lunash:>network interface bonding enable -name bond0 -f


Activating bond-slave-eth0...
Activating bond-slave-eth1...

Command Result : 0 (Success)
[local_host] lunash:>network interface bonding enable -name bond1 -f


Activating bond-slave-eth2...
Activating bond-slave-eth3...

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

[local_host] lunash:>net sh

   Hostname         : local_host
   Name Server(s)   : <not set>
   Search Domain(s) : <not set>

Interface settings and status

   HW Address (eth0)    : 00:15:B2:AD:40:7C
   Bond master (eth0)   : bond0
   Link detected (eth0) : Yes

   HW Address (eth1)    : 00:15:B2:AD:40:7C
   Bond master (eth1)   : bond0
   Link detected (eth1) : Yes

   HW Address (eth2)    : 00:15:B2:AD:40:7E
   Bond master (eth2)   : bond1
   Link detected (eth2) : Yes

   HW Address (eth3)    : 00:15:B2:AD:40:7E
   Bond master (eth3)   : bond1
   Link detected (eth3) : Yes

   HW Address (bond0)    : 00:15:B2:AD:40:7C
   IP Address (bond0)    : 192.168.143.184/22
   Mask (bond0)          : 255.255.252.0
   Gateway (bond0)       : 192.168.140.1
   DNS (bond0)           :
   DNS Search (bond0)    :
   IP Protocol (bond0)   : IPv4
   Protocol (bond0)      : Static
   Auto Connect (bond0)  : Yes
   Activated (bond0)     : Yes
```

```
   Link detected (bond0) : Yes
   Default Route (bond0) : Yes
   Active Slaves (bond0) : eth0 eth1

   HW Address (bond1)    : 00:15:B2:AD:40:7E
   IP Address (bond1)    : 192.168.142.20/22
   Mask (bond1)          : 255.255.252.0
   Gateway (bond1)       : --
   DNS (bond1)           :
   DNS Search (bond1)    :
   IP Protocol (bond1)   : IPv4
   Protocol (bond1)      : Static
   Auto Connect (bond1)  : Yes
   Activated (bond1)     : Yes
   Link detected (bond1) : Yes
   Default Route (bond1) : No
   Active Slaves (bond1) : eth2 eth3


Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
0.0.0.0         192.168.140.1    0.0.0.0         UG    300    0        0 bond0
192.168.140.0    0.0.0.0         255.255.252.0   U     300    0        0 bond0
192.168.140.0    0.0.0.0         255.255.252.0   U     301    0        0 bond1


Command Result : 0 (Success)
[local_host] lunash:>network interface bonding show

bond0:

Bonding Mode: fault-tolerance (broadcast)
MII Status: up
MII Polling Interval (ms): 500
Up Delay (ms): 0
Down Delay (ms): 0

Slave Interface: eth0
MII Status: up
Speed: 1000 Mbps
Duplex: full
Link Failure Count: 0
Permanent HW addr: 00:15:b2:ad:40:7c
Slave queue ID: 0

Slave Interface: eth1
MII Status: up
Speed: 1000 Mbps
Duplex: full
Link Failure Count: 0
Permanent HW addr: 00:15:b2:ad:40:7d
Slave queue ID: 0

Slave status eth0:      Link detected: yes
Slave status eth1:      Link detected: yes
------------------------------------------------------------
bond1:
```

```
Bonding Mode: fault-tolerance (broadcast)
MII Status: up
MII Polling Interval (ms): 500
Up Delay (ms): 0
Down Delay (ms): 0

Slave Interface: eth2
MII Status: up
Speed: 1000 Mbps
Duplex: full
Link Failure Count: 0
Permanent HW addr: 00:15:b2:ad:40:7e
Slave queue ID: 0

Slave Interface: eth3
MII Status: up
Speed: 1000 Mbps
Duplex: full
Link Failure Count: 0
Permanent HW addr: 00:15:b2:ad:40:7f
Slave queue ID: 0

Slave status eth2:      Link detected: yes
Slave status eth3:      Link detected: yes
------------------------------------------------------------

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

Use ping to verify broadcast mode

```
[root@client21 ~]# ping 192.168.143.184
PING 192.168.143.184 (192.168.143.184) 56(84) bytes of data.
64 bytes from 192.168.143.184: icmp_seq=1 ttl=62 time=0.956 ms
64 bytes from 192.168.143.184: icmp_seq=1 ttl=62 time=0.966 ms (DUP!)
64 bytes from 192.168.143.184: icmp_seq=2 ttl=62 time=0.666 ms
64 bytes from 192.168.143.184: icmp_seq=2 ttl=62 time=0.676 ms (DUP!)
64 bytes from 192.168.143.184: icmp_seq=3 ttl=62 time=0.638 ms
64 bytes from 192.168.143.184: icmp_seq=3 ttl=62 time=0.646 ms (DUP!)
64 bytes from 192.168.143.184: icmp_seq=4 ttl=62 time=0.611 ms
64 bytes from 192.168.143.184: icmp_seq=4 ttl=62 time=0.620 ms (DUP!)
64 bytes from 192.168.143.184: icmp_seq=5 ttl=62 time=0.651 ms
64 bytes from 192.168.143.184: icmp_seq=5 ttl=62 time=0.659 ms (DUP!)
64 bytes from 192.168.143.184: icmp_seq=6 ttl=62 time=0.575 ms
64 bytes from 192.168.143.184: icmp_seq=6 ttl=62 time=0.584 ms (DUP!)
^C
--- 192.168.143.184 ping statistics ---
6 packets transmitted, 6 received, +6 duplicates, 0% packet loss, time 5001ms
rtt min/avg/max/mdev = 0.575/0.687/0.966/0.127 ms
[root@aa4221 ~]# ping 192.168.142.20
PING 192.168.142.20 (192.168.142.20) 56(84) bytes of data.
64 bytes from 192.168.142.20: icmp_seq=1 ttl=62 time=0.983 ms
64 bytes from 192.168.142.20: icmp_seq=1 ttl=62 time=0.992 ms (DUP!)
64 bytes from 192.168.142.20: icmp_seq=2 ttl=62 time=0.576 ms
64 bytes from 192.168.142.20: icmp_seq=2 ttl=62 time=0.584 ms (DUP!)
64 bytes from 192.168.142.20: icmp_seq=3 ttl=62 time=0.636 ms
64 bytes from 192.168.142.20: icmp_seq=3 ttl=62 time=0.644 ms (DUP!)
64 bytes from 192.168.142.20: icmp_seq=4 ttl=62 time=0.454 ms
64 bytes from 192.168.142.20: icmp_seq=4 ttl=62 time=0.462 ms (DUP!)
64 bytes from 192.168.142.20: icmp_seq=5 ttl=62 time=0.458 ms
```

```
64 bytes from 192.168.142.20: icmp_seq=5 ttl=62 time=0.466 ms (DUP!)
64 bytes from 192.168.142.20: icmp_seq=6 ttl=62 time=0.526 ms
64 bytes from 192.168.142.20: icmp_seq=6 ttl=62 time=0.533 ms (DUP!)
^C
--- 192.168.142.20 ping statistics ---
6 packets transmitted, 6 received, +6 duplicates, 0% packet loss, time 5000ms
rtt min/avg/max/mdev = 0.454/0.609/0.992/0.182 ms
```

network interface bonding disable

Disable network interface bond0 or bond1.

> **CAUTION!** Using Luna Network HSM 7 Appliance Software 7.8.3 or older, once the default route is added to the bonded interface, disabling the bond for any reason will cause a loss of SSH connectivity to the Luna Network HSM 7. It is highly recommended that you configure manual routes on at least one of the secondary interfaces within the bonded interface (**eth0** or **eth1** for **bond0**, **eth2** or **eth3** for **bond1**). Refer to Disabling a Bonded Interface.

User Privileges

Users with the following privileges can perform this command:

- Admin
- Operator

Syntax

network interface bonding disable -name <netbond> [**-keeproutes**] [**-force**]

Argument(s)	Shortcut	Description
-force	**-f**	Force the action without being prompted.
-keeproutes	**-k**	Using Luna Appliance Software 7.8.4 and older, when a bonded interface is disabled, all associated routes are also deleted automatically as part of interface cleanup. Specify this option to preserve static routes. Using Luna Appliance Software 7.8.5 and newer, when a bonded interface is disabled, all associated *static* routes are also deleted automatically as part of interface cleanup. Specify this option to preserve them. **NOTE** If you had a manual route configured on the bonded interface, and you specify **-keeproutes**, you can use lunash:> "network route show" on page 367 to confirm that the route was preserved. The route information for the inactive bond does not appear in the output for lunash:> "network show" on page 369.
-name <netbond>	**-n**	Specifies the bonded interface you want to disable. **Valid values:** bond0, bond1

Example

```
lunash:>network interface bonding disable -name bond0

WARNING! All network connections through bond0 will be interrupted.
```

```
WARNING! A default route is present on this interface. Disabling this network interface
         will also remove associated default route.
If you are sure that you wish to proceed, then type 'proceed', otherwise type 'quit'

> proceed

Activating eth0...
Activating eth1...

Command Result : 0 (Success)
```

network interface bonding enable

Enable network interface bond0 or bond1.

User Privileges

Users with the following privileges can perform this command:

> Admin

> Operator

Syntax

network interface bonding enable -name <netbond>

Argument(s)	Shortcut	Description
-name <netbond>	**-n**	Specifies the bonded interface you want to enable. **Valid values:** bond0, bond1
-force	**-f**	Force action with no prompt.

Example

```
lunash:>network interface bonding enable -name bond0

WARNING! All network connections through eth0 and eth1 will be interrupted.
If you are sure that you wish to proceed, then type 'proceed', otherwise type 'quit'

> proceed
Proceeding...

Activating bond-slave-eth0...
Activating bond-slave-eth1...

Command Result : 0 (Success)



lunash:>network show

   Hostname         : sa7pw
   Name Server(s)   :
   Search Domain(s) : <not set>

Interface settings and status

   HW Address (eth0)    : 00:15:B2:A9:B7:85
   Bond master (eth0)   : bond0
   Link detected (eth0) : Yes

   HW Address (eth1)    : 00:15:B2:A9:B7:85
```

```
   Bond master (eth1)   : bond0
   Link detected (eth1) : Yes

   HW Address (bond0)    : 00:15:B2:A9:B7:85
   IP Address (bond0)    : 192.20.11.64/24
   Mask (bond0)          : 255.255.255.0
   Gateway (bond0)       : 192.20.11.10
   DNS (bond0)           :
   DNS Search (bond0)    :
   IP Protocol (bond0)   : IPv4
   Protocol (bond0)      : Static
   Auto Connect (bond0)  : Yes
   Activated (bond0)     : Yes
   Link detected (bond0) : Yes
   Active Slaves (bond0) : eth1 eth0

Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
0.0.0.0         192.20.11.10    0.0.0.0         UG    301    0        0 bond0
192.20.11.0     0.0.0.0         255.255.255.0   U     300    0        0 bond0
192.20.11.0     0.0.0.0         255.255.255.0   U     301    0        0 bond0

Command Result : 0 (Success)
```

network interface bonding show

Display the current network bonding interface status.

User Privileges

Users with the following privileges can perform this command:

- Admin
- Operator
- Monitor

Syntax

network interface bonding show

Example using Luna Appliance Software 7.9.0 or newer

```
lunash:>network interface bonding show

bond0:

Bonding Mode: fault-tolerance (broadcast)
MII Status: up
MII Polling Interval (ms): 500
Up Delay (ms): 0
Down Delay (ms): 0

Slave Interface: eth0
MII Status: up
Speed: 1000 Mbps
Duplex: full
Link Failure Count: 0
Permanent HW addr: 00:15:b2:ad:40:7c
Slave queue ID: 0

Slave Interface: eth1
MII Status: up
Speed: 1000 Mbps
Duplex: full
Link Failure Count: 0
Permanent HW addr: 00:15:b2:ad:40:7d
Slave queue ID: 0

Slave status eth0:      Link detected: yes
Slave status eth1:      Link detected: yes
------------------------------------------------------------
bond1:

Bonding Mode: fault-tolerance (broadcast)
MII Status: up
MII Polling Interval (ms): 500
Up Delay (ms): 0
Down Delay (ms): 0
```

```
Slave Interface: eth2
MII Status: up
Speed: 1000 Mbps
Duplex: full
Link Failure Count: 0
Permanent HW addr: 00:15:b2:ad:40:7e
Slave queue ID: 0

Slave Interface: eth3
MII Status: up
Speed: 1000 Mbps
Duplex: full
Link Failure Count: 0
Permanent HW addr: 00:15:b2:ad:40:7f
Slave queue ID: 0

Slave status eth2:      Link detected: yes
Slave status eth3:      Link detected: yes
------------------------------------------------------------

Command Result : 0 (Success)
```

Example using Luna Appliance Software 7.8.5 or older

```
lunash:>network interface bonding show

bond0:

Bonding Mode: fault-tolerance (active-backup)
Primary Slave: None
Currently Active Slave: eth1
MII Status: up
MII Polling Interval (ms): 0
Up Delay (ms): 0
Down Delay (ms): 0
ARP Polling Interval (ms): 500
ARP IP target/s (n.n.n.n form): 192.20.11.10

Slave Interface: eth1
MII Status: up
Speed: 1000 Mbps
Duplex: full
Link Failure Count: 1
Permanent HW addr: 00:15:b2:a9:b7:85
Slave queue ID: 0

Slave Interface: eth0
MII Status: up
Speed: 1000 Mbps
Duplex: full
Link Failure Count: 0
Permanent HW addr: 00:15:b2:a9:b7:84
Slave queue ID: 0

Slave status eth0:      Link detected: yes
Slave status eth1:      Link detected: yes
------------------------------------------------------------
bond1:
```

```
bond1 is configured, but not enabled.

Bonding Interface: bond1
Slave devices: eth2 eth3
------------------------------------------------------------

Command Result : 0 (Success)
```

network interface delete

This command disables a network interface and deletes its current configuration.

> **NOTE**
> - You cannot delete an interface that is a member of an active bond; this command will not proceed. See "network interface bonding" on page 329.
> - Running this command changes the interface state and causes the **ctc** service to restart (see Crypto Traffic Controller for QoS).

User Privileges

Users with the following privileges can perform this command:

- Admin
- Operator

Syntax

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

Argument(s)	Shortcut	Description
-device <netdevice>	**-d**	Specifies the network device to delete. **Valid values:** eth0, eth1, eth2, eth3
-force	**-f**	Specify **-force** if the interface you are deleting has the default route, and you wish to proceed without being prompted for confirmation. When the interface being deleted does not have the default route, no confirmation is prompted; there is no need to include the **-force** option.

Example

```
lunash:>network interface delete -f -device eth1

Command Result : 0 (Success)
lunash:>network interface delete -f -device eth2

Command Result : 0 (Success)
```

network interface dhcp

Configure a network interface to use DHCP. Using DHCP will automatically update the Luna appliance's system name servers and other network settings that are transmitted via DHCP.

> **CAUTION!** 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.

> **NOTE** When DHCP is used, the appliance's IP address may change automatically, which may lead to certificate mismatches and client connection issues.
>
> You cannot configure an interface that is a member of an active bond. You must first disable the bond. See "network interface bonding" on page 329

> **NOTE** Running this command changes the interface state and causes the **ctc** service to restart (see Crypto Traffic Controller for QoS).

User Privileges

Users with the following privileges can perform this command:

- Admin
- Operator

Syntax

network interface dhcp -device <netdevice> [**-force**] [**-ipv6**]

Argument(s)	Shortcut	Description
-device <netdevice>	**-d**	Specifies the network device you want to configure. **Valid values:** eth0, eth1, eth2, eth3
-force	**-f**	Force the action without being prompted.
-ipv6	**-i**	Specifies that you want to obtain an IPv6 address via DHCPv6.

Example

DHCP with IPv4

```
lunash:>network interface dhcp -device eth1

NOTICE: The network connection for device eth3 will be restarted for new network settings to
take effect.
If you are sure that you wish to restart the device connection, then type 'proceed', otherwise
type 'quit'
> proceed
```

```
Proceeding...

Command Result : 0 (Success)



lunash:>network show

   Hostname         : sa7pw
   Name Server(s)   : 192.20.10.20      192.16.2.14
   Search Domain(s) : <not set>

Interface settings and status

   HW Address (eth1)    : 00:15:B2:A9:B7:85
   IP Address (eth1)    : 192.20.11.84/24
   Mask (eth1)          : 255.255.255.0
   Gateway (eth1)       : 192.20.11.10
   DNS (eth1)           :
   DNS Search (eth1)    :
   IP Protocol (eth1)   : IPv4
   Protocol (eth1)      : DHCP
   Auto Connect (eth1)  : Yes
   Activated (eth1)     : Yes
   Link detected (eth1) : Yes


Command Result : 0 (Success)
```

DHCP with IPv6

```
lunash:>network interface dhcp -device eth1 -ipv6

NOTICE: The network connection for device eth1 will be restarted for new network settings to
take effect.
If you are sure that you wish to restart the device connection, then type 'proceed', otherwise
type 'quit'
> proceed
Proceeding...

Command Result : 0 (Success)



lunash:>network show

   Hostname         : sa7pw
   Name Server(s)   : 192.20.10.20      192.16.2.14
   Search Domain(s) : <not set>

Interface settings and status

   HW Address (eth1)    : 00:15:B2:A9:B7:85
   IP Address (eth1)    : 2001:db3:8ba3::8a5e:3f0:7384/64
   Mask (eth1)          : 2001:db3:8ba3:::/64
   Gateway (eth1)       : 2001:db3:a348::6b3a:24:7336
   DNS (eth1)           :
   DNS Search (eth1)    :
```

```
   IP Protocol (eth1)   : IPv6
   Protocol (eth1)      : DHCP
   Auto Connect (eth1)  : Yes
   Activated (eth1)     : Yes
   Link detected (eth1) : Yes


Kernel IPv6 routing table
Destination                    Next Hop                   Flag Met Ref Use If
fe80::/64                      ::                         U    256 0     0 eth1
::/0                           ::                         !n   -1  1     1 lo
fe80::215:b2ff:fea9:b785/128   ::                         Un   0   1     0 lo
ff00::/8                       ::                         U    256 1     0 eth1
::/0                           ::                         !n   -1  1     1 lo


Command Result : 0 (Success)
```

network interface slaac

Configure a network interface to obtain an IPv6 address using the Stateless Address Autoconfiguration (SLAAC) protocol.

Most IPv6-enabled routers have the ability to periodically broadcast router advertisements (RA) messages to all devices on the network. These RA messages include a list of one of more IPv6 prefixes that any device on the local network can use to automatically form a unique IPv6 address. IPv6 client devices, such as the Luna Network HSM 7, listen for these local RA's. When you issue this command, the Luna Network HSM 7 claims one of the advertised prefixes and uses it to automatically configure an IPv6 address that uniquely identifies the device on the network.

You must issue this command on each network interface that will be connected using a SLAAC IPv6 configuration.

> **NOTE** The network interface you want to configure must be connected to the network and have access to the local router used to provide the IPv6 prefixes.
>
> You cannot configure an interface that is a member of an active bond. You must first disable the bond. See "network interface bonding" on page 329.

> **NOTE** Running this command changes the interface state and causes the **ctc** service to restart (see Crypto Traffic Controller for QoS).

User Privileges

Users with the following privileges can perform this command:

- Admin
- Operator

Syntax

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

Argument(s)	Shortcut	Description
-device <netdevice>	**-d**	Specifies the network device you want to configure. **Valid values**: eth0, eth1, eth2, eth3
-force	**-f**	Force the action without prompting.

Example

```
lunash:>network interface slaac -device eth1

NOTICE: The network connection for device eth1 will be restarted for new network settings to
take effect.
If you are sure that you wish to restart the device connection, then type 'proceed', otherwise
type 'quit'
```

```
> proceed
Proceeding...

Command Result : 0 (Success)



lunash:>network show

   Hostname         : sa7pw
   Name Server(s)   :
   Search Domain(s) : <not set>

Interface settings and status

   HW Address (eth1)    : 00:15:B2:A9:B7:85
   IP Address (eth1)    : 2001:db3:8ba3::8a5e:3f0:7384/64
   Mask (eth1)          : 2001:db3:8ba3:::/64
   Gateway (eth1)       : 2001:db3:a348::6b3a:24:7336
   DNS (eth1)           :
   DNS Search (eth1)    :
   IP Protocol (eth1)   : IPv6
   Protocol (eth1)      : SLAAC
   Auto Connect (eth1)  : Yes
   Activated (eth1)     : Yes
   Link detected (eth1) : Yes
```

network interface speed

Access commands that allow you to set the speed/duplex mode on a network interface.

> **NOTE** This command is available using Luna Appliance Software 7.8.1 or newer.

Syntax

network interface speed

set-auto
set
show

Argument(s)	Shortcut	Description
set-auto	**set-**	Set the specified network device to determine speed and duplex via auto-negotiation. See "network interface speed set-auto" on the next page.
set	**set**	Set speed and duplex manually for the specified network device. See "network interface speed set" on page 353.
show	**sh**	Display the current speed settings for the specified network device. See "network interface speed show" on page 354.

network interface speed set-auto

Set the specified network device to determine speed and duplex via auto-negotiation. This is the default setting for network devices.

> **NOTE** This command is available using Luna Appliance Software 7.8.1 or newer.

User Privileges

Users with the following privileges can perform this command:

- Admin
- Operator

Syntax

network interface speed set-auto <netdevice>

Argument(s)	Shortcut	Description
<netdevice>		Specifies the device to set to auto-negotiation mode. **Valid values:** eth0, eth1, eth2, eth3, all

Example

```
lunash:>network interface speed set-auto all


Command Result : 0 (Success)
```

network interface speed set

Set speed and duplex manually for the specified network device.

> **CAUTION!** Ensure that your custom speed and duplex settings are supported by your network. If you set the speed to a level that is higher than your network will allow, you can lose SSH connectivity to that network device. If this happens, connect to LunaSH using a serial connection or another configured ethernet device, and set the lost device back to auto-negotiation mode using lunash:> "network interface speed set-auto" on the previous page.

> **NOTE** This command is available using Luna Appliance Software 7.8.1 or newer.

User Privileges

Users with the following privileges can perform this command:

- Admin
- Operator

Syntax

network interface speed set <netdevice> <speed> [<duplex>]

Argument(s)	Shortcut	Description
<netdevice>		Specifies the device to set to auto-negotiation mode. **Valid values:** eth0, eth1, eth2, eth3, all
<speed>		Specifies the speed to set for the network device. **Valid values:** 10, 100, 1000, 10000 **NOTE** Use the `10000` setting on a Luna Network HSM 7 with the optional 10Gb Optical Ethernet option only. The standard 1Gb copper interfaces should be set to a maximum of `1000` Mb/s.
<duplex>		Specifies the duplex for the network device. **Valid values:** half, full

Example

```
lunash:>network interface speed set eth0 100


Command Result : 0 (Success)
```

network interface speed show

Display the current speed settings for the specified network device.

> **NOTE** This command is available using Luna Appliance Software 7.8.1 or newer.

User Privileges

Users with the following privileges can perform this command:

- Admin
- Operator
- Monitor

Syntax

network interface speed show <netdevice>

Argument(s)	Shortcut	Description
<netdevice>		Specifies the device to display the speed settings for. **Valid values:** eth0, eth1, eth2, eth3, all

Example

```
lunash:>network interface speed show

eth0:
        Speed: 1000Mb/s
        Duplex: Full
        Auto-negotiation: on
eth1:
        Speed: 1000Mb/s
        Duplex: Full
        Auto-negotiation: on
eth2:
        Speed: 1000Mb/s
        Duplex: Full
        Auto-negotiation: on
eth3:
        Speed: 1000Mb/s
        Duplex: Full
        Auto-negotiation: on

Command Result : 0 (Success)
```

network interface static

Configure a network interface to use a static IP configuration. You can use this command to configure a static IPv4 address or a static IPv6 address.

You must issue this command on each network interface that will be connected using a static IP configuration.

> **NOTE** You cannot configure an interface that is a member of an active bond. You must first disable the bond. See "network interface bonding" on page 329

> **NOTE** Running this command changes the interface state and causes the **ctc** service to restart (see Crypto Traffic Controller for QoS).

User Privileges

Users with the following privileges can perform this command:

- Admin
- Operator

Syntax

network interface static -device <netdevice> **-ip** <IP_address> **-netmask** <IP_or_prefixlength> [**-gateway** <IP_address>] [**-force**] [**-ipv6**]

Argument(s)	Shortcut	Description
-device <netdevice>	**-d**	Specifies the network device you want to configure. **Valid values**: eth0, eth1, eth2, eth3
-force	**-f**	Force the action without prompting.
-gateway <IP_address>	**-g**	Specifies the address of the network gateway. > If you are configuring an IPv4 address, you must provide an IPv4 address for the gateway. > If you are configuring an IPv6 address, you must provide an IPv6 address for the gateway.
-ip <IP_address>	**-i**	Specifies the IP address you want to assign to the device. You can specify an IPv4 or IPv6 address. If you are configuring an IPv6 address, you must also include the **-ipv6** flag in the command. When entering an IPv6 address, you can use full or shorthand syntax. For example, the following notations are equivalent: > 2001:0db3:8ba3:0000:0000:8a5e:03f0:7384 > 2001:db3:8ba3::8a5e:3f0:7384

Argument(s)	Shortcut	Description
-ipv6	**-ipv**	Specifies that the address specified using the **-ip** parameter is an IPv6 address.
-netmask <IP_address>	**-n**	Specifies the network mask for the interface. > If you are configuring an IPv4 address, you must specify the network mask in dotted-decimal format (for example, 255.255.255.0) > If you are configuring an IPv6 address, you must specify the prefix length (for example, 64).

Example

IPv4 configuration

```
lunash:>network interface static -device eth0 -ip 192.20.11.78 -gateway 192.20.11.10 -netmask
255.255.255.0


NOTICE: The network connection for device eth0 will be restarted for new network settings to
take effect.
If you are sure that you wish to restart the device connection, then type 'proceed', otherwise
type 'quit'

> proceed
Proceeding...

Command Result : 0 (Success)



lunash:>network show

   Hostname         : sa7pw
   Name Server(s)   :
   Search Domain(s) : <not set>

Interface settings and status

   HW Address (eth0)    : 00:15:B2:A9:B7:84
   IP Address (eth0)    : 192.20.11.78/24
   Mask (eth0)          : 255.255.255.0
   Gateway (eth0)       : 192.20.11.10
   DNS (eth0)           :
   DNS Search (eth0)    :
   IP Protocol (eth0)   : IPv4
   Protocol (eth0)      : Static
   Auto Connect (eth0)  : Yes
   Activated (eth0)     : Yes
   Link detected (eth0) : Yes


Command Result : 0 (Success)
```

IPv6 configuration

```
lunash:>network interface static -device eth1 -ip 2001:0db3:8ba3:0000:0000:8a5e:03f0:7384 -
netmask 64 -gateway 2001:0db3:a348:0000:0000:6b3a:0024:7336 -ipv6


NOTICE: The network connection for device eth1 will be restarted for new network settings to
take effect.
If you are sure that you wish to restart the device connection, then type 'proceed', otherwise
type 'quit'

> proceed
Proceeding...

Command Result : 0 (Success)



lunash:>network show

   Hostname         : sa7pw
   Name Server(s)   :
   Search Domain(s) : <not set>

Interface settings and status

   HW Address (eth1)    : 00:15:B2:A9:B7:85
   IP Address (eth1)    : 2001:db3:8ba3::8a5e:3f0:7384/64
   Mask (eth1)          : 2001:db3:8ba3::/64
   Gateway (eth1)       : 2001:db3:a348::6b3a:24:7336
   DNS (eth1)           :
   DNS Search (eth1)    :
   IP Protocol (eth1)   : IPv6
   Protocol (eth1)      : Static
   Auto Connect (eth1)  : Yes
   Activated (eth1)     : Yes
   Link detected (eth1) : Yes
```

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.

> **NOTE** If the network service has been stopped using the **service stop network** command, all network commands will fail.

User Privileges

Users with the following privileges can perform this command:

- Admin
- Operator
- Monitor

Syntax

network ping <hostname_or_IPaddress> [**-ipv6**]

Argument(s)	Shortcut	Description
<hostname_or_IPaddress>		Specifies the host name or IP address of the host you want to ping.
-ipv6	**-i**	Specifies that the host you want to ping uses IPv6 addressing.

Example

```
lunash:>network ping 192.20.11.40

PING 192.20.11.40 (192.20.11.40) 56(84) bytes of data.
64 bytes from 192.20.11.40: icmp_seq=1 ttl=64 time=0.525 ms

--- 192.20.11.40 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 0.525/0.525/0.525/0.000 ms

Command Result : 0 (Success)
```

network route

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

> **NOTE** If the network service has been stopped using the **service stop network** command, all network commands will fail.

Syntax

network route

add
clear
delete
metric
show

Argument(s)	Shortcut	Description
add	**a**	Add a network route. See "network route add" on the next page.
clear	**c**	Delete all network routes. See "network route clear" on page 363.
delete	**d**	Delete the specified network route. See "network route delete" on page 364.
metric	**m**	Modify a network interface routing metric. See "network route metric" on page 366.
show	**s**	Display the current network route configuration. See "network route show" on page 367.

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.

> **NOTE** Running this command changes the interface state and causes the **ctc** service to restart (see Crypto Traffic Controller for QoS).

User Privileges

Users with the following privileges can perform this command:

- Admin
- Operator

Syntax

network route add <routetype> <IP_address> **-device** <netdevice> [**-metric** <metric>] [**-netmask** <string>] [**-gateway** <IP_address>] [**-force**] [**-ipv6**]

Argument(s)	Shortcut	Description
<routetype>		Specifies the type of route (network or host) you want to add. **Valid values:** host, network
<IP_address>		Specifies the IP address of the network or host you want to add to the routing table. You can specify an IPv4 or IPv6 address. If you are configuring an IPv6 address, you must also include the **-ipv6** flag in the command. When entering an IPv6 address, you can use full or shorthand syntax. For example, the following notations are equivalent: > 2001:0db3:8ba3:0000:0000:8a5e:03f0:7384 > 2001:db3:8ba3::8a5e:3f0:7384
-device <netdevice>	**-d**	Specifies the network device to which you want to add the route. **Valid values:** eth0, eth1, eth2, eth3, bond0, bond1
-force	**-f**	Force the action without prompting
-gateway <IP_address>	**-g**	Specifies the gateway/router IP address if this is not a locally connected network or host. If no default route is already configured on the device, this will be used to set the default route. You can specify 0.0.0.0 as a value.
-ipv6	**-i**	Specifies that the route you are adding uses IPv6 addressing.

Argument(s)	Shortcut	Description
-metric <metric>	**-m**	Specifies the routing metric to use for the route. **Range:** 0 to 65535 **Default:** 0
-netmask <string>	**-n**	Specifies the network mask. Include this option only if you are adding a network route. If not specified, the default netmask is used. > If you are configuring an IPv4 route, you must specify the network mask in dotted-decimal format (for example, 255.255.255.0) > If you are configuring an IPv6 route, you must specify the prefix length (for example, 64) **Default:** > <routetype> = network IPv4: 255.255.255.0 IPv6: 64 > <routetype> = host IPv4: 255.255.255.255 IPv6: 128

Example

Adding an IPv4 route

```
lunash:>network route add host 123.45.67.89 -device eth2 -metric 1000

NOTICE: The network connection for device eth2 will be restarted for new network settings to
take effect.
If you are sure that you wish to restart the device connection, then type 'proceed', otherwise
type 'quit'
> proceed

Proceeding...

Command Result : Success
```

Adding an IPv6 route

```
lunash:>network route add network 2018:1:2:3::0 -device eth2 -netmask 64 -gateway
fe80::20c:29ff:fe9e:5f79 -ipv6


NOTICE: The network connection for device eth2 will be restarted for new network settings to
take effect.
If you are sure that you wish to restart the device connection, then type 'proceed', otherwise
type 'quit'
```

```
> proceed
Proceeding...
Routing table successfully updated.

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 prompted to confirm the action unless you use the **-force** option.

> **NOTE** Running this command changes the interface state and causes the **ctc** service to restart (see Crypto Traffic Controller for QoS).

User Privileges

Users with the following privileges can perform this command:

- Admin
- Operator

Syntax

network route clear [**-force**]

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

Example

```
lunash:>network route clear
WARNING !!  This command deletes all manually configured routes and restarts the network
service.
If you are sure that you wish to proceed, then type 'proceed', otherwise type 'quit'.

> proceed
Proceeding...
Routing table successfully updated.

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.

> **NOTE** Running this command changes the interface state and causes the **ctc** service to restart (see Crypto Traffic Controller for QoS).

User Privileges

Users with the following privileges can perform this command:

- Admin
- Operator

Syntax

network route delete <routetype> <ipaddress> **-device** <netdevice> [**-metric** <metric>] [**-netmask** <ipaddress>] [**-gateway** <ipaddress>] [**-force**] [**-ipv6**]

Argument(s)	Shortcut	Description
<routetype>		Set to "network" or "host" for network or host specific routes respectively. **Valid values:** host, network
<IP_address>		Specifies the IP address of the target network or host to be deleted. You can specify an IPv4 or IPv6 address. If you are deleting an IPv6 address, you must also include the **-ipv6** flag in the command. When entering an IPv6 address, you can use full or shorthand syntax. For example, the following notations are equivalent: > 2001:0db3:8ba3:0000:0000:8a5e:03f0:7384 > 2001:db3:8ba3::8a5e:3f0:7384
-device <netdevice>	**-d**	Specifies a specific network device for the route. **Valid values:** eth0, eth1, eth2, eth3, bond0, bond1
-force	**-f**	Force the action without prompting
-gateway <IP_address>	**-g**	Specifies the gateway/router IP address to be deleted, if this is not a locally connected network or host.

Argument(s)	Shortcut	Description
-metric <metric>	**-m**	Specifies a routing metric. **Range:** 0 to 65535 **Default:** 0
-netmask <IP_address>	**-n**	Specifies the network mask. Include this option only if you are deleting a network route. If not specified, the default netmask is used. > If you are deleting an IPv4 route, you must specify the network mask in dotted-decimal format (for example, 255.255.255.0) > If you are deleting an IPv6 route, you must specify the prefix length (for example, 64) **Default:** > <routetype> = network IPv4: 255.255.255.0 IPv6: 64 > <routetype> = host IPv4: 255.255.255.255 IPv6: 128

Example

```
lunash:>network route delete host 123.45.67.89 -device eth2 -metric 1000

NOTICE: The network connection for device eth2 will be restarted for new network settings to
take effect.
If you are sure that you wish to restart the device connection, then type 'proceed', otherwise
type 'quit'
> proceed

Proceeding...

Command Result : Success
```

network route metric

Configure the metric value for all routing entries to a network device. This command should be used only on the advice of a network administrator.

> **NOTE** Running this command changes the interface state and causes the **ctc** service to restart (see Crypto Traffic Controller for QoS).

User Privileges

Users with the following privileges can perform this command:

- Admin
- Operator

Syntax

network route metric -name <device> **-metric** <metric>

Argument(s)	Shortcut	Description
-name <device>	**-d**	Specifies the network device to which you want to add the route. **Valid values:** eth0, eth1, eth2, eth3, bond0, bond1
-metric <metric>	**-m**	Specifies the routing metric to use for the route. **Range:** 1 to 65535

network route show

Display the current network route configuration. Manually configured routes are displayed for all physical devices (**eth0**, **eth1**, **eth2**, **eth3**), and all *active* bonded devices (**bond0**, **bond1**).

Depending on your Luna Appliance Software version and the options you specified, bonded interface routes may be deleted when the interface is disabled. See lunash:> "network interface bonding disable" on page 338 **-keeproutes** for more information.

User Privileges

Users with the following privileges can perform this command:

- Admin
- Operator
- Monitor

Syntax

network route show

Example using Luna Appliance Software 7.9.0 or newer

```
lunash:>network route show

Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
0.0.0.0         192.20.10.1     0.0.0.0         UG    100    0        0 eth0
192.20.9.0      192.20.10.1     255.255.255.0   UG    100    0        0 eth0
192.20.11.10    192.20.10.1     255.255.255.255 UGH   100    0        0 eth1


Command Result : 0 (Success)
```

Example using Luna Appliance Software 7.8.5 or older

```
lunash:>network route show


Manually configured routes

eth0:
ADDRESS0=192.20.9.1
NETMASK0=255.255.255.0
GATEWAY0=192.20.10.1
eth1:
ADDRESS0=192.20.11.1
NETMASK0=255.255.255.0
GATEWAY0=192.20.12.1
bond0:
ADDRESS0=192.20.13.1
NETMASK0=255.255.255.255
GATEWAY0=192.20.14.1
```

```
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
0.0.0.0         192.20.10.1     0.0.0.0         UG    100    0        0 eth0
192.20.9.0      192.20.10.1     255.255.255.0   UG    100    0        0 eth0
192.20.11.10   192.20.10.1     255.255.255.255 UGH   100    0        0 eth1


Command Result : 0 (Success)
```

network show

Display the network configuration for each network device on the appliance. Verbose mode also includes detailed capability information for each device, such as the supported and active link modes and auto-activation setting. This information is also collected in the **hsm supportinfo** command.

> **NOTE** If the network service has been stopped using the **service stop network** command, all network commands, including **network show**, will fail.

User Privileges

Users with the following privileges can perform this command:

- Admin
- Operator
- Monitor

Syntax

network show [**-verbose**]

Argument(s)	Shortcut	Description
-verbose	**-v**	Display additional capability and configuration information for each network device.

Example - standard 1G copper Ethernet Ports x 4

> **NOTE** For Luna Network HSM 7 appliances with four 1Gbps copper Ethernet ports, the network device configuration is factory set such that the two ports stacked vertically near the HSM card slot are designated Eth0 and Eth1 (Bond 0), while the remaining two ports, arranged horizontally above a ventilation grid near the center of the appliance back panel, are designated Eth2 and Eth3 (Bond 1).

 Copyright 2001-2025 Thales Group

Terse (non-verbose) mode

```
lunash:>network show


Hostname         : 192.20.9.109
Name Server(s)   :
Search Domain(s) : 20.9.109

Interface settings and status

HW Address (eth0)    : 00:15:B2:A8:FD:A8
IP Address (eth0)    : 192.20.9.109/24
Mask (eth0)          : 255.255.255.0
Gateway (eth0)       : 192.20.9.10
DNS (eth0)           :
DNS Search (eth0)    :
IP Protocol (eth0)   : IPv4
Protocol (eth0)      : Static
Auto Connect (eth0)  : Yes
Activated (eth0)     : Yes
Link detected (eth0) : Yes

HW Address (eth1)    : 00:15:B2:A8:FD:A9
IP Address (eth1)    : 192.20.9.102
Mask (eth1)          : 255.255.255.0
Gateway (eth1)       : 192.20.9.10
DNS (eth1)           :
DNS Search (eth1)    :
IP Protocol (eth1)   : IPv4
Protocol (eth1)      : Static
Auto Connect (eth1)  : Yes
Activated (eth1)     : No
Link detected (eth1) : No

HW Address (eth2)    : 00:15:B2:A8:FD:AA
IP Address (eth2)    : 2019:2:3:4:215:b2ff:fea8:fda2
Mask (eth2)          : 2019:2:3:4::/64
Gateway (eth2)       : fe80::c800:5ff:fe95:8
DNS (eth2)           :
DNS Search (eth2)    : sfnt.local.com
IP Protocol (eth2)   : IPv6
Protocol (eth2)      : SLAAC
Auto Connect (eth2)  : Yes
Activated (eth2)     : No
Link detected (eth2) : No

HW Address (eth3)    : 00:15:B2:A8:FD:AB
IP Address (eth3)    :
Mask (eth3)          :
Gateway (eth3)       :
DNS (eth3)           :
DNS Search (eth3)    :
IP Protocol (eth3)   : IPv4
Protocol (eth3)      : DHCP
Auto Connect (eth3)  : No
Activated (eth3)     : No
Link detected (eth3) : No
```

```
Status (bond0)       : Not configured

Status (bond1)       : Not configured

Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
0.0.0.0         192.20.9.10     0.0.0.0         UG    100    0        0 eth0
192.20.9.0      0.0.0.0         255.255.255.0   U     100    0        0 eth0

Kernel IPv6 routing table
Destination                    Next Hop                   Flag Met Ref Use If
::1/128                        ::                         U    256 0     0 lo
fe80::/64                      ::                         U    256 0     0 eth0
::/0                           ::                         !n   -1  1     1 lo
::1/128                        ::                         Un   0   1    69 lo
fe80::215:b2ff:fea8:fda8/128   ::                         Un   0   1     0 lo
ff00::/8                       ::                         U    256 0     0 eth0
::/0                           ::                         !n   -1  1     1 lo


Command Result : 0 (Success)
```

Verbose mode

```
lunash:>network show -verbose
```

[verbose output begins with same information as terse mode, but adds the following information]

```
Device and Connection Details
================================= eth0
=========================================================
BOOT PROTOCOL:                          dhcp
==========================================================================================
Settings for eth0:
Supported ports: [ TP ]
Supported link modes:   10baseT/Half 10baseT/Full
100baseT/Half 100baseT/Full
1000baseT/Full
Supported pause frame use: Symmetric
Supports auto-negotiation: Yes
Advertised link modes:  10baseT/Half 10baseT/Full
100baseT/Half 100baseT/Full
1000baseT/Full
Advertised pause frame use: Symmetric
Advertised auto-negotiation: Yes
Speed: 1000Mb/s
Duplex: Full
Port: Twisted Pair
PHYAD: 1
Transceiver: internal
Auto-negotiation: on
MDI-X: off (auto)
Supports Wake-on: pumbg
Wake-on: g
Current message level: 0x00000007 (7)
drv probe link
Link detected: yes
============================== eth1 ==============================================
BOOT PROTOCOL:                          dhcp
==============================================================================
```

```
Settings for eth1:
Supported ports: [ TP ]
Supported link modes:   10baseT/Half 10baseT/Full
100baseT/Half 100baseT/Full
1000baseT/Full
Supported pause frame use: Symmetric
Supports auto-negotiation: Yes
Advertised link modes:  10baseT/Half 10baseT/Full
100baseT/Half 100baseT/Full
1000baseT/Full
Advertised pause frame use: Symmetric
Advertised auto-negotiation: Yes
Speed: Unknown!
Duplex: Unknown! (255)
Port: Twisted Pair
PHYAD: 1
Transceiver: internal
Auto-negotiation: on
MDI-X: off (auto)
Supports Wake-on: pumbg
Wake-on: g
Current message level: 0x00000007 (7)
drv probe link
Link detected: no
============================ eth2 ==================================================
BOOT PROTOCOL:                           dhcp
==============================================================================
Settings for eth2:
Supported ports: [ TP ]
Supported link modes:   10baseT/Half 10baseT/Full
100baseT/Half 100baseT/Full
1000baseT/Full
Supported pause frame use: Symmetric
Supports auto-negotiation: Yes
Advertised link modes:  10baseT/Half 10baseT/Full
100baseT/Half 100baseT/Full
1000baseT/Full
Advertised pause frame use: Symmetric
Advertised auto-negotiation: Yes
Speed: Unknown!
Duplex: Unknown! (255)
Port: Twisted Pair
PHYAD: 1
Transceiver: internal
Auto-negotiation: on
MDI-X: off (auto)
Supports Wake-on: pumbg
Wake-on: g
Current message level: 0x00000007 (7)
drv probe link
Link detected: no
============================ eth3 ==================================================
BOOT PROTOCOL:                           dhcp
==============================================================================
Settings for eth3:
Supported ports: [ TP ]
Supported link modes:   10baseT/Half 10baseT/Full
100baseT/Half 100baseT/Full
```

```
1000baseT/Full
Supported pause frame use: Symmetric
Supports auto-negotiation: Yes
Advertised link modes:  10baseT/Half 10baseT/Full
100baseT/Half 100baseT/Full
1000baseT/Full
Advertised pause frame use: Symmetric
Advertised auto-negotiation: Yes
Speed: Unknown!
Duplex: Unknown! (255)
Port: Twisted Pair
PHYAD: 1
Transceiver: internal
Auto-negotiation: on
MDI-X: off (auto)
Supports Wake-on: pumbg
Wake-on: g
Current message level: 0x00000007 (7)
drv probe link
Link detected: no



Command Result: : 0 (Success)
```

Example - 10G Optical Ethernet x2 and 1G copper Ethernet x2

> **NOTE** For Network HSM appliances with the 10G optical Ethernet option, the network device configuration is factory set for
> - the optical 10Gbps ports are designated Eth0 and Eth1 (Bond 0) while
> - the remaining 1Gbps copper ports, stacked vertically near the HSM card slot, are designated Eth2 and Eth3 (Bond 1).

```
[10g2] lunash:>network show -verbose

   Hostname         : 10g2
   Name Server(s)   : 172.20.10.20      172.16.2.14
   Search Domain(s) : <not set>

Interface settings and status

   HW Address (eth0)    : 3C:FD:FE:CB:45:30
   Bond master (eth0)   : bond0
   Link detected (eth0) : Yes

   HW Address (eth1)    : 3C:FD:FE:CB:45:30
   Bond master (eth1)   : bond0
   Link detected (eth1) : Yes

   HW Address (eth2)    : 00:15:B2:AC:FC:84
   IP Address (eth2)    : 172.20.11.152/24
   Mask (eth2)          : 255.255.255.0
   Gateway (eth2)       : 172.20.11.10
   DNS (eth2)           : -
   DNS Search (eth2)    : -
```

```
   IP Protocol (eth2)   : IPv4
   Protocol (eth2)      : DHCP
   Auto Connect (eth2)  : Yes
   Activated (eth2)     : Yes
   Link detected (eth2) : Yes

   HW Address (eth3)    : 00:15:B2:AC:FC:85
   IP Address (eth3)    : 172.20.11.94/24
   Mask (eth3)          : 255.255.255.0
   Gateway (eth3)       : 172.20.11.10
   DNS (eth3)           : -
   DNS Search (eth3)    : -
   IP Protocol (eth3)   : IPv4
   Protocol (eth3)      : DHCP
   Auto Connect (eth3)  : Yes
   Activated (eth3)     : Yes
   Link detected (eth3) : Yes

   HW Address (bond0)    : 3C:FD:FE:CB:45:30
   IP Address (bond0)    : 172.20.11.7/24
   Mask (bond0)          : 255.255.255.0
   Gateway (bond0)       : 172.20.11.10
   DNS (bond0)           : -
   DNS Search (bond0)    : -
   IP Protocol (bond0)   : IPv4
   Protocol (bond0)      : Static
   Auto Connect (bond0)  : Yes
   Activated (bond0)     : Yes
   Link detected (bond0) : Yes
   Active Slaves (bond0) : eth0 eth1

   Status (bond1)       : Not configured

Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
0.0.0.0         172.20.11.10    0.0.0.0         UG    102    0        0 eth2
0.0.0.0         172.20.11.10    0.0.0.0         UG    103    0        0 eth3
0.0.0.0         172.20.11.10    0.0.0.0         UG    300    0        0 bond0
172.20.11.0     0.0.0.0         255.255.255.0   U     102    0        0 eth2
172.20.11.0     0.0.0.0         255.255.255.0   U     103    0        0 eth3
172.20.11.0     0.0.0.0         255.255.255.0   U     300    0        0 bond0

Device and Connection Details

================================= eth0 ====================================================
BOOT PROTOCOL:                           dhcp
===========================================================================================
Settings for eth0:
        Supported ports: [ FIBRE ]
        Supported link modes:   1000baseT/Full
                                10000baseT/Full
        Supported pause frame use: Symmetric
        Supports auto-negotiation: No
        Supported FEC modes: Not reported
        Advertised link modes:  1000baseT/Full
                                10000baseT/Full
        Advertised pause frame use: No
        Advertised auto-negotiation: No
```

```
        Advertised FEC modes: Not reported
        Speed: 10000Mb/s
        Duplex: Full
        Port: FIBRE
        PHYAD: 0
        Transceiver: internal
        Auto-negotiation: off
        Supports Wake-on: d
        Wake-on: d
        Current message level: 0x00000007 (7)
                               drv probe link
        Link detected: yes

================================ eth1 ==================================================
BOOT PROTOCOL:                          dhcp
=========================================================================================
Settings for eth1:
        Supported ports: [ FIBRE ]
        Supported link modes:   1000baseT/Full
                                10000baseT/Full
        Supported pause frame use: Symmetric
        Supports auto-negotiation: No
        Supported FEC modes: Not reported
        Advertised link modes:  1000baseT/Full
                                10000baseT/Full
        Advertised pause frame use: No
        Advertised auto-negotiation: No
        Advertised FEC modes: Not reported
        Speed: 10000Mb/s
        Duplex: Full
        Port: FIBRE
        PHYAD: 0
        Transceiver: internal
        Auto-negotiation: off
        Supports Wake-on: d
        Wake-on: d
        Current message level: 0x00000007 (7)
                               drv probe link
        Link detected: yes

================================ eth2 ==================================================
BOOT PROTOCOL:                          dhcp
=========================================================================================
Settings for eth2:
        Supported ports: [ TP ]
        Supported link modes:   10baseT/Half 10baseT/Full
                                100baseT/Half 100baseT/Full
                                1000baseT/Full
        Supported pause frame use: Symmetric
        Supports auto-negotiation: Yes
        Supported FEC modes: Not reported
        Advertised link modes:  10baseT/Half 10baseT/Full
                                100baseT/Half 100baseT/Full
                                1000baseT/Full
        Advertised pause frame use: Symmetric
        Advertised auto-negotiation: Yes
        Advertised FEC modes: Not reported
        Speed: 1000Mb/s
```

```
        Duplex: Full
        Port: Twisted Pair
        PHYAD: 1
        Transceiver: internal
        Auto-negotiation: on
        MDI-X: on (auto)
        Supports Wake-on: pumbg
        Wake-on: g
        Current message level: 0x00000007 (7)
                               drv probe link
        Link detected: yes

================================ eth3 ==================================================
BOOT PROTOCOL:                          dhcp
=========================================================================================
Settings for eth3:
        Supported ports: [ TP ]
        Supported link modes:   10baseT/Half 10baseT/Full
                                100baseT/Half 100baseT/Full
                                1000baseT/Full
        Supported pause frame use: Symmetric
        Supports auto-negotiation: Yes
        Supported FEC modes: Not reported
        Advertised link modes:  10baseT/Half 10baseT/Full
                                100baseT/Half 100baseT/Full
                                1000baseT/Full
        Advertised pause frame use: Symmetric
        Advertised auto-negotiation: Yes
        Advertised FEC modes: Not reported
        Speed: 1000Mb/s
        Duplex: Full
        Port: Twisted Pair
        PHYAD: 1
        Transceiver: internal
        Auto-negotiation: on
        MDI-X: off (auto)
        Supports Wake-on: pumbg
        Wake-on: g
        Current message level: 0x00000007 (7)
                               drv probe link
        Link detected: yes

Command Result : 0 (Success)
```

ntls

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

Syntax

ntls

bind
certificate
information
ipcheck
show
tcp_keepalive
threads
timer

Argument(s)	Shortcut	Description
bind	**b**	Set the NTLS binding. See "ntls bind" on the next page.
certificate	**c**	Access commands that allow you to manage the NTLS certificates. See "ntls certificate" on page 380.
information	**in**	Access commands that allow you to display NTLS status information. See "ntls information" on page 388.
ipcheck	**ip**	Access commands that allow you to manage the NTLS client source IP validation configuration. See "ntls ipcheck" on page 392.
show	**sh**	Show the NTLS binding. See "ntls show" on page 396.
tcp_keepalive	**tc**	Access commands that allow you to manage TCP keepalive. See "ntls tcp_keepalive" on page 397.
threads	**th**	Access commands that allow you to manage the NTLS worker threads. See "ntls threads" on page 401.
timer	**ti**	Access commands that allow you to manage the NTLS timer. See "ntls timer" on page 405.

ntls bind

Binds the network trust link service (NTLS) to a network device. You can bind NTLS to a specific device (eth0, eth1, eth2, or eth3), all devices (eth0, eth1, eth2, and eth3) or to a bonded interface (bond0 or bond1). See "network interface bonding" on page 329 for more information about creating a bonded interface.

> **NOTE** You can bind your NTLS traffic to an IPv4 or IPv6 device, but not to both IPv4 and IPv6 devices simultaneously. If some of the network devices on your Luna Network HSM 7 are configured with IPv4 addresses, while others are configured with IPv6 addresses, the **ntls bind all** command will bind NTLS to all IPv4 devices, while the **ntls bind all -ipv6** command will bind NTLS to all IPv6 devices.

You must restart the NTLS service for the change to take effect (see "service restart" on page 467):

- if the device you are binding to is configured and active, the NTLS traffic is bound to the new device immediately after NTLS restarts.
- if the device you are binding to is not configured or is inactive, the NTLS binding configuration is updated, but the NTLS traffic keeps its current binding. The NTLS traffic will begin using the new configuration only after you configure and connect the interface so that it becomes active, and restart the NTLS service.

If you wish, client traffic restriction could complement SSH traffic restriction using the command "sysconf ssh ip" on page 703 or "sysconf ssh device" on page 702, which restrict administrative traffic (over SSH) to a specific IP address or device name on your Luna Network HSM 7.

User Privileges

Users with the following privileges can perform this command:

- Admin
- Operator

Syntax

ntls bind <netdevice> [**-force**] [**-ipv6**]

Argument(s)	Shortcut	Description
-force	**-f**	Force the action without prompting.
-ipv6	**-i**	Use with **ntls bind all** to bind all IPv6 devices. This parameter is not required when binding to a specific IPv6 device (eth0, eth1, eth2, or eth3), or a specific bonded device (bond0 or bond1).

Argument(s)	Shortcut	Description
<netdevice>		Specifies the network device you want to bind to the NTLS service. All NTLS traffic to the appliance will use the specified network device. **Valid values:** **all:** Bind to all devices. Use without the **-ipv6** parameter to bind to all IPv4 devices. Use with the **-ipv6** parameter to bind to all IPv6 devices. **bond0:** Bind to the bond0 interface. See "network interface bonding" on page 329. **bond1:** Bind to the bond1 interface. **eth0:** Bind to the eth0 device. **eth1:** Bind to the eth1 device. **eth2**: Bind to the eth2 device. **eth3**: Bind to the eth3 device. **Default:** **all** (0.0.0.0). This will bind to all IPv4 devices.

Example

```
lunash:>ntls bind eth0

NTLS binding set to network device eth0.
You must restart the NTLS service for the 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)
```

ntls certificate

Access commands that allow you to manage the NTLS certificates.

Syntax

ntls certificate

monitor
show

Argument(s)	Shortcut	Description
monitor	**m**	Access commands that allow you to manage certificate expiry monitoring. See "ntls certificate monitor" on the next page.
show	**s**	Show the NTLS server certificate. See "ntls certificate show" on page 386.

ntls certificate monitor

Access commands that allow you to manage certificate expiry monitoring.

Syntax

ntls certificate monitor

disable
enable
show
trap trigger

Argument(s)	Shortcut	Description
disable	**d**	Disable certificate expiry monitoring. See "ntls certificate monitor disable" on the next page.
enable	**e**	Enable certificate expiry monitoring. See "ntls certificate monitor enable" on page 383.
show	**s**	Show the certificate expiry monitor status. See "ntls certificate monitor show" on page 384.
trap trigger	**t t**	Set the NTLS certificate expiry SNMP trap trigger. See "ntls certificate monitor trap trigger" on page 385.

ntls certificate monitor disable

Disable NTLS certificate expiry monitoring.

User Privileges

Users with the following privileges can perform this command:

- Admin
- Operator

Syntax

ntls certificate monitor disable

Example

```
lunash:>ntls certificate monitor disable

NTLS Server Cert Monitor disabled
Stopping certmonitord:                                    [  OK  ]

Command Result : 0 (Success)
```

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.

User Privileges

Users with the following privileges can perform this command:

- Admin
- Operator

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.

User Privileges

Users with the following privileges can perform this command:

- Admin
- Operator
- Monitor

Syntax

ntls certificate monitor show

Example

```
lunash:>ntls certificate monitor show


NTLS Server Certificate Expiry Monitor is enabled.

NTLS Server Certificate will expire on "Jul 17 17:23:13 2030 GMT"

Certificate expiry trap will be sent 5 days before the Certificate expiry day "Jul 17 17:23:13
2030 GMT" and on every 12 hour(s)

SNMP Trap is configured as the following:

  SNMP Trap Host                  : 192.168.143.7:162
  SNMP Trap Type                  : inform
  SNMP Version                    : 3
  SNMP v3 Security Name           : testsnmp2
  SNMP v3 Engine ID               : 0x1234567890
  SNMP v3 Security Level          : authPriv
  SNMP v3 Authentication protocol : SHA
  SNMP v3 Privacy protocol        : AES



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.

User Privileges

Users with the following privileges can perform this command:

- Admin
- Operator

Syntax

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

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

Example

```
lunash:>ntls certificate monitor trap trigger -preexpiry 30 -trapinterval 6


Certificate expiry trap is configured to be sent 30 days before the Certificate expiry day "Feb
22 15:19:21 2027 GMT" and on every 6 hour(s)
Stopping certmonitord:                                     [  OK  ]

Starting certmonitord:                                     [  OK  ]

Command Result : 0 (Success)
```

ntls certificate show

Display the contents of the NTLS server certificate.

User Privileges

Users with the following privileges can perform this command:

- Admin
- Operator
- Monitor

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=66331
        Validity
            Not Before: Feb 20 15:19:21 2017 GMT
            Not After : Feb 22 15:19:21 2027 GMT
        Subject: C=CA, ST=Ontario, L=Ottawa, O=Chrysalis-ITS, CN=66331
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
            Public-Key: (2048 bit)
            Modulus:
                00:cf:7b:9b:49:a8:77:dc:00:a4:0b:4a:6a:cc:5f:
                53:51:8a:c2:71:e0:e1:c2:81:15:fd:5a:e9:ee:bb:
                cf:fd:28:72:dc:f2:5a:3b:2b:5e:00:23:bb:4e:f9:
                ab:c3:bf:5d:c7:7f:46:37:b0:33:a5:30:19:01:df:
                db:2d:f7:72:6e:2f:9f:94:e6:49:83:33:71:e0:5c:
                09:71:4a:00:1f:65:53:a5:9a:c8:8c:3d:bf:f7:ac:
                d0:be:4e:0d:9a:c1:58:9a:17:43:10:59:ef:15:35:
                66:09:54:84:d5:0e:42:43:0b:99:11:99:44:89:ca:
                16:9c:70:03:bb:25:85:63:eb:29:7a:4e:8a:27:e7:
                ac:0b:4e:a8:67:d6:3d:c7:89:a9:b9:74:9a:68:f1:
                47:c1:85:09:a5:c8:b6:66:20:a2:51:8e:fe:5a:a5:
                53:b2:42:7c:be:53:56:86:77:2e:ed:94:65:a8:ee:
                f6:bc:01:53:9b:25:91:12:be:68:05:c1:04:0d:69:
                44:91:d1:13:5b:42:db:a4:f8:38:f3:b2:92:9d:6e:
                2b:02:e9:a8:c0:16:21:af:51:3b:39:3b:97:c0:52:
                20:e1:c7:bd:c4:02:4e:eb:87:55:a8:5c:51:be:70:
                9d:5e:52:fe:8f:3c:fa:9c:03:89:90:26:7a:d5:8f:
                a2:ad
            Exponent: 65537 (0x10001)
    Signature Algorithm: sha256WithRSAEncryption
        c3:91:3a:bc:ec:82:ac:a9:27:08:26:3d:9e:cc:ed:12:2b:bd:
```

```
        73:d1:ea:7b:f9:93:48:c9:2b:5a:4d:58:71:87:a6:9a:8f:ca:
        74:d1:d3:a6:92:7e:f9:b8:ff:54:6e:29:93:53:b3:b8:76:e2:
        f7:39:6a:0e:f9:fc:a0:9f:91:a8:8f:b4:65:ff:c4:3f:2e:b5:
        5c:fd:f1:a9:2e:93:b3:41:e8:a8:2d:da:b3:1f:d4:c2:29:62:
        a6:e5:0d:9e:87:fd:71:8a:f3:13:31:3c:5b:e1:1b:0d:db:4a:
        6c:d9:47:21:b4:0a:b3:e6:d5:5f:d1:77:c7:42:e1:c0:54:93:
        d4:ca:85:f7:40:db:6e:5f:39:4e:03:8b:60:e9:7c:94:7a:d8:
        3e:62:7f:23:02:44:f7:58:2d:b2:a7:ae:33:48:96:8d:8b:ff:
        b0:b1:e7:55:41:a4:40:3a:2e:f0:9a:02:d5:8a:e3:ea:74:e7:
        1e:66:48:d6:99:a5:8a:fb:0f:a4:8f:05:d2:89:33:67:2f:7b:
        2c:be:9f:0e:21:f9:6b:2c:86:22:77:68:d9:1a:62:55:28:ea:
        92:39:b3:58:9a:68:17:25:05:a8:ee:57:8b:ca:45:3a:ae:5a:
        f2:f2:09:0a:ea:1f:42:ff:04:86:21:5f:f0:28:9d:d3:69:fc:
        7d:f6:64:77


Command Result : 0 (Success)
```

ntls information

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

Syntax

ntls information

reset
show

Argument(s)	Shortcut	Description
reset	**r**	Reset the NTLS counters. See "ntls information reset" on the next page.
show	**s**	Display NTLS information. See "ntls information show" on page 390.

ntls information reset

Reset the NTLS counters.

> **NOTE** Resetting counters produces what is known as a "counter discontinuity" in the SNMP agent. The use of this functionality is therefore 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.

User Privileges

Users with the following privileges can perform this command:

- Admin
- Operator

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.
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 successfully 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 successfully connect to the HSM using the NTLS connection. This value can be reset using the **ntls information reset** command.

User Privileges

Users with the following privileges can perform this command:

- Admin
- Operator
- Monitor

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
```

ntls ipcheck

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

> **NOTE** If the client certificate was created and registered to the appliance using a hostname that can be resolved by the DNS, **ntls ipcheck** performs a DNS lookup using the registered hostname and compares the resolved IP to the source IP. In this case, ipcheck succeeds even if the client's actual IP changes.

Syntax

ntls ipcheck

disable
enable
show

Argument(s)	Shortcut	Description
disable	**d**	Disable NTLS client source IP validation. See "ntls ipcheck disable" on the next page.
enable	**e**	Enable NTLS client source IP validation. See "ntls ipcheck enable" on page 394.
show	**s**	Display the current client source IP validation configuration. See "ntls ipcheck show" on page 395.

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 Network HSM appliance. The checking is enabled by default.

User Privileges

Users with the following privileges can perform this command:

- Admin
- Operator

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 on a network trust link client connection. The checking is enabled by default. The best security of your client-to-Luna Network HSM 7 link is in force when ipcheck remains enabled. In general, keep ipcheck enabled *except* if network address translation (NAT) is enabled on your network between your client(s) and the Luna Network HSM 7 appliance. Confer with your network administrator in case of this or other situations where the ipcheck and configuration of your overall network might conflict.

> **NOTE** If the client certificate was created and registered to the appliance using a hostname that can be resolved by the DNS, **ntls ipcheck** performs a DNS lookup using the registered hostname and compares the resolved IP to the source IP. In this case, ipcheck succeeds even if the client's actual IP changes.

User Privileges

Users with the following privileges can perform this command:

- Admin
- Operator

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.

User Privileges

Users with the following privileges can perform this command:

- Admin
- Operator
- Monitor

Syntax

ntls ipcheck show

Example

```
lunash:>ntls ipcheck show

NTLS client source IP validation : Enable

Command Result : 0 (Success)
```

ntls show

You can bind the NTLS traffic to a specific device on the appliance. Use this command to display the following information for the NTLS binding:

> the network device that is configured to bind the NTLS traffic.

> the network device that is currently being used to bind the NTLS traffic.

Use the command "ntls bind" on page 378 to configure NTLS binding. The device you configure using the "ntls bind" on page 378 is not used until the following conditions have been met:

> it has been configured with a valid IP address.

> it is active on the network.

> the NTLS service is restarted.

This allows you to preconfigure the NTLS binding and have it become active only after you have completed your network configuration.

User Privileges

Users with the following privileges can perform this command:

> Admin

> Operator

> Monitor

Syntax

ntls show

Example

NTLS bound to a configured, active interface

```
lunash:>ntls show


NTLS is currently bound to IP Address: "192.20.11.78" (eth0)


Command Result : 0 (Success)
```

NTLS is bound to an inactive interface, or has not been restarted

```
lunash:>ntls show


NTLS is configured to bind to eth1, but it is not active at this time.
NTLS will bind to eth1 if it's active and has a valid IP address when NTLS restarts.
NTLS is currently bound to IP Address: "192.20.11.78" (eth0)


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

Argument(s)	Shortcut	Description
set	**-se**	Configure the NTLS TCP keep alive settings. See "ntls tcp_keepalive set" on the next page.
show	**-sh**	Display the current NTLS TCP keep alive configuration. See "ntls tcp_keepalive show" on page 400.

ntls tcp_keepalive set

Configure the NTLS TCP keepalive settings.

TCPKeepAlive is a TCP stack option, available at the Luna HSM Client and the Luna Network HSM 7 appliance. It is controlled via an entry in the Luna HSM Client configuration file, and an equivalent file on the Luna Network HSM 7.

On the Luna Network HSM 7 appliance, where you do not have direct access to the file system, the TCPKeepAlive= setting is controlled by lunash:> **"ntls tcp_keepalive set" above**.

The settings at the appliance and the client are independent. This allows a level of assurance, in case (for example) a firewall setting blocks communication in one direction.

User Privileges

Users with the following privileges can perform this command:

> Admin

> Operator

Syntax

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

Argument(s)	Shortcut	Description
-idle <seconds>	**-id**	Specifies the TCP keep alive idle timer, in seconds. This is the initial wait until a keep alive is issued. Recommended value is 200. **Range**: 10 to 10,000 **Default**: 10
-interval <seconds>	**-in**	Specifies the TCP keep alive interval time, in seconds. This is the duration between any two successive keep alive transmissions. Recommended value is 150. **Range**: 10 to 360 **Default**: 10
-probes <number>	**-p**	Specifies the number of retries to attempt if a transmission is not acknowledged. Recommended value is 15. **Range**: 1 to 30 **Default**: 2

> **NOTE** The default values are simply starting points intended to keep the feature "out of the way" until you configure for your particular network conditions. The recommended values are conservative, and address a common situation where a flurry of network activity might allow the probe count to be reached before the acknowledgment packets are able to return to the HSM appliance, which would cause the appliance to reset the connection.

Example

```
lunash:>ntls tcp_keepalive set -idle 200 -interval 150 -probes 15

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.

TCPKeepAlive is a TCP stack option, available at the Luna HSM Client and the Luna Network HSM 7 appliance. It is controlled via an entry in the Luna HSM Client configuration file, and an equivalent file on the Luna Network HSM 7. On the Luna Network HSM 7 appliance, where you do not have direct access to the file system, the TCPKeepAlive= setting is controlled by lunash:> **"ntls tcp_keepalive set" on page 398**.
The settings at the appliance and the client are independent. This allows a level of assurance, in case (for example) a firewall setting blocks communication in one direction.

User Privileges

Users with the following privileges can perform this command:

- Admin
- Operator
- Monitor

Syntax

ntls tcp_keepalive show

Example

```
lunash:>ntls tcp_keepalive show

NTLS TCP keepalive is configured as follows :

 TCP_KEEPIDLE  : 200
 TCP_KEEPINTVL : 150
 TCP_KEEPCNT   : 15


Command Result : 0 (Success)
```

ntls threads

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

Syntax

ntls threads

set
show

Argument(s)	Shortcut	Description
set	**se**	Configure the NTLS Datapath, CMD processor, and I/O service worker threads. See "ntls threads set" on the next page.
show	**sh**	Show the NTLS worker thread settings. See "ntls threads show" on page 404.

ntls threads set

Configure the datapath and command processor threads for the NTLS service.

> **NOTE** You must configure each member of an HA group to use the same settings. Failure to do so may result in unexpected behavior.

Determining the optimal number of threads for your environment and use cases
The default settings provide optimal performance for the majority of use cases. Increasing the number of threads does not necessarily 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.

If you experience performance or latency issues, you may need to experiment with different settings to determine the combination that provides the best performance and latency figures in your environment. It is recommended that you do not change these settings without first consulting with Thales Support.

User Privileges

Users with the following privileges can perform this command:

- Admin
- Operator

Syntax

ntls threads set [**-datapath** <number>] [**-cmdprocessor** <number>]

Argument(s)	Shortcut	Description
-cmdprocessor <number>	**-c**	Specifies the number of threads used in the command processor to submit HSM requests to the cryptographic module inside the appliance. The default value provides optimal performance for the majority of applications. Changing this value from the default may result in lower maximum throughput of some crypto operations, such as RSA Sign. **Range**: 1 to 70 **Default:** 20
-datapath <number>	**-d**	Specifies the number of worker thread pairs used to process inbound and outbound socket events. In practical terms, this value specifies the number of different NTLS clients, from different sockets, that the data path can support in parallel. You may need to increase this value if NTLS must service a high number of client connections. **Range**: 1 to 15 **Default**: 5

Example

```
lunash:>ntls threads set -cmdprocessor 40 -datapath 10

NOTICE: The NTLS and STCD services 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.

User Privileges

Users with the following privileges can perform this command:

- Admin
- Operator
- Monitor

Syntax

ntls threads show

Example

```
lunash:>ntls threads show


 Data path     : 10 threads
 CMD processor : 40 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

Argument(s)	Shortcut	Description
set	**se**	Configure the NTLS receive timeout value. See "ntls timer set" on the next page.
show	**sh**	Display the NTLS receive timeout value. See "ntls timer show" on page 407.

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.

User Privileges

Users with the following privileges can perform this command:

- Admin
- Operator

Syntax

ntls timer set -timeout <seconds>

Argument(s)	Shortcut	Description
-timeout <seconds>	**-t**	Specifies the timeout, in seconds. **Range:** 10 to 300 **Default**: 20

Example

```
lunash:>ntls timer set -timeout 30


Command Result : 0 (Success)
```

ntls timer show

Display the configured NTLS timeout period.

User Privileges

Users with the following privileges can perform this command:

- Admin
- Operator
- Monitor

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 Network HSM 7, using the **sftp** utility.

Syntax

package

deletefile
erase
list
listfile
update
verify

Argument(s)	Shortcut	Description
deletefile	**d**	Delete a package file. See "package deletefile" on the next page.
erase	**e**	Delete a package . See "package erase" on page 410.
list	**l**	List the installed packages. See "package list" on page 411.
listfile	**listf**	List the uninstalled package files. See "package listfile" on page 414.
update	**u**	Update the package file. See "package update" on page 415.
verify	**v**	Verify the package file. See "package verify" on page 417.

package deletefile

Deletes a named package file from the Luna Network HSM 7 appliance.

User Privileges

Users with the following privileges can perform this command:

- Admin
- Operator

Syntax

package deletefile <package_name>

Argument(s)	Description
<package_name>	Specifies the name of the package you want to delete.

Example

```
lunash:>package deletefile lunacuf_update-1.0.0-1.testCert.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 dependent 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 Thales Technical Support staff.

User Privileges

Users with the following privileges can perform this command:

- Admin
- Operator

Syntax

package erase <package_name>

Argument(s)	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 Thales Technical Support 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.

User Privileges

Users with the following privileges can perform this command Luna:

- Admin
- Operator
- Monitor

Syntax

package list

Example (release 7.8.4 and newer)

This is sample output; yours might differ, depending on which optional packages you have installed.

```
lunash:>package list


RPM LIST (SYSTEM)
-------------------
10GbE-7.8.4-253.x86_64
FM_TOOLS_SA-7.8.4-253.x86_64
NetworkManager-1.18.8-2.el7_9.x86_64
PedServer-7.8.4-253.x86_64
apiplugins-7.8.4-253.x86_64
audit-2.8.5-4.el7.x86_64
centos-release-7-9.2009.1.el7.centos.x86_64
certmonitord-7.8.4-253.x86_64
configurator-7.8.4-253.x86_64
ctc-1.0.0-1.x86_64
errorplugin-7.8.4-253.x86_64
fwupG5_real-6.28.0-20.x86_64
fwupG7_real-7.7.2-98.x86_64
fwupK7-7.8.4-253.x86_64
fwupK7_real-7.8.4-RC12.x86_64
g7-7.8.4-253.x86_64
hsmrecover-7.8.4-253.x86_64
k7-7.8.4-253.x86_64
kernel-3.10.0-327.36.3.el7.x86_64
kernel-3.10.0-1160.99.1.el7.x86_64
kernel-3.10.0-1160.102.1.el7.x86_64
libcryptoki-7.8.4-253.x86_64
lsta-7.8.4-253.x86_64
luna-lic-7.8.4-253.x86_64
luna-setup-7.8.4-253.x86_64
luna-snmp-7.8.4-253.x86_64
lunacm-7.8.4-253.x86_64
lunadiag-7.8.4-253.x86_64
lunalogd-7.8.4-253.x86_64
```

```
lunaped-7.8.4-253.x86_64
lunareset-7.8.4-253.x86_64
lush-base-7.8.4-253.x86_64
lush-config-files-7.8.4-253.x86_64
lush-pam-radius-7.8.4-253.x86_64
lush-spkg-7.8.4-253.x86_64
lush-standard-users-7.8.4-253.x86_64
lush-utils-7.8.4-253.x86_64
lush-utils-scripts-7.8.4-253.x86_64
net-snmp-5.7.2-49.el7_9.3.x86_64
net-snmp-agent-libs-5.7.2-49.el7_9.3.x86_64
net-snmp-libs-5.7.2-49.el7_9.3.x86_64
net-snmp-utils-5.7.2-49.el7_9.3.x86_64
net-tools-2.0-0.25.20131004git.el7.x86_64
ntp-4.2.6p5-29.el7.centos.2.x86_64
oamp-7.8.4-253.x86_64
openssh-7.4p1-23.el7_9.x86_64
openssh-clients-7.4p1-23.el7_9.x86_64
openssh-server-7.4p1-23.el7_9.x86_64
openssl-1.0.2k-26.el7_9.x86_64
openssl-libs-1.0.2k-26.el7_9.x86_64
pam-1.1.8-23.el7.x86_64
pedClient-7.8.4-253.x86_64
reimage-7.8.4-253.x86_64
release-SA-7.8.4-253.x86_64
sa_cmd_processor-7.8.4-253.x86_64
safenet-softtoken-7.8.4-253.x86_64
salogin-7.8.4-253.x86_64
stcd_processor2-7.8.4-253.x86_64
sysmod-7.8.4-253.x86_64
sysstatd-7.8.4-253.x86_64
systemd-219-78.el7_9.7.x86_64
uhd-7.8.4-253.x86_64
vtsd-7.8.4-253.x86_64
webserver-7.8.4-253.x86_64

Command Result : 0 (Success)
```

Example prior to release 7.8.4

```
lunash:>package list


RPM LIST (SYSTEM)
-------------------
libestr-0.1.9-2.el7.x86_64
centos-release-7-2.1511.el7.centos.2.10.x86_64
kernel-3.10.0-327.36.3.el7.x86_64
filesystem-3.2-20.el7.x86_64
NetworkManager-1.0.6-31.el7_2.x86_64
langtable-0.0.31-3.el7.noarch
pciutils-3.2.1-4.el7.x86_64
basesystem-10.0-7.el7.centos.noarch

...(clip 300 package names for space)...

glib-networking-2.42.0-1.el7.x86_64
hwdata-0.252-8.1.el7.x86_64
```

```
json-c-0.11-4.el7_0.x86_64

RPM LIST (SOFTWARE)
-------------------

Command Result : 0 (Success)
```

package listfile

Displays a list of package files that have been transferred to the Luna Network HSM 7 and are available to install.

User Privileges

Users with the following privileges can perform this command:

- Admin
- Operator
- Monitor

Syntax

package listfile

Example

```
lunash:>package listfile

     10562  Mar 15 2017 10:18 lunacuf_update-1.0.0-1.testCert.spkg
  82028450  Mar 15 2017 10:52 lunasa_update-7.0.0-2.x86_64.rpm.spkg
  82348418  Mar 15 2017 16:53 lunasa_update-7.0.0-4.spkg

Command Result : 0 (Success)
```

package update

Update an existing secure package on the Luna appliance. All packages from Thales 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.

> **CAUTION!** Use an uninterruptible power supply (UPS) to power your HSM. There is a small chance that a power failure during an update could leave your HSM in an unrecoverable condition.

If a version of this package is already installed, an error occurs:

```
Command failed: RPM update for original filename (fwupdateK7_RealCert-7.0.2-RC2.i386.rpm)
```

> **NOTE** You must log into the HSM before you run this command.

User Privileges

Users with the following privileges can perform this command:

- Admin
- Operator

Syntax

package update <filename> **-authcode** <authcode> [**-des3** | **-useevp**] [**-force**]

Argument(s)	Shortcut	Description
<filename>		The name of the update package file.
-authcode <authcode>	**-a**	Specifies the secure package authorization code provided by Thales with the secure package - the authorization code is checked during package installation to ensure that the package was encrypted and signed by Thales.
-des3	**-d**	Use DES3 Cipher for backward compatibility with older secure package updates (cannot be used simultaneously with **-useevp**).
-force	**-f**	Force the action - useful when scripting; this option causes the command to proceed without confirmation.
-useevp	**-u**	Use the OpenSSL EVP (Digital EnVeloPe library) API to decrypt and validate the update package in appliance software without need for HSM SO login. If this option is not specified, the default action is to refer update verification to the HSM (cannot be used simultaneously with **-des3**).

Example

```
lunash:>package update lunasa_update-7.1.0.spkg -authcode 5/Rd79MAGd/G9EY5

WARNING!!  Appliance software upgrade is a one-way operation: you
cannot downgrade the appliance software.
If you are sure that you wish to proceed, type 'proceed', otherwise type 'quit'.  >proceed

Command succeeded:  decrypt package

Command succeeded:  verify package certificate

Command succeeded:  verify package signature
Preparing packages...
lunasa_update-7.1.0.x86_64
Running update script

Version file found.
Proceeding with upgrade.
BEGINNING UPDATE......
   Updating to Luna SA Release 7.1.0

UNPACKING UPDATE FILES......

VERIFYING SOFTWARE PACKAGES......

1...Passed  2...Passed  3...Passed  4...Passed  5...Passed  6...Passed  7...Passed  8...Passed
9...Passed  10...Passed  11...Passed  12...Passed  13...Passed  14...Passed  15...Passed
16...Passed  17...Passed  18...Passed  19...Passed  20...Passed  21...Passed  22...Passed
23...Passed  24...Passed  25...Passed  26...Passed  27...Passed  28...Passed  29...Passed
30...Passed  31...Passed  32...Passed  33...Passed

INSTALLING SOFTWARE PACKAGES......

1...Passed  2...Passed  3...Passed  4...Passed  5...Passed  6...Passed  7...Passed  8...Passed
9...Passed  10...Passed  11...Passed  12...Passed  13...Passed  14...Passed  15...Passed
16...Passed  17...Passed  18...Passed  19...Passed  20...Passed  21...Passed  22...Passed
23...Passed  24...Passed  25...Passed  26...Passed  27...Passed  28...Passed  29...Passed
30...Passed  31...Failed  32...Failed  33...Failed

CLEANING UP FILES......

CLEANUP AFTER REMOVAL......


SOFTWARE UPDATE COMPLETED!

The system MUST now be rebooted for the changes to take effect.

Please ensure all client connections are terminated prior to rebooting the system.
To reboot, use the command "sysconf appliance reboot".

Update Completed

Copied all update log files, current and previous

Command Result : 0 (Success)
```

package verify

Verifies that the specified package is from Thales, and that the provided authcode is correct.

User Privileges

Users with the following privileges can perform this command:

> Admin

> Operator

Syntax

package verify <package_name> **-authcode** <authcode> [**-des3**] [**-useevp**]

Option	Shortcut	Description
<filename>	.	The name of the package file to verify.
-authcode <authcode>	**-a**	Specifies the secure package authorization code provided by Thales with the secure package - the authorization code is checked during package verification to ensure that the package was encrypted and signed by Thales.
-des3	**-d**	Use DES3 Cipher for backward compatibility with older secure package updates (cannot be used simultaneously with **-useevp**).
-useevp	**-u**	Use the OpenSSL EVP (Digital EnVeloPe library) API to validate the update package in appliance software without need for HSM SO login. If this option is not specified, the default action is to refer update verification to the HSM (cannot be used simultaneously with **-des3**).

Example

```
lunash:>package verify lunasa_update-7.1.0.spkg -authcode 5/Rd79MAGd/G9EY5


Command succeeded:  decrypt package

Command succeeded:  verify package certificate

Command succeeded:  verify package signature
Preparing packages...

Command Result : 0 (Success)
```

partition

Access commands used to manage partitions on the HSM. These commands are used by the HSM SO to create. delete, or resize partitions on the HSM. The partitions are owned by the Partition SO, and configured using LunaCM.

Syntax

partition

- **activate**
- **backup**
- **changepolicy**
- **changepw**
- **clear**
- **create**
- **createchallenge**
- **deactivate**
- **delete**
- **init**
- **init co**
- **init cu**
- **list**
- **rename**
- **resize**
- **restore**
- **show**
- **showcontents**
- **showpolicies**
- **stcidentity**

Argument(s)	Shortcut	Description
activate	**a**	Activate a role on the partition. See "partition activate" on page 420.
backup	**b**	Back up the contents of an application partition to a backup HSM. See "partition backup" on page 422.
changepolicy	**changepo**	Change policies on the partition. See "partition changePolicy" on page 426.
changepw	**changepw**	Change the password for a role on the partition. See "partition changePw" on page 428.
clear	**cl**	Delete all objects on a partition. See "partition clear" on page 430.

Argument(s)	Shortcut	Description
create	**cr**	Create an application partition on the HSM. See "partition create" on page 432.
createchallenge	**createc**	Create a challenge secret password for the Crypto Officer or Crypto User on a multifactor quorum-authenticated partition. See "partition createChallenge" on page 434.
deactivate	**dea**	De-cache a partition's PED key data. See "partition deactivate" on page 436.
delete	**del**	Delete an application partition from the HSM. See "partition delete" on page 437.
init	**i**	Initialize a newly created application partition, creating the PSO role (optional via LunaSH, if you prefer to do this via the Client-side LunaCM commands). See "partition init" on page 438.
init co	**i co**	Initialize the Crypto Officer (CO) role on a newly created application partition, using the credential of the newly created PSO role (optional via LunaSH, if you prefer to do this via the Client-side LunaCM commands). See "partition init co" on page 442.
init cu	**i cu**	The Crypto Officer can use this command to create a Crypto User role on the partition. See "partition init cu" on page 446.
list	**l**	Display a list of the accessible partitions. See "partition list" on page 447.
rename	**ren**	Renames the specified partition. See "partition rename" on page 448.
resize	**resi**	Re-sizes the storage space for a partition. See "partition resize" on page 450.
restore	**rest**	Restore the contents of an application partition from a backup HSM. See "partition restore" on page 452.
show	**sh**	Display information for a partition. See "partition show" on page 455.
showcontents	**showc**	Using this command, the Crypto Officer can display a list of all objects on a partition. See "partition showContents" on page 457.

Argument(s)	Shortcut	Description
showpolicies	**showp**	Display the policy settings of the specified partition. See "partition showPolicies" on page 459.
stcidentity	**st**	Export the specified partition's public key to a file. See "partition stcidentity" on page 462. This command syntax applies to Luna HSM Firmware 7.7.0 and newer only. For older versions, see "stc partition" on page 515.

partition activate

Activate a role on the partition. See Activation on Multifactor Quorum-Authenticated Partitions for more information.

> **NOTE** This command requires Luna Network HSM 7 Appliance Software 7.8.1 or newer. It cannot be used on STC partitions; the Partition SO must use LunaCM at the client for partition management.

User Privileges

Users with the following privileges can perform this command:

- Admin
- Operator

Syntax

partition activate -partition <name> [**-password** <password>] [**-cu**]

Argument(s)	Shortcut	Description
-partition <name>	**-par**	Specifies the name of the partition to activate. Obtain the partition name by using the **partition list** command.
-password <password>	**-pas**	Specifies the challenge secret for the Crypto Officer role. If you do not specify this secret, you are prompted for it.
-cu	**-c**	Activate the Crypto User role.

Example

```
lunash:>partition activate -partition myPartition


  Please enter the Crypto Officer challenge:
```

```
  > ********

Luna PED operation required to activate the partition - use Crypto Officer PED key.

'partition activate' successful


Command Result : 0 (Success)
```

partition backup

Back up the application partition contents to a Luna Backup HSM. This command copies the contents of a partition to a partition on the Backup HSM.

If you are creating a new backup partition, it is initialized during this process with the same cloning domain as the source partition. If you are backing up new objects to an existing backup partition with existing backup objects, you are prompted to verify if this destructive command should continue.

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

If you are backing up or restoring encrypted blobs stored on a V1 partition, the Backup HSM must be connected to the client:

> Luna Backup HSM 7 Connected to Luna HSM Client Using Direct Multifactor Quorum Authentication
> Luna Backup HSM 7 Connected to Luna HSM Client Using Remote Multifactor Quorum Authentication
> Luna Backup HSM 7 Connected to Luna HSM Client Using Password Authentication
> Backup/Restore Using Luna Backup HSM G5 Connected to Luna HSM Client

Only the SMK can be backed up/restored using an appliance-connected backup HSM.

For a list of required credentials, refer to:

Luna Backup HSM 7:

> **Direct Authentication:** Backing Up a Multifactor Quorum-Authenticated Partition
> **Remote PED Authentication:** Backing Up a Multifactor Quorum-Authenticated Partition
> Backing Up a Password-Authenticated Partition

Luna Backup HSM G5:

> Backing Up an Application Partition

User Privileges

Users with the following privileges can perform this command:

> Admin
> Operator

Syntax

partition backup -partition <name> **-serial** <serialnum> [**-tokenpar** <name>] [**-password** <password>] [**-tokensopwd** <password>] [**-domain** <domain>] [**-defaultdomain**] [**-tokenpw** <password>] [**-add**] [**-replace**] [**-force**]

Argument(s)	Shortcut	Description
-add	**-a**	Add objects to the existing backup partition specified with **-tokenpar**. Incremental backup (append). If the OUIDs of any source objects match OUIDs of objects already stored on the target backup, they are not backed up, and the existing backup objects are not overwritten. You must specify **-add** or **-replace** when backing up to an existing backup partition. You do not need to specify these options when backing up a V1 partition, as only the SMK is backed up.
-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 using this option.
-domain <domain>	**-do**	Specifies the domain string that was used when creating the source partition. If you do not supply this value on the command line, you are prompted for it. Applies to password-authenticated HSMs only; multifactor quorum-authenticated HSMs will prompt for the partition's red PED key. If you are creating a new backup partition, the application partition's domain is automatically used to initialize the backup partition. If you are specifying an existing backup partition as destination, the operation will only succeed if the domains match.
-force	**-f**	Force the action without prompting.
-partition <partition_name>	**-par**	Specifies the name of the source partition from which all data/key objects are backed up. Obtain the partition name by using the **partition list** command.
-password <partition password>	**-pas**	The partition Crypto Officer's password. If you do not supply this value on the command line, you are prompted for it. Applies to password-authenticated HSMs only; multifactor quorum-authenticated HSMs will prompt for the partition Crypto Officer's black PED key.

Argument(s)	Shortcut	Description
-replace	**-r**	Erase the contents of the existing backup and replace them with the contents of the source partition. You must specify **-add** or **-replace** when backing up to an existing backup partition. You do not need to specify these options when backing up a V1 partition, as only the SMK is backed up.
-tokenpar <backup_partition_name>	**-tokenpa**	Specifies the name of the destination backup partition on the Backup HSM. If you specify the name of an existing backup, that partition is selected. If no partition exists with the supplied label, 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 <backup_partition_password>	**-tokenpw**	Specifies the backup partition's Crypto Officer password. If you do not supply this value on the command line, you are prompted for it. Applies to password-authenticated HSMs only; multifactor quorum-authenticated HSMs will prompt for the Crypto Officer's black PED key.
-tokensopwd <backup_HSM_SO_pwd>	**-tokens**	The Backup HSM SO's password.Applies to password-authenticated HSMs only; multifactor quorum-authenticated HSMs will prompt for the Backup HSM SO's blue PED key. The Backup SO password need not be the same password or PED key as used for the source HSM SO.
-serial <serial_number>	**-s**	Specifies the Backup HSM serial number.

Example

```
lunash:>partition backup -partition sa78par1 -tokenpar sa78par1backup -serial 496771

  Please enter the password for the HSM user partition:
  > ********

  Please enter a password for the user on the backup token:
  > ********

  Please enter the cloning domain set when the HSM user partition was created:
  > ********

Object "MT RSA 4096-bit Private KeyGen" (handle 70) cloned to handle 14 on target
Object "MT RSA 4096-bit Public KeyGen" (handle 69) cloned to handle 18 on target
Object "MT RSA 4096-bit Private KeyGen" (handle 53) cloned to handle 19 on target
Object "MT RSA 4096-bit Public KeyGen" (handle 54) cloned to handle 23 on target
Object "MT RSA 4096-bit Private KeyGen" (handle 52) cloned to handle 24 on target
Object "MT RSA 4096-bit Public KeyGen" (handle 47) cloned to handle 28 on target
```

```
'partition backup' successful.

Command Result : 0 (Success)
```

partition changePolicy

Change policies on the partition. This command toggles or alters a policy of the specified 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.

> **NOTE** This command requires Luna Network HSM 7 Appliance Software 7.8.1 or newer. It cannot be used on STC partitions; the Partition SO must use LunaCM at the client for partition management.

This command must be executed by the appliance **admin**, logged in as Partition SO.

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. Refer to Partition Capabilities and Policies, for a list of all partition capabilities/policies and their meanings.

User Privileges

Users with the following privileges can perform this command:

- Admin
- Operator

Syntax

partition changePolicy -partition <name> **-policy** <policy#> **-value** <value> [**-psopin** <PSO_password>] [**-force**]

Argument(s)	Shortcut	Description
-partition <name>	**-pa**	Specifies the name of the partition on which to alter policies. Partition names are obtained with the **partition list** command.
-policy <policy#>	**-po**	Specifies the policy code of the policy to alter. Policy descriptions and codes are obtained with the **partition showpolicies** command.
-psopin <PSO_password>	**-ps**	Specifies the Partition Security Officer password for the partition. If this option is not included, LunaSH will prompt you to enter the PO password.
-value <value>	**-v**	Specifies the value that should be assigned to the specified policy. When specifying values for an on/off type policy, use '1' for on and '0' for off.
-force	**-f**	Force the option. Useful for scripting.

Example

```
lunash:>partition changePolicy -partition myPartition -policy 22 -value 1


Luna PED operation required to login as Partition Security Officer - use Partition Security
Officer (blue) PED key.


'partition changePolicy' successful.

Policy "Allow activation" is now set to: On


Command Result : 0 (Success)
```

partition changePw

Change the password for a role on the partition. For multifactor quorum-authenticated HSMs, this command allows you to change the PED key secret and/or the challenge secret. For password-authenticated HSMs, this command changes the partition password.

> **NOTE** This command requires Luna Network HSM 7 Appliance Software 7.8.1 or newer. It cannot be used on STC partitions; the Partition SO must use LunaCM at the client for partition management.

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

- Regular credential rotation as part of your organization's security policy
- Compromise of a role or secret due to loss or theft of a PED key
- Personnel changes in your organization or changes to individual security clearances
- Changes to your security scheme (implementing/revoking M of N, PINs, or shared secrets)

User Privileges

Users with the following privileges can perform this command:

- Admin
- Operator

Syntax

partition changePw -partition <name> [**-cu**] [**-newpw** <password>] [**-oldpw** <password>]

Parameter(s)	Shortcut	Description
-cu	**-c**	Change the password/PED key secret/challenge secret for the Crypto User role.
-newpw <password>	**-n**	Specifies the new partition password.
-oldpw <password>	**-o**	Specifies the existing partition password, to be replaced by the new password.
-partition <name>	**-p**	Specifies the partition name. Partition names are obtained with the **partition list** command.

Example

```
lunash:>partition changePw -partition myPartition
```

```
  Which part of the partition password do you wish to change?

  1.  change partition PED key data for Crypto Officer
  2.  change the challenge for Crypto Officer
  0.  abort command

  Please select one of the above options: 1


  Please enter the current Crypto Officer's challenge:
  > ********

Luna PED operation required to change partition PED data - use Crypto Officer PED key.

Warning:  PED key change has caused Crypto Officer role deactivation. Please
          use 'partition activate' to re-activate.

'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.

> **NOTE** This command requires Luna Network HSM 7 Appliance Software 7.8.1 or newer. It cannot be used on STC partitions; the Partition SO must use LunaCM at the client for partition management.

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 multifactor quorum-authenticated HSMs, Luna PED action is required, and the Crypto Officer (black) PED key is requested. Any password provided at the command line is ignored. However, if a PIN was specified when the HSM partition was created, that PIN must be entered at the Luna PED keypad.

User Privileges

Users with the following privileges can perform this command:

- Admin
- Operator

Syntax

partition clear -partition <partition_name> [**-password** <password>] [**-force**]

Argument(s)	Shortcut	Description
-force	**-f**	Force the action without prompting.
-partition <name>	**-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 <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 myPartition



  Please enter the Crypto Officer's challenge:
  > ********

CAUTION:  Are you sure you wish to clear the partition named:
            myPartition
          This will ERASE all the objects on the partition.
```

```
          Type 'proceed' to clear the partition, or 'quit'
          to quit now.
          > proceed

'partition clear' successful.


Command Result : 0 (Success)
```

partition create

Create an HSM partition on the HSM. This command creates a new HSM partition on the HSM. You must be logged in as HSM SO to use this command.

Partition names created in LunaSH must be 1-32 characters in length. The following characters are allowed:

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

Spaces are allowed; enclose the partition name in double quotes if it includes spaces.

The following characters are not allowed: `&\|;<>`"?`

No two partitions can have the same name.

Use the LunaCM command **partition init** to initialize the partition.

User Privileges

Users with the following privileges can perform this command:

> Admin

> Operator

Syntax

partition create -partition <name> [**-size** <size>] [**-allfreestorage**] [**-version** <number>] [**-force**]

Argument(s)	Shortcut	Description
-allfreestorage	**-a**	Create the partition using all the remaining unused storage space on the HSM. Existing partitions, if any, are part of 'used space' and are not affected by this operation. After you create a partition with this option, you cannot create another without first deleting or resizing partitions to regain some space.
-force	**-f**	Force the partition creation with no prompting - you are still prompted by Luna PED, if yours is a multifactor quorum-authenticated HSM.
-partition <name>	**-pa**	Specifies the name to assign to the application partition. The name must be unique among all application partitions on the HSM.
-size <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.

Argument(s)	Shortcut	Description
-version	**-v**	*Version 0* [default] specifies that the partition is created to use the pre-firmware 7.7.0 cloning protocol and behaves like any partition created before Luna HSM Firmware 7.7.0, where backup/restore and HA object replication are accomplished via cloning. This partition status in a newly created partition is equivalent to the state of pre-existing partitions after the containing HSM firmware is updated to Luna HSM Firmware 7.7.0 or newer. *Version 1* specifies that the partition is created to use the Luna HSM Firmware 7.7.0 cloning protocol such that backup/restore and HA object replication are accomplished via SKS. The only object that is backed-up or replicated by cloning is the SKS Master Key (SMK). Per-Key Authorization (PKA) and Sole Control of keys are also supported by this partition version (when using updated Client and API). The partition version type can be changed after creation, by the Partition Security Officer - see Partition Policy 41 in Partition Capabilities and Policies. **NOTE** partition changepolicy for policy 41 is > non-destructive in the V0 to V1 direction, but can be set to destructive, if desired > destructive for V1 to V0, and destructiveness cannot be changed by command or by Partition Policy Template (PPT).

Example

```
lunash:>partition create -partition partition1


          Type 'proceed' to create the partition, or
          'quit' to quit now.
          > proceed
'partition create' successful.


Command Result : 0 (Success)



lunash:>partition create -partition partition2 -size 400000


On completion, you will have 2 partition(s) with 32811040 bytes remaining for up to 98 more
partitions.
          Type 'proceed' to create the partition, or
```

```
          'quit' to quit now.
          > proceed
'partition create' successful.

Command Result : 0 (Success)


lunash:>partition create -partition eidas_partition -force

Force option used. Proceed prompt bypassed.

'partition create' successful.

Command Result : 0 (Success)



lunash:> partition create -version 0 -partition my-vee-zero_par -force

Force option used. Proceed prompt bypassed.

'partition create' successful.

Command Result : 0 (Success)
```

partition createChallenge

Create a challenge secret password for the Crypto Officer or Crypto User on a multifactor quorum-authenticated partition.

> **NOTE** This command requires Luna Network HSM 7 Appliance Software 7.8.1 or newer. It cannot be used on STC partitions; the Partition SO must use LunaCM at the client for partition management.

User Privileges

Users with the following privileges can perform this command:

- Admin
- Operator

Syntax

partition createChallenge -partition <name> **-role** <partition_role> [**-challengesecret** <password>]

Argument(s)	Shortcut	Description
-challengesecret <password>	**-c**	Specify the initial challenge secret in the command line.

Argument(s)	Shortcut	Description
-partition <name>	**-p**	Specifies the partition name. Partition names are obtained with the **partition list** command.
-role <role>	**-r**	Specifies the role to set a challenge secret for. Valid Values: **co**, **cu**

Example

```
lunash:>partition createChallenge -partition myPartition -role co



  Please enter a new challenge secret for the partition role:
  > ********

  Please re-enter the challenge secret to confirm:
  > ********

Luna PED operation required to login as Partition Security Officer - use Partition Security
Officer (blue) PED key.


Partition challenge for co role was successfully created.


Command Result : 0 (Success)
```

partition deactivate

De-cache a partition's PED key data. Afterwards, clients cannot authenticate to the partition with just their partition password. While the partition is deactivated, each client attempt initiates a login call, which requires the appropriate Luna PED. See Activation on Multifactor Quorum-Authenticated Partitions for more information.

> **NOTE** This command requires Luna Network HSM 7 Appliance Software 7.8.1 or newer. It cannot be used on STC partitions; the Partition SO must use LunaCM at the client for partition management.

User Privileges

Users with the following privileges can perform this command:

- Admin
- Operator

Syntax

partition deactivate -partition <name> [**-cu**]

Argument(s)	Shortcut	Description
-partition <name>	**-p**	The name of the partition to delete. Obtain the partition name by using the **partition list** command.
-cu	**-c**	Perform the task as Crypto User.

Example

```
lunash:>partition deactivate -partition myPartition


'partition deactivate' successful.


Command Result : 0 (Success)
```

partition delete

Delete an application partition from the HSM. This command deletes an application partition on the HSM and frees the license used by the application partition. To use the **partition delete** command you must be logged in as HSM SO.

User Privileges

Users with the following privileges can perform this command:

- Admin
- Operator

Syntax

partition delete -partition <partition_name> [**-force**]

Argument(s)	Shortcut	Description
-force	**-f**	Force the action without prompting.
-partition <partition_name>	**-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 partition2


CAUTION:  Are you sure you wish to delete the partition named:
            partition2
          Type 'proceed' to delete the partition, or 'quit'
          to quit now.
          > proceed
'partition delete' successful.


Command Result : 0 (Success)
```

partition init

Initialize an application partition.

> **CAUTION!** This command requires Luna Network HSM 7 Appliance Software 7.8.1 or newer. Do not attempt to use it to initialize an STC partition, or assigned clients will lose contact with the partition. The Partition SO must use LunaCM at the client for partition management.

- This command might be preferred in situations where management of the appliance and HSM, and of client configuration, are owned by the same person or organization.
- For situations where the ownership, configuration, and use of application partitions is expected to be held by a separate person or organization, then you might prefer to initialize the partition via client connection and LunaCM commands - see partition init and role commands instead.

For password-authenticated HSMs, if the password is not provided via the command line, the user is interactively prompted for it. Input is echoed as asterisks, and user is asked for password confirmation. This creates the Partition Security Officer role.

For multifactor quorum-authenticated HSMs, Luna PED action is required, and a Partition SO PED key (blue) is imprinted. Any password provided at the command line is ignored.

With the **partition init** command, you create the *Partition Security Officer (PSO) credential*. That credential is then needed by the person who creates the Crypto Officer role in LunaSH or LunaCM.

Domain matching and the default domain

If you do not specify a domain in the command line (password-authenticated HSMs), you are prompted for it.

If you type a character string at the prompt, that string becomes the domain for the partition. This applies to password-authenticated HSMs. For multifactor quorum-authenticated HSMs, the string is not needed and is ignored, because the HSM creates and/or imprints a domain PED key.

Thereafter, for any action that involves cloning, the domain on source and target will need to match (this includes backup and restore operations, HA synchronization operations, or partition clone commands via the client).

Partition initialization via LunaSH is first time only

You can initialize a partition only one time via this command. Any subsequent re-initialization must be done from the client (using lunacm commands).

After initializing a partition with this command (**partition init**),

- you can initialize the Crypto Officer role from the appliance side with the LunaSH command "partition init co" on page 442, or
- you can do it from a registered client using LunaCM role commands.

In either case, you will need the PSO credentials.

User Privileges

Users with the following privileges can use this command:

- **admin**

> **operator**

Syntax

partition init -partition <name> [**-password** <string>] [**-domain** <string>] [**-pptfile** </filename>] [**-defaultdomain**] [**-auth**] [**-force**]

Argument(s)	Shortcut	Description
-defaultdomain	**-def**	This option is deprecated. It applies to password-authenticated HSMs only. It allows you to set a default domain that is compatible with certain legacy HSMs, instead of specifying a unique domain string with **-domain**. Using a default domain secret means that key cloning and backup/restore operations are protected by Crypto Officer authentication only.
-domain	**-d**	Partition cloning domain string. Used only on password-authenticated HSMs; ignored for multifactor quorum-authenticated. The domain secret allows for two layers of cloning security: > The Partition SO determines which partitions can clone objects to each other by setting the same domain on the source and destination partitions. > The Crypto Officer for the partition must authorize the cloning operation. The domain string must be 1-128 characters in length. The following characters are allowed: `abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789 !@#$%^*-_=+[]{}()/:',.~` The following characters are problematic or invalid and must not be used in a domain string: `"&;<>?\`|` Spaces are allowed, as long as the leading character is not a space; to specify a domain string with spaces using the **-domain** option, enclose the string in double quotation marks. For password-authenticated HSMs, the domain string should match the complexity of the partition password. See Domain Planning for more information.
-force	**-f**	Force the action (useful for scripting).
-label <label>	**-l**	Label for the partition. This is how the partition is seen when viewed from the Client side (such as in lunacm slot list). *If an explicit label value is not entered*, then the value provided for the partition *name* is also used for the *label*. In LunaSH, the partition label created during initialization must be 1-32 characters in length. The following characters are allowed: `abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789 !@#$%^*()-_=+[]{}/:',.~` Spaces are allowed; enclose the label in double quotation marks if it includes spaces.

Argument(s)	Shortcut	Description
-partition <partition name>	**-par**	This is the name by which the partition appears to the HSM SO in LunaSH. This name is meaningful to the appliance **admin**, and does not need to reflect how the partition is eventually used by applications (see **-label**, which can match or can be completely different if desired).
-password	**-pas**	Partition Security Officer password. Used only on password-authenticated HSMs; ignored for multifactor quorum-authenticated. Passwords and activation challenge secrets must be 8-255 characters in length. Spaces are allowed; to specify a password with spaces using command-line options, enclose the password in double quotation marks. The space character may not be used as the first character in a password. The following characters are allowed: `!#$%'()*+,-./0123456789:=? @ABCDEFGHIJKLMNOPQRSTUVWXYZ[]^_ abcdefghijklmnopqrstuvwxyz{}~` This character set is enforced when using Luna Appliance Software 7.9.0 or Luna HSM Client 10.8.0 or newer, and recommended for all previous versions. Previously-set passwords and challenge secrets are unaffected, but the new character set is enforced when these passwords are changed.
-pptfile <filename>	**-pp**	Apply a policy template located in the user files. This feature requires minimum Luna HSM Firmware 7.1.0. **NOTE** If there is a mismatch between template policies and the default values of newer or dependent policies, then the attempt to apply the old policy would fail with CKR_FAILED_DEPENDENCIES. You have the option to edit a policy file before applying it, to add newer policies. LunaSH does not include provision for editing template files. You can edit externally, before uploading a Partition Policy Template file, if needed.

Example without Partition Policy Template

```
lunash:>par init -par part1 -l my_pw_partition -pas Some!Pa55w0rd -d domain



Command Result : 0 (Success)
lunash:>

lunash:>par show -p part1


   Partition Name:                                     part1
   Partition SN:                             1552202447876
   Partition Label:                        my_pw_partition
   Partition Version:                                    0
```

```
   Partition SO PIN To Be Changed:                        no
   Partition SO Zeroized:                                 no
   Partition SO Login Attempts Left:                      10
   Partition SO Change Password Attempts Left:            10
   Crypto Officer is not initialized.
   Crypto User is not initialized.
   Legacy Domain Has Been Set:                            no
   Partition Storage Information (Bytes):
                Total=6628214
                Used=0
                Free=6628214
   Partition Object Count:                                 0
   Partition SMK OUIDs:
               SMK-FW4: Not Initialized
               SMK-FW6: Not Initialized
               SMK-FW7-FM: Not Initialized
               SMK-FW7-Rollover: Not Initialized
               SMK-FW7-Primary: Not Initialized


Command Result : 0 (Success)
lun
```

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

Example with Partition Policy Template

```
lunash:>par init -par part1 -l part1_pw -pas default -d domain -pp part1_pw.ppt

    ID  Value   off-to-on Destructive   on-to-off Destructive
   ----------------------------------------------------------
    41      1                       0                       1

   Above Partition policy template values will be applied.
          Type 'proceed' to continue, or 'quit'
          to quit now.
          > proceed


Command Result : 0 (Success)
lunash:>

lunash:>c as -c 10.124.79.145 -p part1


'client assignPartition' successful.


Command Result : 0 (Success)
```

partition init co

> **NOTE** This command is available using Luna Network HSM 7 Appliance Software 7.7.1 or newer.

Initialize the Crypto Officer (CO) role on an application partition where the partition has already been created ("partition create" on page 432) and the Partition Security Officer (PSO) role has already been initialized ("partition init" on page 438). To initialize the CO role on a partition, you need the PSO credentials for that partition.

- This command (**partition init co**) might be preferred in situations where management of the appliance and HSM, and of client configuration, are owned by the same person or organization.
- For situations where the ownership, configuration, and use of application partitions is expected to be held by a separate person or organization, then you might prefer to initialize the partition Crypto Officer role via client connection and LunaCM commands - see role commands instead.

For password-authenticated HSMs, if the password is not provided via the command line, the user is interactively prompted for it. Input is echoed as asterisks, and user is asked for password confirmation. This creates the Partition Security Officer role.

For multifactor quorum-authenticated HSMs, Luna PED action is required, and a Partition SO PED key (blue) is imprinted. Any password provided at the command line is ignored.

First password is temporary

Initialization of the Crypto Officer role sets the *initial* password; that password must be changed via lunacm commands on the client before crypto operations are permitted by the CO role user. The person undertaking the CO role on the client must be given the CO password, because

- all subsequent role password changes on CO and
- all CO activities (administrative or crypto) can be done only from the client (LunaCM).

Initialization of Crypto User and other roles is done only at the client.

Syntax

partition init co -partition <name> [**-psopin** <password>] [**-copin** <password>] [**-force**]

Argument(s)	Shortcut	Description

-copin	**-c**	Partition Crypto Officer password, being assigned to the CO role that is being created by this command. Used only on password-authenticated HSMs; ignored for multifactor quorum-authenticated.
		Passwords and activation challenge secrets must be 8-255 characters in length. Spaces are allowed; to specify a password with spaces using command-line options, enclose the password in double quotation marks. The space character may not be used as the first character in a password.
		The following characters are allowed:
		`!#$%'`
		`()*+,-./0123456789:=? @ABCDEFGHIJKLMNOPQRSTUVWXYZ`
		`[]^_abcdefghijklmnopqrstuvwxyz{}~`
		This character set is enforced when using Luna Appliance Software 7.9.0 or Luna HSM Client 10.8.0 or newer, and recommended for all previous versions. Previously-set passwords and challenge secrets are unaffected, but the new character set is enforced when these passwords are changed.

-force	**-f**	Force the action (useful for scripting).
-partition <partition name>	**-pa**	This is the name by which the partition appears to the HSM SO in LunaSH.
-psopin	**-ps**	Partition Security Officer Password. Used only on password-authenticated HSMs; ignored for multifactor quorum-authenticated.

Example with all required arguments on password-authenticated HSM

```
lunash:>par init co -pa part1  -ps PSOs!Pa55w0rd -c Some!Pa55w0rd


Command Result : 0 (Success)
lunash:>

lunash:>par show -p part1



   Partition Name:                                     part1
   Partition SN:                               1552202447883
   Partition Label:                                 part1_pw
   Partition Version:                                      0
   Partition SO PIN To Be Changed:                        no
   Partition SO Zeroized:                                 no
   Partition SO Login Attempts Left:                      10
   Partition SO Change Password Attempts Left:            10
   Crypto Officer PIN To Be Changed:                     yes
   Crypto Officer Locked Out:                             no
```

```
   Crypto Officer Login Attempts Left:                    10
   Crypto Officer Change Password Attempts Left:          10
   Crypto User is not initialized.
   Legacy Domain Has Been Set:                            no
   Partition Storage Information (Bytes):
                Total=6628214
                Used=0
                Free=6628214
   Partition Object Count:                                 0
   Partition SMK OUIDs:
               SMK-FW4: Not Initialized
               SMK-FW6: Not Initialized
               SMK-FW7-FM: Not Initialized
               SMK-FW7-Rollover: Not Initialized
               SMK-FW7-Primary: Not Initialized


Command Result : 0 (Success)
```

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

Example with neither password provided on password-authenticated HSM

```
lunash:>par init co -pa part1


  Please enter the Partition owner's password:
  > *******


  Please enter the Partition Crypto Officier's initial password:
  > *******

  Please re-enter the Partition Crypto Officer's initial password:
  > *******

Command Result : 0 (Success)
```

Example on multifactor quorum-authenticated HSM

```
lunash:>par init co -pa part1 -c default


Warning:    Initial CO password will be ignored on a PED based SA.

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

Luna PED operation required to initialize the CO role.
Please attend to the PED.
```

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

partition init cu

The Crypto Officer can use this command to create a Crypto User role on the partition.

> **NOTE** This command requires Luna Network HSM 7 Appliance Software 7.8.1 or newer. It cannot be used on STC partitions; the Partition SO must use LunaCM at the client for partition management.

User Privileges

Users with the following privileges can perform this command:

- Admin
- Operator

Syntax

partition init cu -partition <partition_name> [**-copin** <password>] [**-cupin** <password>] [**-force**]

Argument(s)	Shortcut	Description
-copin <password>	**-co**	The password of the Crypto Officer, when creating a Crypto User on a password-authenticated HSM.
-cupin <password>	**-cu**	The initial Crypto User password, being assigned when creating a Crypto User on a password-authenticated HSM.
-force	**-f**	Force the action without prompting.
-partition <name>	**-p**	The name of the HSM partition on which to create the Crypto User. Obtain the HSM partition name by using the **partition list** command.

Example

```
lunash:>partition init cu -partition myPartition


  Please enter the Partition Crypto Officer's challenge:
  > ********


Command Result : 0 (Success)
```

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 having to calculate the exact memory space available for data storage -- 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**.

User Privileges

Users with the following privileges can perform this command:

- Admin
- Operator
- Monitor

Syntax

partition list

Example

```
lunash:>partition list

                                                        Storage (bytes)
                                                  ---------------------------
 Partition            Name                    Objects   Total    Used    Free
 ==============================================================================
 154438865289         partition1                    6  150000    1232  148768
 154438865290         partition2                    0  325873       0  325873
 154438865291         partition3                    0  325891       0  325891
 154438865292         partition4                    0  325909       0  325909
 154438865293         partition5                    0  325928       0  325928


Command Result : 0 (Success)
```

partition rename

Renames the specified partition. This command does not affect the label set by the Partition SO during initialization.

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

Partition names created in LunaSH must be 1-32 characters in length. The following characters are allowed:

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

Spaces are allowed; enclose the partition name in double quotes if it includes spaces.

The following characters are not allowed: `&\|;<>`"?`

No two partitions can have the same name.

> **NOTE** This feature requires minimum Luna HSM Firmware 7.2.0 and Luna Network HSM 7 Appliance Software 7.2.0.

User Privileges

Users with the following privileges can perform this command:

- Admin
- Operator

Syntax

partition rename -partition <name> **-newname** <name> [**-force**]

Argument(s)	Shortcut	Description
-force	**-f**	Force the action without prompting for confirmation.
-newname	**-n**	Specifies the new partition name. To include spaces in the partition name, enclose the new partition name in quotation marks.
-partition	**-p**	Specifies the current name of the partition to be renamed.

Example

```
lunash:>partition rename -partition par1 -newname "user partition1"


CAUTION:  Are you sure you wish to make the following changes to partition "par1"?:
              Partition name:   user partition1
              Partition label:  no change

          Type 'proceed' to change the partition name/label, or 'quit'
          to quit now.
          > proceed
        Partition name successfully updated in the partition file list.
```

```
        Partition name successfully updated in the Client Authenticate Configuration File.

'partition rename' successful.


Command Result : 0 (Success)
```

partition resize

Resizes the storage space of the named partition.

You must be logged in as HSM Security Officer to run this command.

User Privileges

Users with the following privileges can perform this command:

> Admin

> Operator

Syntax

partition resize -partition <name> {**-size** <bytes> | **-allfreestorage**} [**-force**]

Argument(s)	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 <name>	**-p**	Specifies the name of the partition.
-size <bytes>	**-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 Name:                          partition1
   Partition SN:                            154438865289
   Partition Label:                         myPartition
   Partition SO     PIN To Be Changed:      no
   Partition SO     Zeroized:               no
   Partition SO     Login Attempts Left:    10
   Crypto Officer   PIN To Be Changed:      no
   Crypto Officer   Locked Out:             no
   Crypto Officer   Login Attempts Left:    10
   Crypto User      PIN To Be Changed:      no
   Crypto User      Locked Out:             no
   Crypto User      Login Attempts Left:    10
   Legacy Domain Has Been Set:              no
```

```
   Partition Storage Information (Bytes):     Total=324096, Used=1232, Free=322864
   Partition Object Count:                    6

Command Result : 0 (Success)



lunash:>partition resize -partition partition1 -size 150000

'partition resize' successful.

Command Result : 0 (Success)



lunash:>partition show

   Partition Name:                            partition1
   Partition SN:                              154438865289
   Partition Label:                           myPartition
   Partition SO     PIN To Be Changed:        no
   Partition SO     Zeroized:                 no
   Partition SO     Login Attempts Left:      10
   Crypto Officer   PIN To Be Changed:        no
   Crypto Officer   Locked Out:               no
   Crypto Officer   Login Attempts Left:      10
   Crypto User      PIN To Be Changed:        no
   Crypto User      Locked Out:               no
   Crypto User      Login Attempts Left:      10
   Legacy Domain Has Been Set:                no
   Partition Storage Information (Bytes):     Total=150000, Used=1232, Free=148768
   Partition Object Count:                    6

Command Result : 0 (Success)
```

partition restore

Restores the contents of a backup partition stored on a Luna Backup HSM to an application partition. The partition Crypto Officer executing this command has the option of replacing the objects existing on the partition or adding to them.

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

If you are backing up or restoring encrypted blobs stored on a V1 partition, the Backup HSM must be connected to the client:

> Luna Backup HSM 7 Connected to Luna HSM Client Using Direct Multifactor Quorum Authentication
> Luna Backup HSM 7 Connected to Luna HSM Client Using Remote Multifactor Quorum Authentication
> Luna Backup HSM 7 Connected to Luna HSM Client Using Password Authentication
> Backup/Restore Using Luna Backup HSM G5 Connected to Luna HSM Client

Only the SMK can be backed up/restored using an appliance-connected backup HSM.

For a list of required credentials, refer to:

Luna Backup HSM 7:

> **Direct Authentication:** Restoring a Multifactor Quorum-Authenticated Partition From Backup
> **Remote PED Authentication:** Restoring a Multifactor Quorum-Authenticated Partition From Backup
> Restoring a Password-Authenticated Partition From Backup

Luna Backup HSM G5:

> Restoring an Application Partition from Backup

User Privileges

Users with the following privileges can perform this command:

> Admin
> Operator

Syntax

partition restore -partition <name> **-tokenpar** <name> **-serial** <serialnum> {**-add** | **-replace**} [**-password** <password>] [**-tokenpw** <password>] [**-force**]

Argument(s)	Shortcut	Description
-add	**-a**	Add objects to the application partition specified with **-partition**. Incremental backup (append). If the OUIDs of any source objects match OUIDs of objects already stored on the target backup, they are not restored, and the existing objects are not overwritten. You must specify either **-add** or **-replace**. **CAUTION!** If you are restoring a V1 backup to a V1 partition, use **-add** to restore the SMK and keep any existing objects on the partition. Use **-replace** only if you wish to erase any existing objects. By default, V1 backups only include the SMK.
-force	**-f**	Force the action without prompting.
-partition <name>	**-par**	Specifies the name of the target application partition to restore from backup. Obtain the partition name by using the **partition list** command.
-password <password>	**-pas**	The partition Crypto Officer's password. If you do not supply this value on the command line, you are prompted for it. Applies to password-authenticated HSMs only; multifactor quorum-authenticated HSMs will prompt for the partition Crypto Officer's black PED key.
-replace	**-r**	Erase all existing objects on the application partition and replace them with the contents of the backup. You must specify either **-add** or **-replace**. **CAUTION!** If you are restoring a V1 backup to a V1 partition, use **-add** to restore the SMK and keep any existing objects on the partition. Use **-replace** only if you wish to erase any existing objects. By default, V1 backups only include the SMK.
-serial <serialnum>	**-s**	Specifies the Luna Backup HSM serial number.
-tokenpar <name>	**-tokenpa**	Specifies the backup partition name.

Argument(s)	Shortcut	Description
-tokenpw <password>	**-tokenpw**	Specifies the backup partition's Crypto Officer password. If you do not supply this value on the command line, you are prompted for it. Applies to password-authenticated HSMs only; multifactor quorum-authenticated HSMs will prompt for the Crypto Officer's black PED key.

Example

```
lunash:>partition restore -partition sa78par1 -tokenpar sa78par1backup -serial 496771 -add


  Please enter the password for the token user partition:
  > ********

  Please enter the password for the HSM user partition:
  > ********

Object "MT RSA 4096-bit Private KeyGen" (handle 14) cloned to handle 46 on target
Object "MT RSA 4096-bit Public KeyGen" (handle 18) cloned to handle 49 on target
Object "MT RSA 4096-bit Private KeyGen" (handle 19) cloned to handle 52 on target
Object "MT RSA 4096-bit Public KeyGen" (handle 23) cloned to handle 48 on target
Object "MT RSA 4096-bit Private KeyGen" (handle 24) cloned to handle 57 on target
Object "MT RSA 4096-bit Public KeyGen" (handle 28) cloned to handle 70 on target
'partition restore' successful.


Command Result : 0 (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 Network HSM 7 appliance's internal HSM. It is not necessary to be logged in as HSM SO 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

User Privileges

Users with the following privileges can perform this command:

- Admin
- Operator
- Monitor

Syntax

partition show [**-partition** <partition_name>] [**-all**]

Argument(s)	Shortcut	Description
-partition <partitionname>	**-p**	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.
-all	**-a**	All partitions

Pre-firmware-7.7.0 Example

```
lunash:>partition show


   Partition Name:                          partition1
   Partition SN:                            154438865289
   Partition Label:                         testpartition
   Partition SO     PIN To Be Changed:      no
   Partition SO     Zeroized:               no
   Partition SO     Login Attempts Left:    10
```

```
   Crypto Officer   PIN To Be Changed:        no
   Crypto Officer   Locked Out:               no
   Crypto Officer   Login Attempts Left:      10
   Crypto User      PIN To Be Changed:        no
   Crypto User      Locked Out:               no
   Crypto User      Login Attempts Left:      10
   Legacy Domain Has Been Set:                no
   Partition Storage Information (Bytes):     Total=324096, Used=1232, Free=322864
   Partition Object Count:                    6


Command Result : 0 (Success)
```

Luna HSM Firmware 7.7.0 (and newer) V1 Partition Example

```
lunash:>partition show -partition v1par1


   Partition Name:                                  v1par1
   Partition SN:                              1238700701512
   Partition Label:
   Partition Version:                                   1
   Partition SO is not initialized.
   Crypto Officer is not initialized.
   Crypto User is not initialized.
   Limited Crypto Officer is not initialized.
   Legacy Domain Has Been Set:                         no
   Partition Storage Information (Bytes):
                Total=6628214
                Used=0
                Free=6628214
   Partition Object Count:                              0
   Partition SMK OUIDs:
               SMK-FW4: Not Initialized
               SMK-FW6: Not Initialized
               SMK-FW7-FM: Not Initialized
               SMK-FW7-Rollover: Not Initialized
               SMK-FW7-Primary: Not Initialized


Command Result : 0 (Success)
```

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

partition showContents

Using this command, the Crypto Officer can 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.

> **NOTE** This command requires Luna Network HSM 7 Appliance Software 7.8.1 or newer. It cannot be used on STC partitions; the Partition SO must use LunaCM at the client for partition management.

User Privileges

Users with the following privileges can perform this command:

- Admin
- Operator

Syntax

partition showContents -partition <partition_name> [**-cu**] **-password** <password>

Argument(s)	Shortcut	Description
-cu	**-c**	Perform task as Crypto-User. This option is required if you are using the Crypto-Officer/Crypto-User distinction.
-partition <name>	**-par**	Specifies the name of the partition for which contents are to be displayed. Obtain the partition name by using the **partition list** command.
-password <password>	**-pas**	The Crypto Officer password or partition challenge password.

Example

```
lunash:>partition showContents -partition myPartition



  Please enter the Crypto Officer's challenge:
  > ********

   Partition Name:                                myPartition
   Partition SN:                                 154438865353
   Partition Label:                               myPartition
   Partition Version:                                       0
   Storage (Bytes): Total=6628003, Used=16760, Free=6611243
   Number objects:  10

   Object Label:  MT RSA 4096-bit Private KeyGen
   Object Type:   Private Key
   Object Handle: 167
```

```
   Object Label:  MT RSA 4096-bit Public KeyGen
   Object Type:   Public Key
   Object Handle: 166

   Object Label:  MT RSA 4096-bit Private KeyGen
   Object Type:   Private Key
   Object Handle: 162

   Object Label:  MT RSA 4096-bit Public KeyGen
   Object Type:   Public Key
   Object Handle: 161

   Object Label:  MT RSA 4096-bit Private KeyGen
   Object Type:   Private Key
   Object Handle: 157

   Object Label:  MT RSA 4096-bit Public KeyGen
   Object Type:   Public Key
   Object Handle: 156

   Object Label:  MT RSA 4096-bit Private KeyGen
   Object Type:   Private Key
   Object Handle: 147

   Object Label:  MT RSA 4096-bit Public KeyGen
   Object Type:   Public Key
   Object Handle: 139

   Object Label:  MT RSA 4096-bit Private KeyGen
   Object Type:   Private Key
   Object Handle: 125

   Object Label:  MT RSA 4096-bit Public KeyGen
   Object Type:   Public Key
   Object Handle: 122


Command Result : 0 (Success)
```

partition showPolicies

Display the policy settings of the specified partition. This command displays the specified partition's policies and capabilities. See Partition Capabilities and Policies for more information.

> **NOTE** This command requires Luna Network HSM 7 Appliance Software 7.8.1 or newer. It cannot be used on STC partitions; the Partition SO must use LunaCM at the client for partition management.

Each policy's current setting is displayed. For modifiable policies, the policy code is displayed for use when changing policies.

User Privileges

Users with the following privileges can perform this command:

- Admin
- Operator

Syntax

partition showPolicies -partition <name> [**-configonly**] [**-verbose**]

Argument(s)	Shortcut	Description
-configonly	**-c**	List only the modifiable 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.
-verbose	**-v**	Display all partition policies, modifiable or not.

Example

```
lunash:>partition showPolicies -partition myPartition -verbose


   Partition Name:                                 myPartition
   Partition SN:                                 154438865353
   Partition Label:                                myPartition
   Partition Version:                                        0
   The following capabilities describe this partition and can
   never be changed.

   Description                              Value
   ===========                              =====
   Enable private key cloning               Allowed
   Enable private key wrapping              Allowed
   Enable private key unwrapping            Allowed
   Enable private key masking               Allowed
   Enable secret key cloning                Allowed
```

```
Enable secret key wrapping               Allowed
Enable secret key unwrapping             Allowed
Enable secret key masking                Allowed
Enable multipurpose keys                 Allowed
Enable changing key attributes           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) 247
Maximum pin length                       255
Enable Key Management Functions          Allowed
Enable RSA signing without confirmation  Allowed
Enable private key unmasking             Allowed
Enable secret key unmasking              Allowed
Enable RSA PKCS mechanism                Allowed
Enable CBC-PAD (un)wrap keys of any size Allowed
Enable private key SFF backup/restore    Disallowed
Enable secret key SFF backup/restore     Disallowed
Enable enforcing Secure Trusted Channel  Allowed
Enable Fast-Path                         Disallowed
Enable Start/End Date Attributes         Allowed
Enable Per-Key Authorization Data        Allowed
Enable Partition Version                 Allowed
Enable CPv1                              Allowed
Enable non-FIPS algorithms               Allowed
```

The following policies describe the current configuration
of this partition and may be changed by the Partition Security Officer.

Code	Description	Value	Destructive Off-To-On	Destructive On-To-Off
0	Allow private key cloning	On	Yes	No
1	Allow private key wrapping	Off	Yes	No
2	Allow private key unwrapping	On	No	No
3	Allow private key masking	Off	Yes	No
4	Allow secret key cloning	On	Yes	No
5	Allow secret key wrapping	On	Yes	No
6	Allow secret key unwrapping	On	No	No
7	Allow secret key masking	Off	Yes	No
10	Allow multipurpose keys	On	Yes	No
11	Allow changing key attributes	On	Yes	No
15	Ignore failed challenge responses	On	Yes	No
16	Operate without RSA blinding	On	Yes	No
17	Allow signing with non-local keys	On	No	No
18	Allow raw RSA operations	On	Yes	No
20	Max failed user logins allowed	10	N/A	N/A
21	Allow high availability recovery	On	No	No

```
  22  Allow activation                              On      No        No
  23  Allow auto-activation                         On      No        No
  25  Minimum pin length (inverted: 255 - min)      247     N/A       N/A
  26  Maximum pin length                            255     N/A       N/A
  28  Allow Key Management Functions                On      Yes       No
  29  Perform RSA signing without confirmation      On      Yes       No
  31  Allow private key unmasking                   Off     No        No
  32  Allow secret key unmasking                    Off     No        No
  33  Allow RSA PKCS mechanism                      On      Yes       No
  34  Allow CBC-PAD (un)wrap keys of any size       On      Yes       No
  37  Force Secure Trusted Channel                  Off     No        Yes
  39  Allow Start/End Date Attributes               Off     No        Yes
  40  Require Per-Key Authorization Data            Off     Yes       Yes
  41  Partition Version                              0      No        Yes
  42  Allow CPv1                                    On      Yes       No
  43  Allow non-FIPS algorithms                     On      Yes       No


Command Result : 0 (Success)
```

partition stcidentity

Export the STC partition identity, or display the hash for an STC partition.

> **NOTE** This command syntax applies to Luna Network HSM 7 Appliance Software 7.7.0 and newer only. For older versions, see **"stc partition" on page 515**.

You must be logged in as the HSM SO to use the **partition stcidentity** commands.

Syntax

partition stcidentity

export
show

Argument(s)	Shortcut	Description
export	**e**	Export the specified partition's public key to a file. See "partition stcIdentity export" on the next page.
show	**s**	Display the public key hash and serial number for the current partition. See "partition stcIdentity show" on page 464.

partition stcIdentity export

Export the specified partition's public key to a file. You must be logged in as HSM SO to use this command, and it can only be run on an uninitialized partition. Once the partition has been initialized, the public key can be exported by the Partition SO only, using LunaCM (see stcconfig partitionidexport).

> **NOTE** This command syntax applies to Luna Network HSM 7 Appliance Software 7.7.0 and newer only. For older versions, see **"stc partition" on page 515**.

User Privileges

Users with the following privileges can perform this command:

- Admin
- Operator

Syntax

partition stcIdentity export -partition <partition_name>

Argument(s)	Shortcut	Description
-partition <partition_name>	**-p**	Specifies the name of the partition whose public key you want to export.

Example

```
lunash:>partition stcIdentity export -partition partition2

Successfully exported partition identity for partition partition2 to file: 154438865290.pid

Command Result : 0 (Success)
```

partition stcIdentity show

Display the public key hash and serial number for the specified partition. You must be logged in as HSM SO to use this command, and it can only be run on an uninitialized partition. Once the partition has been initialized, this information is available only to the Partition SO using LunaCM (see stcconfig partitionidshow).

> **NOTE** This command syntax applies to Luna Network HSM 7 Appliance Software 7.7.0 and newer only. For older versions, see **"stc partition" on page 515**.

User Privileges

Users with the following privileges can perform this command:

- Admin
- Operator

Syntax

partition stcIdentity show -partition <partition_name>

Argument(s)	Shortcut	Description
-partition<partition_name>	**-p**	Specifies the name of the partition whose public key hash and serial number you want to display.

Example

```
lunash:>partition stcIdentity show -partition partition2

Partition Serial Number:                 154438865290
Partition Identity Public Key SHA1 Hash: 67a26c546f0bdd911375c833babcf702aa61e3ee


Command Result : 0 (Success)
```

service

Access commands that allow you to view or manage services.

Syntax

service

list
restart
start
status
stop

Argument(s)	Shortcut	Description
list	**l**	Display a list of the services. See "service list" on the next page.
restart	**r**	Restart a service. See "service restart" on page 467.
start	**star**	Start a service. See "service start" on page 469.
status	**stat**	Display the status for a service. See "service status" on page 470.
stop	**sto**	Stop a service. See "service stop" on page 471.

service list

Lists the services that the user can start, stop, restart, or for which the user can request status information.

User Privileges

Users with the following privileges can perform this command:

- Admin
- Operator
- Monitor

Syntax

service list

Example

```
lunash:>service list

   The following are valid luna SA service names:
      cbs           - HSM callback service
      lsta          - Luna SNMP trap agent service
      network       - Network service (Needed for ntls, ssh and sftp)
      ntls          - Network trust link service
      ntp           - Network time protocol service
      snmp          - SNMP agent service
      ssh           - Secure shell service (Needed for ssh and scp/sftp)
      stc           - Secure trusted channel service
      syslog        - Syslog service
      sysstat       - System status monitoring (controls LCD)
      webserver     - REST API service
      pedserver     - Remote PED service
      cluster       - Cluster service
      clusteradmin  - Cluster Administration service
      ctc           - Crypto traffic controller

Command Result : 0 (Success)
```

service restart

Restart a service on the Luna Network HSM 7 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 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.
>
> **service restart network** also restarts the CTC service if it was running.
>
> **service restart sysstat** also restarts the Front-panel LCD Display.

User Privileges

Users with the following privileges can perform this command:

- Admin
- Operator

Syntax

service restart <service_name> [**-force**]

Argument(s)	Shortcut	Description
<service_name>		Specifies the service to restart. **Valid values:** cbs, cluster, clusteradmin, ctc, lsta, network, ntls, ntp, pedserver, snmp, ssh, stc, syslog, sysstat, webserver
-force	**-f**	Force the action without prompting.

Example

```
lunash:>service restart syslog

Stopping syslog:                                           [  OK  ]

Starting syslog:                                           [  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 Network HSM
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)
```

service start

Start a named service on the Luna Network HSM 7 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.

User Privileges

Users with the following privileges can perform this command:

- Admin
- Operator

Syntax

service start <service_name>

Argument(s)	Shortcut	Description
<service_name>		Specifies the service to start. **Valid values:** cbs, cluster, clusteradmin, ctc, lsta, network, ntls, ntp, pedserver, snmp, ssh, stc, syslog, sysstat, webserver
-force	**-f**	Applies to the **cluster** service only. Including this option will force the cluster service to start, regardless of whether other members of the cluster can be reached. Use only with the guidance of a Thales Support Engineer.

Example

```
lunash:>service start syslog

Starting syslog:                                           [  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 NTLS, 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.

User Privileges

Users with the following privileges can perform this command:

- Admin
- Operator
- Monitor

Syntax

service status <service_name>

Argument(s)	Description
<service_name>	Specifies the service for which you want to display the status. **Valid values:** cbs, cluster, clusteradmin, ctc, lsta, network, ntls, ntp, pedserver, snmp, ssh, stc, syslog, sysstat, webserver

Example

```
lunash:>service status network

   eth0 is up
   eth1 is down
   eth2 is down
   eth3 is down
   bond0 is down
   bond1 is down

Command Result : 0 (Success)
```

Example

```
lunash:>service status ctc
service status ctc

  ctc@eth0 is inactive
  ctc@eth1 is inactive
  All interfaces are down


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 Network HSM, 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.

> **NOTE** Issuing **service stop network** stops the network service. Stopping the network service stops all network traffic (SSH, NTLS, etc.), and any network commands issued thereafter will fail. If the CTC service was running, it also stops. You can start the network service using the **service start network** command from a serial port connection or by rebooting the appliance using the **sysconf appliance reboot** command.

User Privileges

Users with the following privileges can perform this command:

- Admin
- Operator

Syntax

service stop <servicename>

Argument(s)	Shortcut	Description
<service_name>		Specifies the service to stop. **Valid values:** cbs, cluster, clusteradmin, ctc, lsta, network, ntls, ntp, pedserver, snmp, ssh, stc, syslog, sysstat, webserver
-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
handles
mac
mem
memmap
netstat
ps
sensors
sysstat
time
zone

Argument(s)	Shortcut	Description
cpu	**c**	Display the current CPU load. See "status cpu" on page 474.
date	**da**	Display the current date and time. See "status date" on page 475.
disk	**di**	Display the current disk usage. See "status disk" on page 476.
handles	**h**	Display the open handle count for each process. See "status handles" on page 478.
interface	**i**	Display the current network interface information. See "status interface" on page 480.
mac	**ma**	Display the current MAC address configuration. See "status mac" on page 481.
mem	**me**	Display the current memory usage. See "status mem" on page 482.
memmap	**memm**	Display the Process Memory Map. See "status memmap" on page 483.

Argument(s)	Shortcut	Description
netstat	**n**	Display the current network connections. See "status netstat" on page 485.
ps	**ps**	Display the current status of processes. See "status ps" on page 491.
sensors	**se**	Display the sensors output. See "status sensors" on page 493.
sysstat	**sy**	Display system status monitor information. See "status sysstat" on page 496.
time	**t**	Display the current time. See "status time" on page 500.
zone	**z**	Display the current time zone. See "status zone" on page 501.

status cpu

Display the current CPU load. The CPU load average is an indication of processor queue size and is presented as a series of five entries, as follows:

1. The average CPU load for the previous minute. This value is 0.30 in the example below.
2. The average CPU load for the previous five minutes. This value is 0.22 in the example below.
3. The average CPU load for the previous ten minutes. This value is 0.18 in the example below.
4. The number of currently running processes and the total number of processes. The example below shows 2 of 325 processes running.
5. The last process ID used. This value is 27794 in the example below.

Without knowledge of the entire workload and type, this status information is an approximation, and useful only if an audit agency specifically asks for it. There is no action to take.

User Privileges

Users with the following privileges can perform this command:

> Admin

> Operator

> Monitor

Syntax

status cpu

Example

```
lunash:>status cpu

CPU Load Averages:
0.30 0.22 0.18 2/365 27794

System uptime:
At Wed Mar  1 09:24:11 EST 2017, I am up 17:24

Command Result : 0 (Success)
```

status date

Display the current date and time.

User Privileges

Users with the following privileges can perform this command:

- Admin
- Operator
- Monitor

Syntax

status date

Example

```
lunash:>status date

Wed Mar  1 09:27:45 EST 2017

Command Result : 0 (Success)
```

status disk

Display the current disk usage information from the SMART monitoring service.

User Privileges

Users with the following privileges can perform this command:

- Admin
- Operator
- Monitor

Syntax

status disk

Example

```
lunash:>status disk


===================== Hard Disk utilization =====================
Filesystem     1K-blocks    Used Available Use% Mounted on
/dev/sda5        8125880  108244   7581824   2% /
/dev/sda8       41153760 1159100  37881124   3% /usr
/dev/sda6        1998672   80204   1797228   5% /boot
/dev/sda12      57667680   53540  54661744   1% /home
/dev/sda9        3997376   86724   3684556   3% /var
/dev/sda7        3997376  118996   3652284   4% /tmp
/dev/sda10       1998672    6144   1871288   1% /var/tmp
/dev/sda13     231063860   61476 219241952   1% /var/audit
/dev/sda11      10190100   38916   9610512   1% /var/log
/dev/sda14      10190100   39160   9610268   1% /var/log/audit

===================== Hard Disk SMART Report =====================

=== START OF INFORMATION SECTION ===
Device Model:     HGST HUS726020ALE611
Serial Number:    N4G55WPS
LU WWN Device Id: 5 000cca 245c25bfa
Firmware Version: APGNV7J0
Copyright (C) 2002-13, Bruce Allen, Christian Franke, www.smartmontools.org

=== 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     0x000b   100   100   016    Pre-fail  Always       -       0
  2 Throughput_Performance  0x0005   136   136   054    Pre-fail  Offline      -       108
  3 Spin_Up_Time            0x0007   131   131   024    Pre-fail  Always       -       227
(Average 228)
  4 Start_Stop_Count        0x0012   100   100   000    Old_age   Always       -       14
```

```
  5 Reallocated_Sector_Ct   0x0033   100   100   005    Pre-fail  Always       -       0
  7 Seek_Error_Rate         0x000b   100   100   067    Pre-fail  Always       -       0
  8 Seek_Time_Performance   0x0005   128   128   020    Pre-fail  Offline      -       18
  9 Power_On_Hours          0x0012   100   100   000    Old_age   Always       -       4385
 10 Spin_Retry_Count        0x0013   100   100   060    Pre-fail  Always       -       0
 12 Power_Cycle_Count       0x0032   100   100   000    Old_age   Always       -       14
192 Power-Off_Retract_Count 0x0032   100   100   000    Old_age   Always       -       185
193 Load_Cycle_Count        0x0012   100   100   000    Old_age   Always       -       185
194 Temperature_Celsius     0x0002   206   206   000    Old_age   Always       -       29
(Min/Max 23/35)
196 Reallocated_Event_Count 0x0032   100   100   000    Old_age   Always       -       0
197 Current_Pending_Sector  0x0022   100   100   000    Old_age   Always       -       0
198 Offline_Uncorrectable   0x0008   100   100   000    Old_age   Offline      -       0
199 UDMA_CRC_Error_Count    0x000a   200   200   000    Old_age   Always       -       0

SMART Error Log Version: 1
No Errors Logged


Command Result : 0 (Success)
```

status handles

Gets the open handle count for each process.

User Privileges

Users with the following privileges can perform this command:

- Admin
- Operator
- Monitor

Syntax

status handles

Example

```
lunash:>status handles

 HANDLES    PID  CMD
      55      1  /usr/lib/systemd/systemd
       4      2  [kthreadd]
       4      3  [ksoftirqd/0]
       4      5  [kworker/0:0H]
       4      7  [migration/0]
       4      8  [rcu_bh]
       4      9  [rcuob/0]
       4     10  [rcuob/1]
       4     11  [rcuob/2]
       4     12  [rcuob/3]
       4     13  [rcuob/4]
       4     14  [rcuob/5]
       4     15  [rcuob/6]
       4     16  [rcuob/7]

...(clip)...

      22   2417  /usr/lunasa/bin/pedClient
      29   2426  /usr/lunasa/vts/stcd_vtsd
       4   9587  [kworker/3:1]
       4  11108  [kworker/u16:2]
       0  11666  sleep
      16  11667  /bin/bash
       4  12764  [kworker/3:0]
      15  14383  /bin/bash
      33  14400  /usr/lunasa/vts/ntls_vtsd
       4  15853  [kworker/1:1]
      73  18956  sshd:
      15  18988  -lush
       4  19861  [kworker/u16:1]
       4  23551  [kworker/2:0]
       4  23655  [kworker/3:3]
       4  25593  [kworker/3:4]
       4  29384  [kworker/0:1]
```

```
       4  30314  [kworker/1:2]
      44  32204  /usr/sbin/rsyslogd
       4  32442  [kworker/u16:0]

    1557  Total handles allocated.


Command Result : 0 (Success)
```

status interface

Display network interface information.

User Privileges

Users with the following privileges can perform this command:

- Admin
- Operator
- Monitor

Syntax

status interface

Example

```
lunash:>status interface

1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq state UP qlen 1000
    link/ether 00:15:b2:a9:b7:84 brd ff:ff:ff:ff:ff:ff
    inet 192.20.11.78/24 brd 192.20.11.255 scope global dynamic eth0
       valid_lft 107785sec preferred_lft 107785sec
3: eth1: <NO-CARRIER,BROADCAST,MULTICAST,UP> mtu 1500 qdisc mq state DOWN qlen 1000
    link/ether 00:15:b2:a9:b7:85 brd ff:ff:ff:ff:ff:ff
4: eth2: <NO-CARRIER,BROADCAST,MULTICAST,UP> mtu 1500 qdisc mq state DOWN qlen 1000
    link/ether 00:15:b2:a9:b7:86 brd ff:ff:ff:ff:ff:ff
5: eth3: <NO-CARRIER,BROADCAST,MULTICAST,UP> mtu 1500 qdisc mq state DOWN qlen 1000
    link/ether 00:15:b2:a9:b7:87 brd ff:ff:ff:ff:ff:ff

Command Result : 0 (Success)
```

status mac

Display the network interface MAC addresses.

User Privileges

Users with the following privileges can perform this command:

- Admin
- Operator
- Monitor

Syntax

status mac

Example

```
lunash:>status mac

eth0 00:15:b2:a9:b7:84
eth1 00:15:b2:a9:b7:85
eth2 00:15:b2:a9:b7:86
eth3 00:15:b2:a9:b7:87

Command Result : 0 (Success)
```

status mem

Display the current memory usage.

User Privileges

Users with the following privileges can perform this command:

- Admin
- Operator
- Monitor

Syntax

status mem

Example

```
lunash:>status mem

              total        used        free      shared  buff/cache   available
Mem:        3958580      169292     3303072       17120      486216     3558836
Swap:       4064252           0     4064252

Command Result : 0 (Success)
```

status memmap

Display the current memory usage.

User Privileges

Users with the following privileges can perform this command:

- Admin
- Operator
- Monitor

Syntax

status memmap

Example

```
lunash:>status memmap

   PID CMD                                  MAPPED(K)  WR/PR(K) SHARED(K)
     1 /usr/lib/systemd/systemd                 45092      5176         0
     2 [kthreadd]                                   0         0         0
     3 [ksoftirqd/0]                                0         0         0
     5 [kworker/0:0H]                               0         0         0
     7 [migration/0]                                0         0         0
     8 [rcu_bh]                                     0         0         0
     9 [rcuob/0]                                    0         0         0
    10 [rcuob/1]                                    0         0         0
    11 [rcuob/2]                                    0         0         0
    12 [rcuob/3]                                    0         0         0

 ...(clip)...

  2417 /usr/lunasa/bin/pedClient               390372     43500        16
  2426 /usr/lunasa/vts/stcd_vtsd               782544    558944        24
  3555 [kworker/u16:2]                              0         0         0
 11442 [kworker/1:2]                                0         0         0
 12764 [kworker/3:0]                                0         0         0
 14383 /bin/bash                              115380       548        28
 14400 /usr/lunasa/vts/ntls_vtsd             1012848    592120        40
 14555 [kworker/u16:1]                              0         0         0
 16198 sshd:                                  125332      1172      2560
 16693 -lush                                   12932       660         0
 18956 sshd:                                  125332      1172      2560
 18988 -lush                                   12932       660         0
 19305 [kworker/3:1]                                0         0         0
 23551 [kworker/2:0]                                0         0         0
 23823 [kworker/u16:0]                              0         0         0
 24051 sleep                                        0         0         0
 24052 /bin/bash                                 9516       388         0
 25512 [kworker/1:0]                                0         0         0
 25593 [kworker/3:4]                                0         0         0
 29384 [kworker/0:1]                                0         0         0
```

```
 32204 /usr/sbin/rsyslogd                      299876     25772     16384

Command Result : 0 (Success)
```

status netstat

Display the current network connections

User Privileges

Users with the following privileges can perform this command:

- Admin
- Operator
- Monitor

Syntax

status netstat

Luna Appliance Software 7.8.5 and Newer Example

```
lunash:>status netstat


Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program
name
tcp        0      0 0.0.0.0:8443            0.0.0.0:*               LISTEN      2151/nginx:
master
tcp        0      0 127.0.0.1:443           0.0.0.0:*               LISTEN      1460/./websrv

tcp        0      0 127.0.0.1:1501          0.0.0.0:*               LISTEN      2268/pedClient

tcp        0      0 127.0.0.1:1502          0.0.0.0:*               LISTEN      1396/PedServer

tcp        0      0 127.0.0.1:1503          0.0.0.0:*               LISTEN      1396/PedServer

tcp        0      0 0.0.0.0:1792            0.0.0.0:*               LISTEN      2200/ntls_vtsd

tcp        0      0 0.0.0.0:9697            0.0.0.0:*               LISTEN      2268/pedClient

tcp        0      0 127.0.0.1:199           0.0.0.0:*               LISTEN      1291/snmpd

tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN      2260/sshd

tcp        0      0 0.0.0.0:5656            0.0.0.0:*               LISTEN      2250/stcd_vtsd

tcp        0      0 10.124.139.214:38480    10.124.139.170:514      ESTABLISHED 1300/rsyslogd

tcp        0      0 10.124.139.214:22       10.124.93.174:47036     ESTABLISHED 4835/sshd:
root@pts
tcp        0      0 10.124.139.214:38486    10.124.139.170:514      ESTABLISHED 1300/rsyslogd

tcp        0      0 10.124.139.214:38482    10.124.139.170:514      ESTABLISHED 1300/rsyslogd

tcp        0      0 10.124.139.214:38484    10.124.139.170:514      ESTABLISHED 1300/rsyslogd

tcp6       0      0 :::22                   :::*                    LISTEN      2260/sshd
```

```
udp        0      0 0.0.0.0:68              0.0.0.0:*                           1236/dhclient

udp        0      0 0.0.0.0:161             0.0.0.0:*                           1291/snmpd

udp        0      0 127.0.0.1:514           0.0.0.0:*                           1300/rsyslogd

Active UNIX domain sockets (servers and established)
Proto RefCnt Flags       Type       State         I-Node   PID/Program name     Path
unix  2      [ ACC ]     STREAM     LISTENING     21509    1/systemd
/run/dbus/system_bus_socket
unix  2      [ ACC ]     STREAM     LISTENING     21512    1/systemd
/run/docker.sock
unix  2      [ ACC ]     STREAM     LISTENING     28450    1291/snmpd
/var/agentx/master
unix  2      [ ACC ]     STREAM     LISTENING     31798    1317/dockerd
/var/run/docker/metrics.sock
unix  2      [ ACC ]     STREAM     LISTENING     11335    1/systemd
/run/systemd/private
unix  2      [ ACC ]     SEQPACKET  LISTENING     8782     1/systemd
/run/udev/control
unix  2      [ ACC ]     STREAM     LISTENING     26447    1149/containerd
/run/containerd/containerd.sock.ttrpc
unix  2      [ ACC ]     STREAM     LISTENING     26451    1149/containerd
/run/containerd/containerd.sock
unix  2      [ ACC ]     STREAM     LISTENING     26466    961/NetworkManager
/var/run/NetworkManager/private-dhcp
unix  3      [ ]         DGRAM                    1403     1/systemd
/run/systemd/notify
unix  2      [ ]         DGRAM                    1405     1/systemd
/run/systemd/cgroups-agent
unix  2      [ ACC ]     STREAM     LISTENING     1419     1/systemd
/run/systemd/journal/stdout
unix  5      [ ]         DGRAM                    1422     1/systemd
/run/systemd/journal/socket
unix  19     [ ]         DGRAM                    1424     1/systemd            /dev/log
unix  2      [ ]         DGRAM                    12695    1/systemd
/run/systemd/shutdownd
unix  2      [ ACC ]     STREAM     LISTENING     28575    1317/dockerd
/var/run/docker/libnetwork/79787aad65dc.sock
unix  2      [ ACC ]     STREAM     LISTENING     32244    2127/containerd-shi
/run/containerd/s/0ec98232930540a072c3790274944abd27f2148251080edd76e69202d2be9f8a
unix  3      [ ]         STREAM     CONNECTED     23795    1/systemd
/run/systemd/journal/stdout
unix  3      [ ]         STREAM     CONNECTED     26954    1291/snmpd
unix  3      [ ]         STREAM     CONNECTED     32502    1/systemd
/run/systemd/journal/stdout
unix  3      [ ]         STREAM     CONNECTED     19158    1/systemd
/run/systemd/journal/stdout
unix  3      [ ]         STREAM     CONNECTED     22550    656/systemd-logind
unix  2      [ ]         DGRAM                    27435    1460/./websrv
unix  3      [ ]         STREAM     CONNECTED     35436    2254/luna-snmp
unix  2      [ ]         DGRAM                    27514    1300/rsyslogd
unix  2      [ ]         DGRAM                    21252    657/dbus-daemon
unix  3      [ ]         STREAM     CONNECTED     19156    1/systemd
/run/systemd/journal/stdout
unix  3      [ ]         STREAM     CONNECTED     26195    657/dbus-daemon
/run/dbus/system_bus_socket
```

```
unix  2      [ ]         DGRAM                    26469    1236/dhclient
unix  3      [ ]         STREAM     CONNECTED     22785    676/lcdController
unix  2      [ ]         DGRAM                    12270    436/systemd-udevd
unix  3      [ ]         STREAM     CONNECTED     21248    657/dbus-daemon
unix  3      [ ]         STREAM     CONNECTED     21095    626/auditd
unix  2      [ ]         DGRAM                    33392    2268/pedClient
unix  2      [ ]         DGRAM                    33391    2254/luna-snmp
unix  2      [ ]         DGRAM                    24810    683/crond
unix  3      [ ]         STREAM     CONNECTED     21094    626/auditd
unix  2      [ ]         DGRAM                    25063    961/NetworkManager
unix  3      [ ]         STREAM     CONNECTED     32606    2250/stcd_vtsd
unix  2      [ ]         DGRAM                    9639     397/systemd-journal
unix  3      [ ]         STREAM     CONNECTED     23219    666/polkitd
unix  3      [ ]         STREAM     CONNECTED     22253    1/systemd
unix  2      [ ]         DGRAM                    34893    2250/stcd_vtsd
unix  3      [ ]         STREAM     CONNECTED     23277    1/systemd
/run/systemd/journal/stdout
unix  3      [ ]         STREAM     CONNECTED     29866    1/systemd
/run/systemd/journal/stdout
unix  3      [ ]         STREAM     CONNECTED     33279    1/systemd
/run/systemd/journal/stdout
unix  3      [ ]         STREAM     CONNECTED     26457    657/dbus-daemon
/run/dbus/system_bus_socket
unix  2      [ ]         DGRAM                    24627    676/lcdController
unix  3      [ ]         STREAM     CONNECTED     25525    1/systemd
/run/systemd/journal/stdout
unix  3      [ ]         STREAM     CONNECTED     30761    1149/containerd
/run/containerd/containerd.sock
unix  3      [ ]         STREAM     CONNECTED     30252    1317/dockerd
unix  3      [ ]         STREAM     CONNECTED     34862    2254/luna-snmp
unix  3      [ ]         STREAM     CONNECTED     30590    2127/containerd-shi
/run/containerd/s/0ec98232930540a072c3790274944abd27f2148251080edd76e69202d2be9f8a
unix  3      [ ]         STREAM     CONNECTED     26752    1129/python2
unix  3      [ ]         STREAM     CONNECTED     34594    1/systemd
/run/systemd/journal/stdout
unix  2      [ ]         DGRAM                    56405    4835/sshd: root@pts
unix  3      [ ]         STREAM     CONNECTED     25524    1149/containerd
unix  3      [ ]         DGRAM                    12283    436/systemd-udevd
unix  3      [ ]         STREAM     CONNECTED     23145    1/systemd
/run/systemd/journal/stdout
unix  3      [ ]         STREAM     CONNECTED     21247    657/dbus-daemon
unix  3      [ ]         STREAM     CONNECTED     36820    1291/snmpd
/var/agentx/master
unix  3      [ ]         STREAM     CONNECTED     32965    1149/containerd
unix  3      [ ]         STREAM     CONNECTED     27190    1317/dockerd
unix  2      [ ]         DGRAM                    13295    1/systemd
unix  3      [ ]         DGRAM                    12282    436/systemd-udevd
unix  3      [ ]         STREAM     CONNECTED     30612    2127/containerd-shi
unix  3      [ ]         STREAM     CONNECTED     34891    1/systemd
/run/systemd/journal/stdout
unix  3      [ ]         STREAM     CONNECTED     34593    2260/sshd
unix  3      [ ]         STREAM     CONNECTED     30759    1149/containerd
/run/containerd/containerd.sock
unix  3      [ ]         STREAM     CONNECTED     21249    657/dbus-daemon
/run/dbus/system_bus_socket
unix  3      [ ]         STREAM     CONNECTED     30698    2200/ntls_vtsd
unix  3      [ ]         STREAM     CONNECTED     33161    2151/nginx: master
unix  3      [ ]         STREAM     CONNECTED     33062    1149/containerd
```

```
/run/containerd/containerd.sock.ttrpc
unix  3      [ ]         STREAM     CONNECTED     26194    961/NetworkManager
unix  2      [ ]         DGRAM                    34260    2200/ntls_vtsd
unix  3      [ ]         STREAM     CONNECTED     25055    657/dbus-daemon
/run/dbus/system_bus_socket
unix  3      [ ]         STREAM     CONNECTED     24144    961/NetworkManager
unix  3      [ ]         STREAM     CONNECTED     13730    1/systemd
/run/systemd/journal/stdout
unix  2      [ ]         DGRAM                    22254    656/systemd-logind
unix  2      [ ]         DGRAM                    28448    1291/snmpd
unix  3      [ ]         STREAM     CONNECTED     26371    657/dbus-daemon
/run/dbus/system_bus_socket
unix  3      [ ]         STREAM     CONNECTED     24361    961/NetworkManager
unix  3      [ ]         STREAM     CONNECTED     22592    657/dbus-daemon
unix  3      [ ]         STREAM     CONNECTED     12268    436/systemd-udevd
unix  2      [ ]         DGRAM                    25957    691/sysstatd
unix  3      [ ]         STREAM     CONNECTED     22786    1/systemd
/run/systemd/journal/stdout
unix  3      [ ]         STREAM     CONNECTED     26567    1/systemd
/run/systemd/journal/stdout
unix  3      [ ]         STREAM     CONNECTED     26760    1/systemd
/run/systemd/journal/stdout
unix  2      [ ]         DGRAM                    25057    666/polkitd
unix  3      [ ]         STREAM     CONNECTED     19140    1/systemd
/run/systemd/journal/stdout
unix  2      [ ]         DGRAM                    21093    626/auditd
unix  3      [ ]         STREAM     CONNECTED     24747    683/crond
unix  2      [ ]         DGRAM                    22599    660/ipmievd
unix  3      [ ]         STREAM     CONNECTED     21250    657/dbus-daemon
/run/dbus/system_bus_socket
unix  3      [ ]         STREAM     CONNECTED     18236    649/irqbalance
unix  3      [ ]         STREAM     CONNECTED     25144    1129/python2
unix  3      [ ]         STREAM     CONNECTED     21238    656/systemd-logind
unix  3      [ ]         STREAM     CONNECTED     24496    1153/bash
unix  3      [ ]         STREAM     CONNECTED     28507    1317/dockerd
unix  3      [ ]         STREAM     CONNECTED     33160    2151/nginx: master

Command Result : 0 (Success)
```

Luna Appliance Software 7.8.4 and Older Example

```
lunash:>status netstat

Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 0.0.0.0:8443            0.0.0.0:*               LISTEN
tcp        0      0 127.0.0.1:443           0.0.0.0:*               LISTEN
tcp        0      0 127.0.0.1:1501          0.0.0.0:*               LISTEN
tcp        0      0 127.0.0.1:1502          0.0.0.0:*               LISTEN
tcp        0      0 127.0.0.1:1503          0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:1792            0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:9697            0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:5656            0.0.0.0:*               LISTEN
tcp        0    320 10.124.143.156:22       10.105.187.172:63240    ESTABLISHED
tcp6       0      0 :::22                   :::*                    LISTEN
udp        0      0 0.0.0.0:68              0.0.0.0:*
udp        0      0 127.0.0.1:514           0.0.0.0:*
```

```
Active UNIX domain sockets (servers and established)
Proto RefCnt Flags       Type       State         I-Node   Path
unix  2      [ ACC ]     STREAM     LISTENING     9733     /run/systemd/private
unix  2      [ ACC ]     STREAM     LISTENING     23046    /run/dbus/system_bus_socket
unix  2      [ ACC ]     STREAM     LISTENING     23049    /run/docker.sock
unix  2      [ ACC ]     SEQPACKET  LISTENING     13853    /run/udev/control
unix  2      [ ]         DGRAM                    13855    /run/systemd/shutdownd
unix  3      [ ]         DGRAM                    1603     /run/systemd/notify
unix  2      [ ]         DGRAM                    1605     /run/systemd/cgroups-agent
unix  2      [ ACC ]     STREAM     LISTENING     1623     /run/systemd/journal/stdout
unix  5      [ ]         DGRAM                    1626     /run/systemd/journal/socket
unix  18     [ ]         DGRAM                    1628     /dev/log
unix  2      [ ACC ]     STREAM     LISTENING     30328
/var/run/docker/libnetwork/8115501f92e0.sock
unix  2      [ ACC ]     STREAM     LISTENING     29310
/run/containerd/s/66d65a708f91ff34101944436d238dec94bb85dd72a75d0a77dfa958476fd088
unix  2      [ ACC ]     STREAM     LISTENING     25989
/run/containerd/containerd.sock.ttrpc
unix  2      [ ACC ]     STREAM     LISTENING     25993    /run/containerd/containerd.sock
unix  2      [ ACC ]     STREAM     LISTENING     29103    /var/run/NetworkManager/private-dhcp
unix  2      [ ACC ]     STREAM     LISTENING     29168    /var/run/docker/metrics.sock
unix  2      [ ]         DGRAM                    24353
unix  3      [ ]         STREAM     CONNECTED     27451
unix  2      [ ]         DGRAM                    12308
unix  3      [ ]         STREAM     CONNECTED     25770    /run/dbus/system_bus_socket
unix  2      [ ]         DGRAM                    24362
unix  3      [ ]         STREAM     CONNECTED     31871
/run/containerd/containerd.sock.ttrpc
unix  3      [ ]         STREAM     CONNECTED     12734
unix  3      [ ]         STREAM     CONNECTED     25771    /run/systemd/journal/stdout
unix  3      [ ]         STREAM     CONNECTED     28039    /run/systemd/journal/stdout
unix  3      [ ]         STREAM     CONNECTED     28026
unix  3      [ ]         STREAM     CONNECTED     33481
unix  3      [ ]         STREAM     CONNECTED     25235
unix  2      [ ]         DGRAM                    22434
unix  3      [ ]         STREAM     CONNECTED     30253    /run/containerd/containerd.sock
unix  2      [ ]         DGRAM                    470667356
unix  3      [ ]         STREAM     CONNECTED     22298
unix  3      [ ]         STREAM     CONNECTED     27886
unix  2      [ ]         DGRAM                    34681
unix  3      [ ]         STREAM     CONNECTED     27452    /run/dbus/system_bus_socket
unix  3      [ ]         STREAM     CONNECTED     20631
unix  3      [ ]         STREAM     CONNECTED     34468    /run/systemd/journal/stdout
unix  2      [ ]         DGRAM                    22433
unix  2      [ ]         DGRAM                    22285
unix  2      [ ]         DGRAM                    279585
unix  2      [ ]         DGRAM                    15911
unix  3      [ ]         STREAM     CONNECTED     20632
unix  2      [ ]         DGRAM                    20630
unix  3      [ ]         STREAM     CONNECTED     20965    /run/systemd/journal/stdout
unix  3      [ ]         STREAM     CONNECTED     22273
unix  3      [ ]         STREAM     CONNECTED     21290
unix  3      [ ]         STREAM     CONNECTED     22300    /run/dbus/system_bus_socket
unix  3      [ ]         STREAM     CONNECTED     28344    /run/containerd/containerd.sock
unix  2      [ ]         DGRAM                    470666541
unix  3      [ ]         STREAM     CONNECTED     21190
unix  3      [ ]         STREAM     CONNECTED     22299
unix  3      [ ]         STREAM     CONNECTED     8966     /run/systemd/journal/stdout
```

```
unix  3      [ ]         DGRAM                    12747
unix  2      [ ]         DGRAM                    14773
unix  3      [ ]         STREAM     CONNECTED     23768    /run/systemd/journal/stdout
unix  3      [ ]         STREAM     CONNECTED     29676
unix  2      [ ]         DGRAM                    28190
unix  2      [ ]         DGRAM                    23814
unix  2      [ ]         DGRAM                    23771
unix  3      [ ]         STREAM     CONNECTED     28346
unix  3      [ ]         DGRAM                    12746
unix  3      [ ]         STREAM     CONNECTED     22370
unix  3      [ ]         STREAM     CONNECTED     22056
unix  2      [ ]         DGRAM                    35370
unix  2      [ ]         DGRAM                    22303
unix  3      [ ]         STREAM     CONNECTED     23781
unix  3      [ ]         STREAM     CONNECTED     30252
unix  3      [ ]         STREAM     CONNECTED     32628    /run/systemd/journal/stdout
unix  3      [ ]         STREAM     CONNECTED     32627
unix  3      [ ]         STREAM     CONNECTED     25688    /run/systemd/journal/stdout
unix  3      [ ]         STREAM     CONNECTED     22306    /run/systemd/journal/stdout
unix  3      [ ]         STREAM     CONNECTED     29677
unix  3      [ ]         STREAM     CONNECTED     23764    /run/systemd/journal/stdout
unix  3      [ ]         STREAM     CONNECTED     23744    /run/systemd/journal/stdout
unix  3      [ ]         STREAM     CONNECTED     25301
unix  3      [ ]         STREAM     CONNECTED     22301    /run/dbus/system_bus_socket
unix  3      [ ]         STREAM     CONNECTED     31851
unix  3      [ ]         STREAM     CONNECTED     34679    /run/systemd/journal/stdout
unix  2      [ ]         DGRAM                    32634
unix  3      [ ]         STREAM     CONNECTED     25681
unix  3      [ ]         STREAM     CONNECTED     21349    /run/systemd/journal/stdout
unix  3      [ ]         STREAM     CONNECTED     21112
unix  2      [ ]         DGRAM                    31524
unix  3      [ ]         STREAM     CONNECTED     33597
unix  3      [ ]         STREAM     CONNECTED     27600    /run/systemd/journal/stdout
unix  3      [ ]         STREAM     CONNECTED     31855
/run/containerd/s/66d65a708f91ff34101944436d238dec94bb85dd72a75d0a77dfa958476fd088
unix  3      [ ]         STREAM     CONNECTED     22493    /run/dbus/system_bus_socket
unix  3      [ ]         STREAM     CONNECTED     28914
unix  3      [ ]         STREAM     CONNECTED     27546    /run/dbus/system_bus_socket
unix  3      [ ]         STREAM     CONNECTED     25986
unix  3      [ ]         STREAM     CONNECTED     29654
unix  3      [ ]         STREAM     CONNECTED     20775

Command Result : 0 (Success)
```

status ps

Display the status of the appliance processes.

User Privileges

Users with the following privileges can perform this command:

- Admin
- Operator
- Monitor

Syntax

status ps

Example

```
lunash:>status ps


COMMAND          %CPU  %MEM     VSZ   RSS TTY   START TIME
systemd           0.4   0.2   44344  8256 ?     Dec03 00:53:32
kthreadd          0.0   0.0       0     0 ?     Dec03 00:00:00
systemd-journal   0.0   0.2   36828  9452 ?     Dec03 00:02:07
systemd-udevd     0.0   0.0   42396  3468 ?     Dec03 00:00:00
auditd            0.0   0.0  116732  3200 ?     Dec03 00:00:08
lcdController     0.6   0.1  108164  3960 ?     Dec03 01:12:51
rsyslogd          0.0   0.5  422764 21956 ?     Dec03 00:02:13
systemd-logind    0.0   0.0   27404  3936 ?     Dec03 00:00:32
smartd            0.0   0.0   26528  3876 ?     Dec03 00:00:00
irqbalance        0.0   0.0   19308  2596 ?     Dec03 00:01:30
dbus-daemon       0.0   0.0   26740  2740 ?     Dec03 00:01:12
NetworkManager    0.0   0.3  438068 12904 ?     Dec03 00:04:21
crond             0.0   0.0  126340  3112 ?     Dec03 00:00:04
ipmievd           0.0   0.0   23204  2128 ?     Dec03 00:00:06
ntpd              0.0   0.1   97944  4776 ?     Dec03 00:00:48
sysstatd          0.0   0.0   14824  2640 ?     Dec03 00:01:26
polkitd           0.0   0.4  527576 16716 ?     Dec03 00:00:26
dhclient          0.0   0.4  111024 19472 ?     Dec03 00:00:00
luna-snmp         0.2   0.3  255692 12120 ?     Dec03 00:33:04
tuned             0.0   0.5  553584 23040 ?     Dec03 00:01:12
oamp              0.6   0.0   18968  1684 ?     Dec03 01:18:46
snmpd             0.1   0.3  223824 15516 ?     Dec03 00:16:34
monitor_DSR.sh    0.3   0.0  115764  3472 ?     Dec03 00:35:27
agetty            0.0   0.0  110044  2072 ttyS0 Dec03 00:00:00
agetty            0.0   0.0  110044  1624 tty1  Dec03 00:00:00
PedServer         0.9   0.0   94104  3256 ?     Dec03 01:52:21
ntls_vtsd         0.0   0.5 2654052 23440 ?     Dec03 00:10:53
pedClient         0.0   0.2  615512  9552 ?     Dec03 00:02:50
stcd_vtsd         0.0   0.3  785532 14852 ?     Dec03 00:01:06
sshd              0.0   0.2  106348  8292 ?     10:27 00:00:00
bash              0.0   0.0  115524  3572 pts/1 10:28 00:00:00
sleep             0.0   0.0  107904   720 ?     11:44 00:00:00
ps                0.0   0.0  148916  3700 pts/1 11:44 00:00:00
```

```
dhclient         0.0   0.4  111024 19396 ?     Dec10 00:00:00
sshd             0.0   0.1   66880  6072 ?     Dec08 00:00:00
sshd             0.0   0.2  106396  8216 ?     Dec09 00:00:01
bash             0.0   0.0  115524  3388 pts/0 Dec09 00:00:00


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 Network HSM 7 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 Network HSM 7) has no A/C power connected to it (it is in an audible alarm state).

User Privileges

Users with the following privileges can perform this command:

- Admin
- Operator
- Monitor

Syntax

status sensors [**-log**]

Argument(s)	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          . | 3700.000   | RPM        | ok    | 1000.000  | 2000.000  | na        | na
Fan1B          . | 4900.000   | RPM        | ok    | 1000.000  | 2000.000  | na        | na
Fan2A          . | 3700.000   | RPM        | ok    | 1000.000  | 2000.000  | na        | na
Fan2B          . | 5100.000   | RPM        | ok    | 1000.000  | 2000.000  | na        | na
Fan3A          . | 3800.000   | RPM        | ok    | 1000.000  | 2000.000  | na        | na
Fan3B          . | 5100.000   | RPM        | ok    | 1000.000  | 2000.000  | na        | na
CPU            . | 26.000     | degrees C  | ok    | na        | na        | 95.000    |
100.000
VRD            . | 28.000     | degrees C  | ok    | na        | na        | 105.000   |
110.000
PCH            . | 29.000     | degrees C  | ok    | na        | na        | 99.000    |
104.000
Inlet          . | 24.000     | degrees C  | ok    | na        | na        | 87.000    | 97.000
CHA DIMM 0     . | 11.000     | degrees C  | ok    | na        | na        | 87.000    | 97.000
CHA DIMM 1     . | 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
```

```
RAM TMax        . | 11.000     | degrees C  | ok    | na        | na        | na        | na
+12V            . | 12.240     | Volts      | ok    | na        | 11.160    | 12.900    | na
+5V             . | 5.250      | Volts      | ok    | na        | 4.650     | 5.370     | na
3VMain          . | 3.420      | Volts      | ok    | na        | 3.060     | 3.540     | na
5VSB            . | 5.250      | Volts      | ok    | na        | 4.650     | 5.370     | na
3VSB            . | 3.400      | Volts      | ok    | na        | 3.060     | 3.540     | na
CPU_VCORE       . | 0.330      | Volts      | ok    | na        | na        | na        | na
VCCSA           . | 1.060      | Volts      | ok    | na        | 0.980     | 1.130     | na
VCCIO           . | 0.970      | Volts      | ok    | na        | 0.880     | 1.020     | na
1V2             . | 1.250      | Volts      | ok    | na        | 1.130     | 1.290     | na
2V5_VPP         . | 2.540      | Volts      | ok    | na        | 2.320     | 2.680     | na
1V0_PCH         . | 1.010      | Volts      | ok    | na        | 0.930     | 1.080     | na
1V5_BMC         . | 1.550      | Volts      | ok    | na        | 1.470     | 1.930     | na
1V26_BMC        . | 1.270      | Volts      | ok    | na        | 1.170     | 1.350     | na
1V8_AUX         . | 1.820      | Volts      | ok    | na        | 1.670     | 1.930     | na
VBAT            . | 3.220      | Volts      | ok    | 2.100     | 2.500     | na        | na
PSU1_+12V_value. | 12.360     | Volts      | ok    | na        | 10.800    | 13.200    | na
PSU1 Temp_value. | 33.000     | degrees C  | ok    | na        | na        | 50.000    | na
PSU1 FAN_value . | 4600.000   | RPM        | ok    | 1000.000  | 1300.000  | na        | na
PSU2_+12V_value. | 0.000      | Volts      | CR *  | na        | 10.800    | 13.200    | na
PSU2 Temp_value. | 0.000      | degrees C  | ok    | na        | na        | 50.000    | na
PSU2 FAN_value . | 0.000      | RPM        | NR *  | 1000.000  | 1300.000  | na        | na
PSU1_Status     . | 0x0        | discrete   | 0x0180| na        | na        | na        | na
PSU2_Status     . | 0x0        | discrete   | 0x0080| na        | na        | na        | na
CPU_Thermtrip   . | 0x0        | discrete   | 0x0080| na        | na        | na        | na
Watchdog        . | 0x0        | discrete   | 0x0080| 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 --------------
PSU1_Status     . | Presence detected
PSU2_Status     . | Presence detected
CPU_Thermtrip   . | OK
Watchdog        . | OK

----------- Front Cooling Fans Status --------------
Fan1A           . | OK  | 3700 RPM
Fan1B           . | OK  | 4900 RPM
Fan2A           . | OK  | 3700 RPM
Fan2B           . | OK  | 5100 RPM
Fan3A           . | OK  | 3800 RPM
Fan3B           . | OK  | 5100 RPM
PSU1 FAN_value . | OK  | 4800 RPM
PSU2 FAN_value . | OK  | 4800 RPM

-------------- chassis status  -----------------
System Power         : on
Power Overload       : false
Power Interlock      : inactive
Main Power Fault     : false
```

```
Power Control Fault  : false
Power Restore Policy : previous
Last Power Event     : ac-failed
Chassis Intrusion    : inactive
Front-Panel Lockout  : inactive
Drive Fault          : false
Cooling/Fan Fault    : true
Sleep Button Disable : not allowed
Diag Button Disable  : not allowed
Reset Button Disable : allowed
Power Button Disable : allowed
Sleep Button Disabled: false
Diag Button Disabled : false
Reset Button Disabled: false
Power Button Disabled: false


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

Argument(s)	Shortcut	Description
code	**c**	Display descriptive text for a status code. See "status sysstat code" on the next page.
show	**s**	Display system status monitor service information. See "status sysstat show" on page 499.

status sysstat code

Display descriptions for the system status codes displayed on the appliance front-panel LCD. You can display information for all of the codes, or you can specify a specific code for which you want to display a description.

User Privileges

Users with the following privileges can perform this command:

- Admin
- Operator
- Monitor

Syntax

status sysstat code {**all** | <status_code>}

Argument(s)	Shortcut	Description
all	**a**	Display descriptions for all system status codes. See Front-panel LCD Display for a detailed description of all of the possible status codes.
<status_code>		Specifies the system status code for which you want to display information.

Example

```
lunash:>status sysstat code all

Code    State   Description
============================
0       ISO     In service and operational.
15      OOS     The cluster service is not running.
                Run "cluster show" and commands to view log files for more information.
20      OOS     The NTLS service is not running.
                Run commands to display NTLS status for more information.
25      OOS     The NTLS is not bound to an Ethernet device.
                Run commands to display NTLS status and to view log files for more information.
                See help on how to bind an NTLS interface.
30      OOS     The HSM service has experienced one or more errors.
                Or the HSM service has experienced one or more critical events.
                Run "hsm show" and commands to view HSM log files for more information.
40      OOS     The cobradb service is not running.
                Run commands to show network connection details and to view log files for more
information.
50      OFL     No Ethernet interfaces are connected to the network.
                Run commands to display network status and to view log files for more
information.
60      ISO     eth0 is offline.
                Run the command to restart the network service if it is not running.
                Run the command to show network status for more information.
```

```
61      ISO     eth1 is offline.
                Run the command to restart the network service if it is not running.
                Run the command to show network status for more information.
62      ISO     eth2 is offline.
                Run the command to restart the network service if it is not running.
                Run the command to show network status for more information.
63      ISO     eth3 is offline.
                Run the command to restart the network service if it is not running.
                Run the command to show network status for more information.
70      IST     The logging service is not running.
                Run commands to display the logging service status and to view log files for
more information.
                Run the command to restart the logging service if it is not running.
80      ISO     The STC service is not running.
                Run commands to display STC status for more information.
90      IST     The SSH service is not running.
                Run commands to display the SSH service status and to view log files for more
information.
                Run the command to restart the SSH service if it is not running.
95      ISO     The webserver service is not running.
                Run commands to display webserver status for more information.
100     ISO     The SNMP service is not running.
                Run commands to display the SNMP service status and to view log files for more
information.
                Run the command to restart the SNMP service if it is not running.
110     IST     One or more partitions on the disk drive are reaching maximum capacity.
                Run commands to delete files and clear logs to free some disk space.

Command Result : 0 (Success)
```

status sysstat show

Display system status monitor service information.

User Privileges

Users with the following privileges can perform this command:

- Admin
- Operator
- Monitor

Syntax

status sysstat show

Example

```
lunash:>status sysstat show

Volatile State:
sysstat is running
Service Status: sysstat is running

Non-volatile State:
Enabled


  System Status Monitor - Current Status
  ======================================
  Hostname:            sa7pw
  Interface eth0:      192.20.11.78
  Interface eth1:      not configured
  Interface eth2:      not configured
  Interface eth3:      not configured
  Software Version:    SA:7.0.0
  System Status:       ISO
  System Status Code:  100,61,62,63,95
  Status Check Time:   10:17 on 01/03/2017


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
operational 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.

User Privileges

Users with the following privileges can perform this command:

- Admin
- Operator
- Monitor

Syntax

status time

Example

```
lunash:> status time

10:23.11

Command Result : 0 (Success)
```

status zone

Displays the current time zone. This command is equivalent to the **sysconf timezone show** command.

User Privileges

Users with the following privileges can perform this command:

- Admin
- Operator
- Monitor

Syntax

status zone

Example

```
lunash:>status zone

EST

Command Result : 0 (Success)
```

stc

Use these commands to configure and manage secure trusted channel (STC) partition-client network links.

> **NOTE** Secure Trusted Channel (STC) changes format for Luna HSM Firmware 7.7.0; LunaSH commands used by the HSM SO for STC are described here for Luna HSM Firmware 7.4.2 and older, and are *discontinued* for Luna HSM Firmware 7.7.0 and newer.
>
> For Luna HSM Firmware 7.7.0 and newer, only the Partition SO can configure these STC options, using LunaCM (see **stcconfig**) after the partition is initialized.

You must be logged in as the HSM SO to use the **stc** commands.

Syntax

stc

activationtimeout
cipher
hmac
partition
rekeythreshold

Argument(s)	Shortcut	Description
activationtimeout	**a**	Set the activation timeout for an STC link. See "stc activationtimeout" on the next page.
cipher	**ci**	Disable the use of a symmetric encryption cipher algorithm for data encryption on an STC link. See "stc cipher" on page 506.
hmac	**h**	Disable the use of an HMAC message digest algorithm for identity verification on an STC link. See "stc hmac" on page 511.
partition	**p**	Export the specified partition's public key to a file. See "stc partition" on page 515. This command syntax has changed in Luna Network HSM 7 Appliance Software 7.7.0 and newer. See "partition stcidentity" on page 462.
rekeythreshold	**rek**	Set the key life for the symmetric key used to encrypt data on the STC link for the specified partition. See "stc rekeythreshold" on page 518.

stc activationtimeout

Control and monitor the STC activation timeout.

> **NOTE** Secure Trusted Channel (STC) changes format for Luna HSM Firmware 7.7.0; LunaSH commands used by the HSM SO for STC are described here for Luna HSM Firmware 7.4.2 and older, and are *discontinued* for Luna HSM Firmware 7.7.0 and newer.
>
> For Luna HSM Firmware 7.7.0 and newer, only the Partition SO can configure these STC options, using LunaCM (see **stcconfig**) after the partition is initialized.

You must be logged in as the HSM SO to use the **stc activationtimeout** commands.

Syntax

stc activationtimeout

set
show

Argument(s)	Shortcut	Description
set	**se**	Set the activation timeout for an STC link. See "stc activationTimeOut set" on the next page.
show	**sh**	Display the STC link activation timeout for the specified partition. See "stc activationTimeOut show" on page 505

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.

> **NOTE** Secure Trusted Channel (STC) changes format for Luna HSM Firmware 7.7.0; LunaSH commands used by the HSM SO for STC are described here for Luna HSM Firmware 7.4.2 and older, and are *discontinued* for Luna HSM Firmware 7.7.0 and newer.
>
> For Luna HSM Firmware 7.7.0 and newer, only the Partition SO can configure these STC options, using LunaCM (see **stcconfig**) after the partition is initialized.

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

User Privileges

Users with the following privileges can perform this command:

- Admin
- Operator

Syntax

stc activationTimeOut set -partition <partition_name> **-time** <timeout>

Argument(s)	Shortcut	Description
-partition <partition_name>	**-p**	Specifies the name of the partition for which you want to set the STC link activation timeout.
-time <timeout>	**-t**	Specifies the activation timeout, in seconds. **Range:** 1 to 240 **Default:** 120

Example

```
lunash:>stc activationTimeOut set -partition partition2 -time 60

Successfully changed the activation timeout for partition partition2 to 60 seconds.


Command Result : 0 (Success)
```

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.

> **NOTE** Secure Trusted Channel (STC) changes format for Luna HSM Firmware 7.7.0; LunaSH commands used by the HSM SO for STC are described here for Luna HSM Firmware 7.4.2 and older, and are *discontinued* for Luna HSM Firmware 7.7.0 and newer.
>
> For Luna HSM Firmware 7.7.0 and newer, only the Partition SO can configure these STC options, using LunaCM (see **stcconfig**) after the partition is initialized.

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

User Privileges

Users with the following privileges can perform this command:

- Admin
- Operator
- Monitor

Syntax

stc activationTimeOut show -partition <partition_name>

Argument(s)	Shortcut	Description
-partition <partition_name>	**-p**	Specifies the name of the partition for which you want to display the STC link activation timeout.

Example

```
lunash:>stc activationTimeOut show -partition partition2

The channel activation timeout for partition partition2 is 120 seconds.


Command Result : 0 (Success)
```

stc cipher

Control the use of symmetric encryption ciphers for STC.

> **NOTE** Secure Trusted Channel (STC) changes format for Luna HSM Firmware 7.7.0; LunaSH commands used by the HSM SO for STC are described here for Luna HSM Firmware 7.4.2 and older, and are *discontinued* for Luna HSM Firmware 7.7.0 and newer.
>
> For Luna HSM Firmware 7.7.0 and newer, only the Partition SO can configure these STC options, using LunaCM (see **stcconfig**) after the partition is initialized.

You must be logged in as the HSM SO to use the **stc cipher** commands.

Syntax

stc cipher

disable
enable
show

Argument(s)	Shortcut	Description
disable	**d**	Disable the use of a symmetric encryption cipher algorithm for data encryption on an STC link. See "stc cipher disable" on the next page.
enable	**e**	Enable the use of a symmetric encryption cipher algorithm used for data encryption on an STC link. See "stc cipher enable" on page 509.
show	**s**	List the symmetric encryption cipher algorithms you can use for STC data encryption on the specified partition. See "stc cipher show" on page 510.

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 510 to show which ciphers are currently enabled/disabled.

> **NOTE** Secure Trusted Channel (STC) changes format for Luna HSM Firmware 7.7.0; LunaSH commands used by the HSM SO for STC are described here for Luna HSM Firmware 7.4.2 and older, and are *discontinued* for Luna HSM Firmware 7.7.0 and newer.
>
> For Luna HSM Firmware 7.7.0 and newer, only the Partition SO can configure these STC options, using LunaCM (see **stcconfig**) after the partition is initialized.

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.

User Privileges

Users with the following privileges can perform this command:

- Admin
- Operator

Syntax

stc cipher disable -partition <partition_name> {**-all** | **-id** <cipher_id>} [**-force**]

Argument(s)	Shortcut	Description
-all	**-a**	Disable all ciphers
-force	**-f**	Force the action without prompting
-id <cipher_id>	**-i**	Specifies the numerical identifier of the cipher you want to disable, as listed using the command "stc cipher show" on page 510. **Valid values:** 1,2,3
-partition <partition_name>	**-p**	Specifies the name of the partition on which to disable the cipher (s).

Example

```
lunash:>stc cipher disable -partition partition2 -id 2

AES 192 Bit with Cipher Block Chaining is now disabled.


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 the next page to show which ciphers are currently enabled/disabled.

> **NOTE** Secure Trusted Channel (STC) changes format for Luna HSM Firmware 7.7.0; LunaSH commands used by the HSM SO for STC are described here for Luna HSM Firmware 7.4.2 and older, and are *discontinued* for Luna HSM Firmware 7.7.0 and newer.
>
> For Luna HSM Firmware 7.7.0 and newer, only the Partition SO can configure these STC options, using LunaCM (see **stcconfig**) after the partition is initialized.

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

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

User Privileges

Users with the following privileges can perform this command:

- Admin
- Operator

Syntax

stc cipher enable -partition <partition_name> {**-all** | **-id** <cipher_id>}

Argument(s)	Shortcut	Description
-all	**-a**	Enable all ciphers.
-id <cipher_id>	**-i**	Specifies the numerical identifier of the cipher you want to use, as listed using the command "stc cipher show" on the next page.
-partition <partition_name>	**-p**	Specifies the name of the partition for which you want to enable the specified cipher.

Example

```
lunash:>stc cipher enable -partition partition2 -id 2


AES 192 Bit with Cipher Block Chaining is now enabled.


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.

> **NOTE** Secure Trusted Channel (STC) changes format for Luna HSM Firmware 7.7.0; LunaSH commands used by the HSM SO for STC are described here for Luna HSM Firmware 7.4.2 and older, and are *discontinued* for Luna HSM Firmware 7.7.0 and newer.
>
> For Luna HSM Firmware 7.7.0 and newer, only the Partition SO can configure these STC options, using LunaCM (see **stcconfig**) after the partition is initialized.

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

User Privileges

Users with the following privileges can perform this command:

- Admin
- Operator
- Monitor

Syntax

stc cipher show -partition <partition_name>

Argument(s)	Shortcut	Description
-partition <partition_name>	**-p**	Specifies the partition for which you want to display the available ciphers.

Example

```
lunash:>stc cipher show -partition partition2

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 hmac

Enable, disable, and monitor the use of HMAC algorithms for STC.

> **NOTE** Secure Trusted Channel (STC) changes format for Luna HSM Firmware 7.7.0; LunaSH commands used by the HSM SO for STC are described here for Luna HSM Firmware 7.4.2 and older, and are *discontinued* for Luna HSM Firmware 7.7.0 and newer.
>
> For Luna HSM Firmware 7.7.0 and newer, only the Partition SO can configure these STC options, using LunaCM (see **stcconfig**) after the partition is initialized.

Syntax

stc hmac

disable
enable
show

Argument(s)	Shortcut	Description
disable	**d**	Disable the use of an HMAC message digest algorithm for identity verification on an STC link. See "stc hmac disable" on the next page.
enable	**e**	Enable the use of an HMAC message digest algorithm for integrity verification on an STC link. See "stc hmac enable" on page 513
show	**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 514

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 514 to show which HMAC message digest algorithms are currently enabled/disabled.

> **NOTE** Secure Trusted Channel (STC) changes format for Luna HSM Firmware 7.7.0; LunaSH commands used by the HSM SO for STC are described here for Luna HSM Firmware 7.4.2 and older, and are *discontinued* for Luna HSM Firmware 7.7.0 and newer.
>
> For Luna HSM Firmware 7.7.0 and newer, only the Partition SO can configure these STC options, using LunaCM (see **stcconfig**) after the partition is initialized.
>
> 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.

User Privileges

Users with the following privileges can perform this command:

- Admin
- Operator

Syntax

stc hmac disable -partition <partition_name> **-id** <hmac_id>

Argument(s)	Shortcut	Description
-partition <partition_name>	**-p**	Specifies the partition for which you want to disable an HMAC algorithm.
-id <hmac_id>	**-i**	Specifies the numerical identifier of the HMAC algorithm you want to disable, as listed using the command "stc hmac show" on page 514.

Example

```
lunash:>stc hmac disable -partition partition2 -id 1

HMAC with SHA 512 Bit is now disabled.


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 the next page to show which HMAC message digest algorithms are currently enabled/disabled.

> **NOTE** Secure Trusted Channel (STC) changes format for Luna HSM Firmware 7.7.0; LunaSH commands used by the HSM SO for STC are described here for Luna HSM Firmware 7.4.2 and older, and are *discontinued* for Luna HSM Firmware 7.7.0 and newer.
>
> For Luna HSM Firmware 7.7.0 and newer, only the Partition SO can configure these STC options, using LunaCM (see **stcconfig**) after the partition is initialized.
>
> 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.

User Privileges

Users with the following privileges can perform this command:

- Admin
- Operator

Syntax

stc hmac enable -partition <partition_name> **-id** <hmac_id>

Argument(s)	Shortcut	Description
-partition <partition_name>	**-p**	Specifies the partition for which you want to enable the HMAC algorithm.
-id <hmac_id>	**-i**	Specifies the numerical identifier of the HMAC algorithm you want to enable, as listed using the command "stc hmac show" on the next page.

Example

```
lunash:>stc hmac enable -partition partition2 -id 1

HMAC with SHA 512 Bit is now enabled.


Command Result : 0 (Success)
```

stc hmac show

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

> **NOTE** Secure Trusted Channel (STC) changes format for Luna HSM Firmware 7.7.0; LunaSH commands used by the HSM SO for STC are described here for Luna HSM Firmware 7.4.2 and older, and are *discontinued* for Luna HSM Firmware 7.7.0 and newer.
>
> For Luna HSM Firmware 7.7.0 and newer, only the Partition SO can configure these STC options, using LunaCM (see **stcconfig**) after the partition is initialized.

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

User Privileges

Users with the following privileges can perform this command:

- Admin
- Operator
- Monitor

Syntax

stc hmac show -partition <partition_name>

Argument(s)	Shortcut	Description
-partition <partition_name>	**-p**	Specifies the partition for which you want to display the available HMAC algorithms.

Example

```
lunash:>stc hmac show -partition partition2

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


 HMAC ID      HMAC Name                                  Enabled
_____________________________________________________________________

 0            HMAC with SHA 256 Bit                      Yes

 1            HMAC with SHA 512 Bit                      Yes


Command Result : 0 (Success)
```

stc partition

Export the STC partition identity, or display the hash for an STC partition.

> **NOTE** This command syntax has changed in Luna Network HSM 7 Appliance Software 7.7.0 and newer. See **"partition stcidentity" on page 462**.

You must be logged in as the HSM SO to use the **stc partition** commands.

Syntax

stc partition

export
show

Argument(s)	Shortcut	Description
export	**e**	Export the specified partition's public key to a file. See "stc partition export" on the next page.
show	**s**	Display the public key hash and serial number for the current partition. See "stc partition show" on page 517.

stc partition export

Export the specified partition's public key to a file. You must be logged in as HSM SO to use this command, and it can only be run on an uninitialized partition. Once the partition has been initialized, the public key can be exported by the Partition SO only, using LunaCM (see stcconfig partitionidexport).

> **NOTE** This command syntax has changed in Luna Network HSM 7 Appliance Software 7.7.0 and newer. See **"partition stcIdentity export" on page 463**.
>
> 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.

User Privileges

Users with the following privileges can perform this command:

- Admin
- Operator

Syntax

stc partition export -partition <partition_name>

Argument(s)	Shortcut	Description
-partition <partition_name>	**-p**	Specifies the name of the partition whose public key you want to export.

Example

```
lunash:>stc partition export -partition partition2

Successfully exported partition identity for partition partition2 to file: 154438865290.pid

Command Result : 0 (Success)
```

stc partition show

Display the public key hash and serial number for the specified partition. You must be logged in as HSM SO to use this command, and it can only be run on an uninitialized partition. Once the partition has been initialized, this information is available only to the Partition SO using LunaCM (see stcconfig partitionidshow).

> **NOTE** This command syntax has changed in Luna Network HSM 7 Appliance Software 7.7.0 and newer. See **"partition stcIdentity show" on page 464**.

User Privileges

Users with the following privileges can perform this command:

- Admin
- Operator
- Monitor

Syntax

stc partition show -partition <partition_name>

Argument(s)	Shortcut	Description
-partition<partition_name>	**-p**	Specifies the name of the partition whose public key hash and serial number you want to display.

Example

```
lunash:>stc partition show -partition partition2

Partition Serial Number:                 154438865290
Partition Identity Public Key SHA1 Hash: 67a26c546f0bdd911375c833babcf702aa61e3ee


Command Result : 0 (Success)
```

stc rekeythreshold

Monitor and set the STC re-keying threshold for the named partition.

> **NOTE** Secure Trusted Channel (STC) changes format for Luna HSM Firmware 7.7.0; LunaSH commands used by the HSM SO for STC are described here for Luna HSM Firmware 7.4.2 and older, and are *discontinued* for Luna HSM Firmware 7.7.0 and newer.
>
> For Luna HSM Firmware 7.7.0 and newer, only the Partition SO can configure these STC options, using LunaCM (see **stcconfig**) after the partition is initialized.

You must be logged in as the HSM SO to use the **stc rekeythreshold** commands.

Syntax

stc rekeythreshold

set
show

Argument(s)	Shortcut	Description
set	**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 the next page.
show	**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 520.

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.

> **NOTE** Secure Trusted Channel (STC) changes format for Luna HSM Firmware 7.7.0; LunaSH commands used by the HSM SO for STC are described here for Luna HSM Firmware 7.4.2 and older, and are *discontinued* for Luna HSM Firmware 7.7.0 and newer.
>
> For Luna HSM Firmware 7.7.0 and newer, only the Partition SO can configure these STC options, using LunaCM (see **stcconfig**) after the partition is initialized.

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.

User Privileges

Users with the following privileges can perform this command:

- Admin
- Operator

Syntax

stc rekeyThreshold set -partition <partition> **-value** <threshold>

Argument(s)	Shortcut	Description
-partition <partition_name>	**-p**	Specifies the name of the partition for which you want to specify the STC rekey threshold.
-value <threshold>	**-v**	An integer that specifies the key life (in millions of encoded messages) for the STC symmetric key. Enter a value of **0** to disable rekeying. **Range:** 0 to 4000 million messages. **Default:** 400 million messages.

Example

```
lunash:>stc rekeyThreshold set -partition partition2 -value 200

Successfully changed the rekey threshold for partition partition2 to 200 million messages.


Command Result : 0 (Success)
```

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.

> **NOTE** Secure Trusted Channel (STC) changes format for Luna HSM Firmware 7.7.0; LunaSH commands used by the HSM SO for STC are described here for Luna HSM Firmware 7.4.2 and older, and are *discontinued* for Luna HSM Firmware 7.7.0 and newer.
>
> For Luna HSM Firmware 7.7.0 and newer, only the Partition SO can configure these STC options, using LunaCM (see **stcconfig**) after the partition is initialized.

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

User Privileges

Users with the following privileges can perform this command:

- Admin
- Operator
- Monitor

Syntax

stc rekeyThreshold show -partition <partition_name>

Argument(s)	Shortcut	Description
-partition <partition_name>	**-p**	Specifies the name of the partition for which you want to display the STC rekey threshold.

Example

```
lunash:>stc rekeyThreshold show -partition partition2

Current rekey threshold for partition partition2 is 400 million messages.


Command Result : 0 (Success)
```

sysconf

Access commands that allow you to configure the appliance.

Syntax

sysconf

appliance
banner
config
ctc
drift
fingerprint
forceSOLogin
license
installCert
ntp
radius
regencert
snmp
ssh
time
timezone
tls

Argument(s)	Shortcut	Description
appliance	**a**	Access commands that allow you to manage the appliance. See "sysconf appliance" on page 523.
banner	**b**	Access commands to set and clear an extended text banner, displayed to appliance administrative users when they log into a LunaSH session. See "sysconf banner" on page 532.
config	**co**	Access the system configuration commands. See "sysconf config" on page 536.
ctc	**ct**	Access the system configuration commands. See "sysconf ctc" on page 555.
drift	**d**	Access commands that allow you to view and configure the drift. See "sysconf drift" on page 573.
fingerprint	**fi**	Display the certificate fingerprints. See "sysconf fingerprint" on page 580.

Argument(s)	Shortcut	Description
forcesologin	**fo**	Access commands that allow you to enable or disable SO login enforcement, or display the current SO login enforcement setting. See "sysconf forceSOLogin" on page 584.
installcert	**i**	Installs a signed certificate file as the appliance's server certificate (renaming to and replacing **server.pem**). See "sysconf installCert" on page 590.
license	**l**	Access commands that allow you to manage feature licensing for capability and partition upgrades. See "sysconf license" on page 592.
ntp	**n**	Access commands that allow you to view or configure the network time protocol (NTP). See "sysconf ntp" on page 596.
radius	**ra**	Manage RADIUS configuration and identify RADIUS servers to use for enhanced authentication, authorization, and accounting of your Luna Network HSM 7 appliance users and roles "sysconf radius" on page 631 .
regencert	**re**	Generate or re-generate the Luna appliance server hardware certificate. See "sysconf regenCert" on page 637.
snmp	**sn**	Access commands that allow you to view or configure the Simple Network Management Protocol (SNMP) settings for Luna Network HSM 7 appliance. See "sysconf snmp" on page 650.
ssh	**ss**	Access commands that allow you to view or configure the SSH options on the appliance. See "sysconf ssh" on page 676.
time	**t**	Set or display the time and date. See "sysconf time" on page 713.
timezone	**timez**	Set or display the time zone. See "sysconf timezone" on page 714.
tls	**tl**	Configure the set of ciphers that TLS can use when negotiating link security. See "sysconf tls ciphers" on page 718.

sysconf appliance

Access the **sysconf appliance** commands to manage the appliance.

Syntax

sysconf appliance

hardreboot
poweroff
reboot
rebootonpanic

Argument(s)	Shortcut	Description
hardreboot	**h**	Reboot the appliance, bypassing graceful closing of services. See "sysconf appliance hardReboot" on the next page.
poweroff	**p**	Power off the appliance. See "sysconf appliance poweroff" on page 525.
reboot	**r**	Reboot the appliance. See "sysconf appliance reboot" on page 526.
rebootonpanic	**rebooto**	System reboot on panic. See "sysconf appliance rebootonpanic" on page 528.

 Copyright 2001-2025 Thales Group

sysconf appliance hardReboot

Perform a hard restart (reboot) of the Luna Network HSM 7 appliance.

When you do not have convenient physical access to your Luna Network HSM 7 appliances, this command replaces the **sysconf appliance reboot** command (see "sysconf appliance reboot" on page 526) 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 Network HSM 7 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.

User Privileges

Users with the following privileges can perform this command:

> Admin

Syntax

sysconf appliance hardReboot [**-force**]

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

Example

```
lunash:>sysconf appliance hardReboot

WARNING !!  This command will reboot the appliance without gracefully shutdown.
            All clients will be disconnected.
If you are sure that you wish to proceed, then type 'proceed', otherwise type 'quit'

> proceed
```

sysconf appliance poweroff

Power off the Luna Network HSM 7 appliance.

Appliance reboot and power-off automatically take a snapshot of the system's known state and saves it to the **supportinfo.txt** file, so that you can send it to Technical Support for further investigation. This is useful if the system is not behaving and needs reboot or power-off. See "hsm supportInfo" on page 281 for more information.

User Privileges

Users with the following privileges can perform this command:

> Admin

> Operator

Syntax

sysconf appliance poweroff [**-force**]

Argument(s)	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/sftp' from a client machine to get file named:
supportInfo.txt


Broadcast message from root@local_host (Wed Mar  1 11:20:38 2017):

The system is going down for system halt NOW!
Power off commencing
```

sysconf appliance reboot

Performs a warm restart (reboot) of the Luna Network HSM 7 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 and saves it to the **supportinfo.txt** file, so that you can send it to Technical Support for further investigation. This is useful if the system is not behaving and needs reboot or power-off. See "hsm supportInfo" on page 281 for more information.

To deal with the possibility that a controlled shutdown might not be possible, see "sysconf appliance rebootOnPanic enable" on page 530.

> **NOTE** If you encounter messages like "Unrecoverable Error: Cannot get child exit status" (or similar) during shutdown / reboot, this is a result of some services not knowing that other services have already shut down. Ignore the message. See also System Operational and Error Messages.

> **NOTE** If you restart/reboot the Luna Network HSM 7 appliance, while using CTC measurement, then existing measurement records are lost. If you have an intentional restart coming up, consider running "sysconf ctc measurement show" on page 570 first, to capture bandwidth usage information that is about to be deleted.

User Privileges

Users with the following privileges can perform this command:

- Admin
- Operator

Syntax

sysconf appliance reboot [**-force**]

Argument(s)	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/sftp' from a client machine to get file named:
```

```
supportInfo.txt


Broadcast message from root@local_host (Wed Mar  1 11:24:08 2017):

The system is going down for reboot NOW!
Reboot commencing
```

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

Argument(s)	Shortcut	Description
disable	**d**	Disable system reboot on panic. See "sysconf appliance rebootOnPanic disable" on the next page.
enable	**e**	Enable system reboot on panic. See "sysconf appliance rebootOnPanic enable" on page 530.
show	**s**	Show system reboot on panic information. See "sysconf appliance rebootOnPanic show" on page 531.

sysconf appliance rebootOnPanic disable

Disable system automatic reboot on kernel panic.

User Privileges

Users with the following privileges can perform this command:

- Admin
- Operator

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 526 causes the appliance to shut down in a controlled manner.

This command configures the Luna Network HSM 7 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.

User Privileges

Users with the following privileges can perform this command:

- Admin
- Operator

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.

User Privileges

Users with the following privileges can perform this command:

- Admin
- Operator
- Monitor

Syntax

sysconf appliance rebootOnPanic show

Example

```
lunash:>sysconf appliance rebootOnPanic show

System auto reboot on panic is enabled.

Command Result : 0   (Success)
```

 Copyright 2001-2025 Thales Group

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 LunaSH session.

Syntax

sysconf banner

add
clear

Argument(s)	Shortcut	Description
add	**a**	Add extended banner text from a file. See "sysconf banner add" on the next page.
clear	**c**	Clear the extended banner text. See "sysconf banner clear" on page 535.

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 **pscp**/**sftp**.

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 the following characters:

`abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ.-_`

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**.

User Privileges

Users with the following privileges can perform this command:

> Admin

Syntax

sysconf banner add -file <filename>

Argument(s)	Shortcut	Description
-file <filename>	**-f**	Banner text file name.

Example

```
lunash:>my file list

   273 Mar  1 11:42 banner1.txt
   515 Mar  1 10:57 154438865290.pid
133913 Feb 28 15:59 supportInfo.txt
  4330 Feb 28 15:07 firstboot.log

Command Result : 0 (Success)



lunash:>sysconf banner add -file banner1.txt


Command Result : 0 (Success)
```

```
login as: admin
admin@192.20.11.78's password:
Last login: Wed Mar  1 10:36:40 2017 from 10.124.0.87

Luna SA 7.0.0 Command Line Shell - Copyright (c) 2001-2017 SafeNet, Inc. All rights reserved.


-----------------------------------------W A R N I N G-----------------------------------------
-


                    Your use of this resource is monitored and recorded for
                            security and quality-control purposes.


                                                d=(^_-)


----------------------------------H A V E---A---N I C E---D A Y--------------------------------
-


[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**.

User Privileges

Users with the following privileges can perform this command:

> Admin

Syntax

sysconf banner clear [**-force**]

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

Example

```
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)
```

sysconf config

Access the system configuration commands. All the commands in this subset deal with the handling of configuration files for the network HSM appliance, external to the cryptographic module. (For configuration and management of the crypto module, see the "hsm" on page 163 and "partition" on page 418 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, CTC, etc.

Syntax

sysconf config

backup
clear
delete
export
factoryreset
import
list
restore
show

Argument(s)	Shortcut	Description
backup	**b**	Backs up configuration data. See "sysconf config backup" on the next page.
clear	**c**	Deletes all the configuration backup files except the initial factory configuration file. See "sysconf config clear" on page 540.
delete	**d**	Deletes a configuration backup file. See "sysconf config delete" on page 541.
export	**e**	Exports a configuration backup file. See "sysconf config export" on page 542.
factoryreset	**f**	Factory reset. See "sysconf config factoryReset" on page 543.
import	**i**	Imports a configuration backup file. See "sysconf config import" on page 547.
list	**l**	List configuration backup files. See "sysconf config list" on page 549.
restore	**r**	Restores configuration backup. See "sysconf config restore" on page 550.
show	**s**	Show the current configuration. See "sysconf config show" on page 553.

sysconf config backup

Back up the appliance configuration data, and save it to the appliance file system. There is no limit on the size of individual backup files (using Luna Appliance Software 7.8.5 or newer) or the number of backups that can be stored on the file system, other than the available space. This space is shared by other files, such as spkg and log files, so account for this when planning your backup and restore strategy.

> **NOTE** If the configuration content is less than 64 KB, a single file is generated with a name that includes the creation date and time.
>
> If the lunash:> "sysconf config backup" above command detects that your configuration is more than 64 KB, then it breaks the config content into chunks, each of less than 64 KB. The backup chunk files get the same name, except that each has a sequential number appended. An additional generated file contains a hash of all the chunk files, and is used to reassemble the large backup when you later restore with lunash:> "sysconf config restore" on page 550 (using Luna Appliance Software 7.8.5 or newer).

If desired, you can use the command "sysconf config export" on page 542 to save the backup file to the internal HSM, or an external backup token after you create it.

> **NOTE** This command does not backup the HSM and partition configurations. See "hsm backup" on page 166 and "partition backup" on page 422 for more information.

Certificates, if any, are added to the backup archive, and are restored to the trust store upon "sysconf config restore" on page 550.

Audit log encryption uses the same certificates, so it is important to coordinate with the audit user for any changes.

The backup file includes configuration data for the following modules and services:

CTC	Crypto Traffic Control configuration (requires Luna Appliance Software 7.8.3 or newer)
Network	Network configuration
NTLS	NTLS configuration
NTP	Network Time Protocol configuration
SNMP	SNMP configuration
SSH	SSH configuration
Syslog	Syslog configuration
System	System configuration (keys and certificates)
Users	User accounts, passwords, and files

Webserver	Webserver configuration for REST API

User Privileges

Users with the following privileges can perform this command:

> Admin

Syntax

sysconf config backup -description <comment> [**-service** <name>] [**-factoryconfig**]

Argument(s)	Shortcut	Description
-description <comment>	**-d**	Comment describing this backup. The description must be enclosed in double quotes if it contains spaces.
-service <name>	**-s**	Specifies the individual service configuration to back up. If this option is not included, all service configurations are backed up as described above. **Valid Values:** network, ssh, ntls, syslog, ntp, snmp, users, system, webserver, ctc Service syslog uses the same certificates as audit log encryption. This option requires Luna Appliance Software 7.8.5 or newer.
-factoryconfig	**-f**	Binary option.

Example using Luna Appliance Software 7.8.5 or newer

With a service selected

```
lunash:>sysconf config backup -service ntls -d ntls

Created configuration backup file: local_host_Config_ntls_20240206_1657.tar.gz

It is recommended to export the backup file to the internal HSM, or an external backup token to
mitigate the risk of data loss.


Command Result : 0 (Success)
[local_host] lunash:>sysconf config list


Configuration backup files in file system:

Size     |  File Name                                                  |  Description
-------------------------------------------------------------------------------------------------
------
10970    |  local_host_Config_ntls_20240206_1657.tar.gz                |  ntls

Command Result : 0 (Success)
```

Without a service selected

```
lunash:>sysconf config backup -d "all of them"

Created configuration backup file: local_host_Config_all_20240206_1657.tar.gz

It is recommended to export the backup file to the internal HSM, or an external backup token to
mitigate the risk of data loss.


Command Result : 0 (Success)
[local_host] lunash:>sysconf config list


Configuration backup files in file system:

Size    |  File Name                                                |  Description
------------------------------------------------------------------------------------------------------
------
10970   |  local_host_Config_ntls_20240206_1657.tar.gz              |  ntls
62972   |  local_host_Config_all_20240206_1657.tar.gz              |  all of them

Command Result : 0 (Success)
```

Example using Luna Appliance Software older than 7.8.5

```
lunash:>sysconf config backup -description "Configuration Backup 17-03-01"


Created configuration backup file: local_host_Config_20170301_1200.tar.gz


Command Result : 0 (Success)
```

sysconf config clear

Deletes 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".

User Privileges

Users with the following privileges can perform this command:

> Admin

Syntax

sysconf config clear [**-force**] [**-devicetype** <devicetype>] [**-serialnumber** <serialnum>]

Argument(s)	Shortcut	Description
-devicetype <devicetype>	**-d**	Specifies whether to delete configuration backup files in the internal HSM or an external backup token. **Valid values:** hsm,token
-force	**-f**	Force the action without prompting.
-serialnumber <serialnum>	**-s**	Specifies the serial number of the token where backup files are to be deleted. Required if **-devicetype** is "**token**", optional if "**hsm**".

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.

User Privileges

Users with the following privileges can perform this command:

> Admin

Syntax

sysconf config delete -file <filename> [**-deviceType** <devicetype>] [**-serialnumber** <serialnum>] [**-force**]

Argument(s)	Shortcut	Description
-devicetype <devicetype>	**-d**	Device Type **Valid values**: hsm, token
-file <filename>	**-fi**	File name to delete
-force	**-fo**	Force action (no prompting for confirmation)
-serialnumber <serialnum>	**-s**	Token Serial Number

Example

```
lunash:>sysconf config delete -file local_host_Config_20170301_1222.tar.gz


WARNING !!  This command deletes the configuration backup file: local_host_Config_20170301_
1222.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".

The maximum size of configuration files that can be exported is 64 KB. The Luna Network HSM 7's Admin/SO partition has a maximum capacity of 384 KB.

User Privileges

Users with the following privileges can perform this command:

> Admin

Syntax

sysconf config export -file <filename> [**-devicetype** <devicetype>] [**-serialnumber** <serialnum>] [**-force**]

Argument(s)	Shortcut	Description
-devicetype <devicetype>	**-d**	Device Type (hsm, token)
-file <filename>	**-fi**	Name to be assigned to the exported configuration backup file.
-force	**-fo**	Force Action (no prompting for confirmation)
-serialnumber <serialnum>	**-s**	Token Serial Number

Example

```
lunash:>sysconf config export -file local_host_Config_20170301_1212.tar.gz -devicetype hsm -
serialnumber 66331


WARNING !!  This command exports the configuration backup file: local_host_Config_20170301_
1212.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 factoryReset

Reset the appliance to the settings created at the factory. 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" on page 173** (which can be run from a local serial console only).

This command factory resets the configuration file and removes all certificates from the trust store.

We recommend disconnecting all NTLS connections before performing factory reset.

> **NOTE** Using Luna Appliance Software 7.3.0 or older, following a factory reset of network services, it is normal for NTLS service to be still running. However, the CTC service stops (if it was running). Since none of the devices has a gateway, after reconfiguring of eth0, CTC is still inactive. Run "sysconf ctc enable" on page 566 to resume CTC operation.
>
> Using Luna Appliance Software 7.8.4 or newer, NTLS service stops after command "sysconf config factoryReset" above.

Files are not affected

The log files, and the content of users' home directories are not affected by this command.

- To clear log files you can use the **"syslog cleanup" on page 742** command. If you need to keep the logs, you should use the **"syslog tarlogs" on page 764** command, then sftp the logs file to another computer before clearing the log files.
- To clear the content of the user's home directory, use the **my file clear** command.

SO login required if "Force SO login" policy is set

If the Force SO login policy is set for the HSM (see command **"sysconf forceSOLogin show" on page 589**), then you must log in as SO before resetting

- the 'ntls' service,
- the ctc service,
- the ntp service,
- or 'all' services (which would include the previous three).

If the HSM is zeroized, then **hsm login** is not needed, even if ForceSOlogin is enabled.

ForceSOlogin is disabled following a successful **"hsm login" on page 198** if 'ntls' or 'all' services are reset.

What to do

To preserve desired settings and capabilities, we recommend that you perform **sysconf config backup** on your system whenever you upgrade or update or reconfigure, so as to have a backup with all desired configurations in place, and then use **"sysconf config restore" on page 550** if needed, reserving **"sysconf config factoryReset" above** for only those occasions when you want the appliance set all the way back to original factory specification.

- Use this command along with the **"hsm factoryReset" on page 173** command, if you want internal cryptographic module (HSM) settings returned to factory default values.
- Use this command from a locally-connected serial terminal (or console server). This command resets network settings to use DHCP; as a result the network interfaces might be assigned new IP addresses. You can get the new IP addresses on the LCD or from a serial port connection.
- Disconnect all NTLS connections before factory reset.

User Privileges

Users with the following privileges can perform this command:

- Admin

Syntax

sysconf config factoryReset -service <service> [**-force**]

Argument(s)	Shortcut	Description
-force	**-f**	Force the action without prompting.
-service <service>	**-s**	Specifies the service name. **Valid values:** network,ssh,ntls,syslog,ntp,snmp,users,system,webserver,all

Example with no active client connections

```
lunash:>sysconf config factoryReset -service all

 Checking for connected clients


 There are no active clients at this time.


 This command resets the configuration of the selected service(s) to factory defaults.
 Resetting services to factory defaults can affect connectivity and the operation of the HSM.
 If you are sure that you wish to proceed, then type 'proceed', otherwise type 'quit'.

> proceed
Proceeding...
 Resetting service(s) to factory defaults:
 ----------------------------------------
 webserver :          succeeded
 users     :          succeeded
 snmp      :          succeeded
 ntp       :          succeeded
 ntls      :          succeeded
 system    :          succeeded
 ssh       :          succeeded
 syslog    :          succeeded
```

```
 network   :          succeeded

Command Result : 0 (Success)
```

Example with no active client connections and force option used

```
lunash:>sysconf config factoryReset -service all -force

 Checking for connected clients
 There are no active clients at this time.

 Force option used. Proceed prompt bypassed.


 Resetting service(s) to factory defaults:
 -----------------------------------------
 webserver :          succeeded
 users     :          succeeded
 snmp      :          succeeded
 ntp       :          succeeded
 ntls      :          succeeded
 system    :          succeeded
 ssh       :          succeeded
 syslog    :          succeeded
 network   :          succeeded

Command Result : 0 (Success)
```

Example with active client connections

```
lunash:>sysconf config factoryReset -service all

 Checking for connected clients


 WARNING !! There are 1 client(s) connected to this Luna Network HSM
 appliance. It is recommended that you disconnect all clients
 before using this command.
 This command resets the configuration of the selected service(s) to factory defaults.
 Resetting services to factory defaults can affect connectivity and the operation of the HSM.
 If you are sure that you wish to proceed, then type 'proceed', otherwise type 'quit'.

> proceed
Proceeding...
 Resetting service(s) to factory defaults:
 -----------------------------------------
 webserver :          succeeded
 users     :          succeeded
 snmp      :          succeeded
 ntp       :          succeeded
 ntls      :          succeeded
 system    :          succeeded
 ssh       :          succeeded
 syslog    :          succeeded
 network   :          succeeded

Command Result : 0 (Success)
```

Example with active client connections and force option used

```
lunash:>sysconf config factoryReset -service all -force


 Checking for connected clients


 WARNING !! There are 1 client(s) connected to this Luna SA
 appliance. It is recommended that you disconnect all clients
 before using this command.
 Force option used. Proceed prompt bypassed.


 Resetting service(s) to factory defaults:
 -----------------------------------------
 webserver :          succeeded
 users     :          succeeded
 snmp      :          succeeded
 ntp       :          succeeded
 ntls      :          succeeded
 system    :          succeeded
 ssh       :          succeeded
 syslog    :          succeeded
 network   :          succeeded

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".

User Privileges

Users with the following privileges can perform this command:

> Admin

Syntax

sysconf config import -file <filename> [**-devicetype** <devicetype>] [**-serialnumber** <serialnum>] [**-force**]

Argument(s)	Shortcut	Description
-devicetype <devicetype>	**-d**	Device Type (hsm, token)
-file <filename>	**-fi**	Name of configuration backup file to be imported.
-force	**-fo**	Force the action without prompting.
-serialnumber <serialnum>	**-s**	Token Serial Number

Example (pre-7.8.5 filesize limit was 64 KB)

```
lunash:>sysconf config import -file local_host_Config_20170301_1212.tar.gz -devicetype hsm -
serialnumber 66331


WARNING !!  This command imports the configuration backup file: local_host_Config_20170301_
1212.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)
```

Example (7.8.5 onward)

This import example is for the new case, where your exported configuration was larger than 64 KB and needed to be split into smaller chunk files.
Notice that the filename provided for this import is as it would be for a single file, *without* the added chunk-numbering. lunash takes care of bringing the chunks back together.

```
[local_host] lunash:>sysconf config import -file local_host_Config_ntls_20240510_0145.tar.gz -d
token -s 7001966


WARNING !!  This command imports the configuration backup file: local_host_Config_ntls_
20240510_0145.tar.gz from the token.
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)
[local_host] lunash:>
[local_host] lunash:>sysconf config list

Configuration backup files in file system:

Size (in bytes) |  File Name                                                |  Description
-----------------------------------------------------------------------------------------------
------
136661          |  local_host_Config_ntls_20240510_0145.tar.gz              |  taking backup of
NTLS configuration with ipcheck disabled

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

sysconf config list

Show the list of configuration backup files stored in the file system, the internal HSM, or in an external token.

Use this command without any parameters to list the configuration files stored in the file system.

User Privileges

Users with the following privileges can perform this command:

- Admin
- Operator
- Monitor

Syntax

sysconf config list [**-devicetype** <devicetype>] [**-serialnumber** <serialnumber>]

Argument(s)	Shortcut	Description
-devicetype <devicetype>	**-d**	Specifies the device type. You must be logged in as the HSM SO to use this parameter. **Valid values:** hsm, token
-serialnumber <serialnum>	**-s**	Specifies the token serial number: > this parameter is not required, and is ignored, if **-devicetype** is not specified. > this parameter is required if **-devicetype** is **token** > this parameter is optional if **-devicetype** is **hsm**.

Example

```
lunash:>sysconf config list


Configuration backup files in file system:

Size    |  File Name                                                |  Description
-------------------------------------------------------------------------------------------------
------
14551   |  local_host_Config_20170301_1200.tar.gz                   |  Configuration Backup 17-
03-01
14555   |  local_host_Config_20170301_1212.tar.gz                   |  Backup before Factory
Reset
14568   |  local_host_Config_20170301_1222.tar.gz                   |  Automatic Backup Before
Restoring: ntls

Command Result : 0 (Success)
```

sysconf config restore

Restore configuration of the selected services from a backup file. This command automatically creates a backup file of the current configurations before restoring a previous configuration. You can restore the previous configurations from this backup if the new settings are not acceptable.

> **NOTE** If the configuration content is less than 64 KB, a single file is generated with a name that includes the creation date and time.
>
> If the lunash:> "sysconf config backup" on page 537 command detects that your configuration is more than 64 KB, then it breaks the config content into chunks, each of less than 64 KB. The backup chunk files get the same name, except that each has a sequential number appended. An additional generated file contains a hash of all the chunk files, and is used to reassemble the large backup when you later restore with lunash:> "sysconf config restore" above (using Luna Appliance Software 7.8.5 or newer).

If you store your appliance configuration on an HSM (using **"sysconf config export" on page 542**) you must first use the command **"sysconf config import" on page 547** to import the configuration file from the HSM to the appliance file system before using this **restore** command.

The service(s) must be stopped before restoring their configuration.

You must reboot the appliance for the changes to take effect. Please check the new configurations before rebooting or restarting the services.

Certificates, if any, are added to the backup archive, and are restored to the strust store upon config restore.

> **NOTE** This command does not restore the HSM (crypto module) and Partition configurations (see "hsm restore" on page 231 and "partition restore" on page 452 for more information).

User Privileges

Users with the following privileges can perform this command:

> Admin

Syntax

sysconf config restore -file <filename> **-service** <service> [**-force**]

Argument(s)	Shortcut	Description
-file <filename>	**-fi**	Name of the configuration backup file to restore.
-force	**-fo**	Force the action without prompting.

Argument(s)	Shortcut	Description
-service <service>	**-s**	The service name. This option requires Luna Appliance Software 7.8.5 or newer. **Valid values:** network,ssh,ntls,ctc,syslog,ntp,snmp,users,system,webserver,all Service **syslog** uses the same certificates as audit log encryption.

Example using Luna Appliance Software 7.9.0 or newer

```
lunash:>sysconf config restore -s network -fi  local_host_Config_network_20241023_0849.tar.gz


WARNING !! This command restores the configuration from the backup file: local_host_Config_
network_20241023_0849.tar.gz.
It first creates a backup of the current configuration before restoring: local_host_Config_
network_20241023_0849.tar.gz.
If you are sure that you wish to proceed, then type 'proceed', otherwise type 'quit'

> proceed
Proceeding

Created configuration backup file: local_host_Config_network_20241023_0915.tar.gz

It is recommended to export the backup file to the internal HSM, or an external backup token to
mitigate the risk of data loss.

Restore the network configuration: Succeeded.

You must reboot the appliance for all changes to take effect.
You can restore the previous configurations if the new settings are not acceptable.
If the service being restored was disabled prior to restoring, then the user needs to manually
enable it.

Command Result : 0 (Success)
```

Example using Luna Appliance Software older than 7.8.5

```
lunash:>sysconf config restore -file local_host_Config_20170301_1212.tar.gz -service ntls


WARNING !! This command restores the configuration from the backup file: local_host_Config_
20170301_1212.tar.gz.
It first creates a backup of the current configuration before restoring: local_host_Config_
20170301_1212.tar.gz.
If you are sure that you wish to proceed, then type 'proceed', otherwise type 'quit'.

> proceed
Proceeding...


Created configuration backup file: local_host_Config_20170301_1222.tar.gz


Restore the ntls 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)
```

> **NOTE** Noticeable changes using Luna Appliance Software 7.8.5 or newer:
> - backups would have either "all" or a single service in the filename
> - backups *could* be larger than 64 KB and therefore be spread across multiple files (that must all be stored, handled, used together).

sysconf config show

Shows the system information of a configuration backup file.

User Privileges

Users with the following privileges can perform this command:

- Admin
- Operator
- Monitor

Syntax

sysconf config show -file <filename>

Argument(s)	Shortcut	Description
-file <filename>	**-f**	Name of the configuration backup file.

Example (pre-7.8.5)

```
lunash:>sysconf config show -file local_host_Config_20170301_1200.tar.gz


System information when this backup was created:

hostname: local_host
eth0 IP Address: 192.20.11.78
eth1 IP Address:
eth2 IP Address:
eth3 IP Address:
Software Version: Luna SA 7.0.0 [Build Time: 20170228 12:16]
HSM Firmware Version: 7.0.1
HSM Serial Number: 66331
uptime:  12:00:07 up 20:00,  1 user,  load average: 0.31, 0.28, 0.25
Current time: Wed Mar  1 12:00:07 EST 2017

Description: Configuration Backup 17-03-01



Command Result : 0 (Success)
```

Example (7.8.5 onward)

(Note the addition of "Service backed up:")

```
lunash:>sysconf config show -file docs_lab_Config_ntls_20240625_1248.tar.gz


System information when this backup was created:
```

```
hostname: docs_lab
eth0 IP Address: 192.168.11.156
eth1 IP Address:
eth2 IP Address:
eth3 IP Address:
Software Version: Luna Network HSM v7.8.5-13 [Build Time: 20240620 13:48]
HSM Firmware Version: 7.8.4
HSM Serial Number: 532018
uptime:  12:48:49 up 1 day,  3:07,  2 users,  load average: 0.28, 0.26, 0.24
Current time: Tue Jun 25 12:48:49 EDT 2024

Service backed up: ntls
Description: testing321


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

sysconf ctc

Access the Crypto Traffic Controller (CTC) commands to measure, and to differentially control, bandwidth usage by each connected client, as part of your planning and provisioning and QoS efforts. See Crypto Traffic Controller (CTC) for QoS.

Syntax

sysconf ctc

class
client
disable
enable
measurement
show

Argument(s)	Shortcut	Description
class	**cla**	> Configure and assign classes of controlled bandwidth usage by clients. See "sysconf ctc class" on the next page.
client	**cli**	> Display Class to Client Mapping. See "sysconf ctc client show" on page 564.
disable	**d**	Disable CTC Service. See "sysconf ctc disable" on page 565.
enable	**e**	Enable CTC Service. See "sysconf ctc enable" on page 566.
measurement	**m**	> Measure the bandwidth consumed by each client. See "sysconf ctc measurement" on page 567.
show	**s**	Get CTC Service Information. See "sysconf ctc show" on page 572.

sysconf ctc class

The Crypto Traffic Controller (CTC) commands, to create and populate classes of permitted bandwidth consumption, to which clients can be assigned for control of their relative access to the appliance's network and crypto resources.

Syntax

sysconf ctc class

assign
define
delete
revoke
show

Argument(s)	Shortcut	Description
assign	**a**	Assign a client to a class of permitted bandwidth usage. See "sysconf ctc class assign" on the next page.
define	**def**	Define a class of permitted bandwidth usage. See "sysconf ctc class define" on page 558.
delete	**del**	Delete a class. See "sysconf ctc class delete" on page 560.
revoke	**r**	Revoke a client from a class. See "sysconf ctc class revoke" on page 561.
show	**s**	Show configured classes of permitted bandwidth usage. See "sysconf ctc class show" on page 562.

sysconf ctc class assign

Assigns a client to a class.

The number of classes that can be created, and the number of clients that can be assigned, are not explicitly limited. Practical limits arise from the overall bandwidth of the interface, .

> **NOTE** Changes made to CTC configuration come into effect the next time CTC service is restarted. This gives you control over when changes become effective.

> **TIP** Because CTC works on egress traffic only, be aware of the effects on outgoing interface selection when the choice is affected by Impact of route metric on CTC and Impact of default route on CTC.

User Privileges

Users with the following privileges can perform this command:

- Admin
- Operator

Syntax

sysconf ctc class assign -class <class_name> **-interface** <eth0> | <eth1> | <eth2> | <eth3> | <bond0> | <bond1> **-ipaddress** <IPv4_address>

Argument(s)	Shortcut	Description
-class <class_name>	**-c**	Class name. Assigning to a non-existing or “default” class returns an error.
-interface <net_device>	**-if**	A network interface devicename on the Luna Network HSM 7 (eth0, eth1, eth2, eth3, bond0, or bond1).
-ipaddress <IPv4_address>	**-ip**	Client IP address.

Example

```
lunash:>sysconf ctc class assign -in eth0 -class class1 -ip 192.168.0.16


Command Result : 0 (Success)
```

sysconf ctc class define

Creates a class under the Crypto Traffic Controller.

When the appliance is not fully loaded, the definition of a class directs the underlying system, at any point during operation, to guarantee **-min** amount of interface bandwidth for the current client, but at no time should that exceed **-max** amount of bandwidth.
If the appliance is considerably loaded with traffic, the system might borrow any unused bandwidth from another class, to serve the client that needs it, in order to sustain quality of service (QoS) for that client.

> **NOTE** You can define as many classes as you like, with whatever **-min** setting, until the total of all **-min** values assigned to one interface reaches the capacity of the interface, after which any further attempts to define a class against that interface are refused, with an error.
>
> If you want to *make a change to an existing class*, just reissue the **sysconf ctc class define** command with the revised parameter(s). This edits/overwrites the existing class.

> **NOTE** Changes made to CTC configuration come into effect the next time CTC service is restarted. This gives you control over when changes become effective.

> **TIP** Because CTC works on egress traffic only, be aware of the effects on outgoing interface selection when the choice is affected by Impact of route metric on CTC and Impact of default route on CTC.

User Privileges

Users with the following privileges can perform this command:

- Admin
- Operator

Syntax

sysconf ctc class define -class <class_name> **-interface** <eth0> | <eth1> | <eth2> | <eth3> | <bond0> | <bond1> **-minimum** <minimum_bandwidth> [**-maximum** <maximum_bandwidth>]

Argument(s)	Shortcut	Description
-class <class_name>	**-c**	Class name. • The name “default” is a reserved class name and is not permitted.
-interface <net_device>	**-i**	A network interface devicename on the Luna Network HSM 7 (eth0, eth1, eth2, eth3, bond0, or bond1).
-minimum <min_bandwidth>	**-min**	Minimum bandwidth in Kilobits.

Argument(s)	Shortcut	Description
-maximum <max_bandwidth>	**-max**	[Optional] Maximum bandwidth in Kilobits. If a "max" value is not provided, the value provided for “min” is used to set the maximum bandwidth.

Example

```
lunash:>sysconf ctc class define -c class1 -i eth0 -min 100 -max 200


Command Result : 0 (Success)
```

sysconf ctc class delete

Deletes a class.

> **NOTE** Changes made to CTC configuration come into effect the next time CTC service is restarted. This gives you control over when changes become effective.

User Privileges

Users with the following privileges can perform this command:

- Admin
- Operator

Syntax

sysconf ctc class delete -class <class_name> **-interface** <eth0> | <eth1> | <eth2> | <eth3> | <bond0> | <bond1>

Argument(s)	Shortcut	Description
-class <class_name>	**-c**	Class name.
-interface <net_device>	**-if**	A network interface devicename on the Luna Network HSM 7 (eth0, eth1, eth2, eth3, bond0, or bond1).

Example

```
lunash:>sysconf ctc class delete -i eth0 -class class1


Command Result : 0 (Success)
.
```

sysconf ctc class revoke

Revokes a client from a class.

> **NOTE** Changes made to CTC configuration come into effect the next time CTC service is restarted. This gives you control over when changes become effective.

User Privileges

Users with the following privileges can perform this command:

- Admin
- Operator

Syntax

sysconf ctc class revoke -interface <eth0> | <eth1> | <eth2> | <eth3> | <bond0> | <bond1> **-ipaddress** <IPv4_address>

Argument(s)	Shortcut	Description
-interface <net_device>	**-if**	A network interface devicename on the Luna Network HSM 7 (eth0, eth1, eth2, eth3, bond0, or bond1).
-ipaddress <IPv4_address>	**-ip**	Client IP address. Revoking a non-registered client results in an error.

Example

```
lunash:>sysconf ctc class revoke -in eth0 -ip 192.168.0.16


Command Result : 0 (Success)
```

sysconf ctc class show

Show configured classes.

User Privileges

Users with the following privileges can perform this command:

- Admin
- Operator
- Monitor

Syntax

sysconf ctc class show -interface <eth0> | <eth1> | <eth2> | <eth3> | <bond0> | <bond1>

Argument(s)	Shortcut	Description
-interface <net_device>	**-i**	A network interface devicename on the Luna Network HSM 7 (eth0, eth1, eth2, eth3, bond0, or bond1). If the "**-i**" option is not specified, interfaces without class definitions are skipped. If no class is defined, the message "No class configured" is shown. If an interface is specified with the "**-i**" option, classes defined for that interface are displayed. If no class definitions are present, a response of "None" is shown.

Example with no interface specified but one is found with class configured

```
lunash:>sysconf ctc class show
eth0:
          class            min            max
---------------------------------------------
         class1         10kbit         15kbit
---------------------------------------------


Command Result : 0 (Success)
```

Example with an interface specified and class is configured

```
lunash:>sysconf ctc class show -i eth2

          class            min            max
---------------------------------------------
         class1         10kbit         15kbit
---------------------------------------------


Command Result : 0 (Success)
```

Example with an interface specified but no class configured

```
lunash:>sysconf ctc class show -i eth2

          class            min            max
---------------------------------------------
NONE
---------------------------------------------


Command Result : 0 (Success)
```

Example with no interface specified and no class configured

```
lunash:>sysconf ctc class show

No class configured.


Command Result : 0 (Success)
```

sysconf ctc client show

Show assigned clients.

User Privileges

Users with the following privileges can perform this command:

- Admin
- Operator
- Monitor

Syntax

sysconf ctc client show -interface <eth0> | <eth1> | <eth2> | <eth3> | <bond0> | <bond1>

Argument(s)	Shortcut	Description
-interface <net_device>	**-i**	A network interface devicename on the Luna Network HSM 7 (eth0, eth1, eth2, eth3, bond0, or bond1). If the "**-i**" option is not specified, interfaces without assigned clients are skipped. If no clients have been assigned, the message "No clients are configured" is shown. If the interface is specified with the "**-i**" option, clients assigned to that interface are displayed. If no clients have been assigned, "None" is shown.

Example with no interface specified, but a client is assigned

```
lunash:>sysconf ctc client show
eth0:
         client          class
------------------------------
  192.168.10 13         class1
  192.168.10.16         class1
------------------------------


Command Result : 0 (Success)
```

Example with interface specified, and a client is assigned

```
lunash:>sysconf ctc client show -i eth0

         client          class
------------------------------
  192.168.10 13         class1
  192.168.10.16         class1
------------------------------


Command Result : 0 (Success)
```

Example with no interface specified and none have been assigned

```
lunash:>sysconf ctc class show

No class configured.


Command Result : 0 (Success)
```

Example with interface specified, but no clients assigned

```
lunash:>sysconf ctc client show -i eth0

         client          class
------------------------------
NONE
------------------------------


Command Result : 0 (Success)
```

sysconf ctc disable

Disables the Crypto Traffic Controller.

User Privileges

Users with the following privileges can perform this command:

- Admin
- Operator

Syntax

sysconf ctc disable

Example

```
lunash:>sysconf ctc disable

ctc@eth0 is disabled
Stopping ctc@eth0:                                          [  OK  ]
ctc@eth0 is stopped
ctc@eth1 is disabled
Stopping ctc@eth1:                                          [  OK  ]
ctc@eth1 is stopped


Command Result : 0 (Success)
```

sysconf ctc enable

Enables the Crypto Traffic Controller.

> **NOTE** If the CTC service is started with **sysconf ctc enable** command, then it is *on* until explicitly disabled, and it resumes, without intervention, after appliance restart/reboot.
>
> If CTC is started with **service start** command instead, and CTC enable is not in effect, then it must be manually restarted following any system restart/reboot.

User Privileges

Users with the following privileges can perform this command:

- Admin
- Operator

Syntax

sysconf ctc enable

Example

```
lunash:>sysconf ctc enable

ctc@eth0 is enabled
Stopping ctc@eth0:                                          [  OK  ]

Starting ctc@eth0:                                          [  OK  ]
ctc@eth0 is running
ctc@eth1 is enabled
Stopping ctc@eth1:                                          [  OK  ]

Starting ctc@eth1:                                          [  OK  ]
ctc@eth1 is running


Command Result : 0 (Success)
```

sysconf ctc measurement

Measure the bandwidth consumed by each client.

Use the measurement commands to track the bandwidth usage of every client communicating with Luna Network HSM 7 over a network interface. This allows the User to identify noisy clients and assign them to appropriate classes, thus restricting their bandwidth. Measurement is enabled/disabled globally and causes packets to be captured over all active interfaces running the CTC service. After enabling, the User will be able to see the minimum, maximum and average bit rate for each client over an interface. Non-registered clients are assigned to the default class.

Syntax

sysconf ctc measurement

disable
enable
show

Argument(s)	Shortcut	Description
disable	**d**	Disable measurement. See "sysconf ctc measurement disable" on the next page.
enable	**e**	Enable measurement. See "sysconf ctc measurement enable" on page 569.
show	**s**	Show measurement statistics. See "sysconf ctc measurement show" on page 570.

sysconf ctc measurement disable

Disables measurement over active network interfaces, including bond interfaces, that have CTC running as a service.

User Privileges

Users with the following privileges can perform this command:

- Admin
- Operator

Syntax

sysconf ctc measurement disable

Example

```
lunash:>sysconf ctc measurement disable


Command Result : 0 (Success)
```

sysconf ctc measurement enable

Enables measurement over active network interfaces, including bond interfaces, that have CTC running as a service. This command starts the activity of taking bandwidth usage measurements for all clients, at a measurement rate defined by -interval, and storing those measurement records in memory.

If the "sysconf ctc measurement enable" above command was run first, then "sysconf ctc measurement show" on the next page presents actual metrics, otherwise the show command displays only the 'disabled' status of the measurement feature.

For CTC measurement,

- the **-interval** value (set by "sysconf ctc measurement enable" above) defines the time span between measurements of bandwidth usage; that is, how often a measurement is taken
- The **-duration** value (set by "sysconf ctc measurement show" on the next page) defines how far back in time, from the present moment, measurement results should be captured and displayed. If the **-duration** value exceeds the length of time that measurement has been active, then just the available measurements are used.
- The content of the records depends on how many interfaces are active, and how many clients are accessing the interfaces.

> **NOTE** The archive of CTC measurement records is maintained in memory and is rotated when more space is needed. Do not count on older records being available, as they could have been rotated out. If a restart is performed, the records are wiped entirely.

User Privileges

Users with the following privileges can perform this command:

- Admin
- Operator

Syntax

sysconf ctc measurement enable -interval <measurement_interval>

Argument(s)	Shortcut	Description
-interval <measurement_interval>	**-i**	Measurement interval, in seconds. .

Example

```
lunash:>sysconf ctc measurement enable -i 5


Command Result : 0 (Success)
```

sysconf ctc measurement show

Displays the minimum, maximum and average packet rates of clients based on a span starting "-duration" seconds back from the current time, and displays the results for all clients. Measurement must be enabled to view the metrics.

If the "sysconf ctc measurement enable" on the previous page command was run first, then "sysconf ctc measurement show" above presents actual metrics, otherwise the show command displays only the 'disabled' status of the measurement feature.

For CTC measurement,

- the **-interval** value (set by "sysconf ctc measurement enable" on the previous page) defines the time span between measurements of bandwidth usage; that is, how often a measurement is taken
- The **-duration** value (set by "sysconf ctc measurement show" above) defines how far back in time, from the present moment, measurement results should be captured and displayed. If the **-duration** value exceeds the length of time that measurement has been active, then just the available measurements are used.
- The content of the records depends on how many interfaces are active, and how many clients are accessing the interfaces.

> **NOTE** The archive of CTC measurement records is maintained in memory and is rotated when more space is needed. Do not count on older records being available, as they could have been rotated out. If a restart is performed, the records are wiped entirely.

User Privileges

Users with the following privileges can perform this command:

- Admin
- Operator
- Monitor

Syntax

sysconf ctc measurement show -duration <seconds>

Argument(s)	Shortcut	Description
-duration <seconds>	**-d**	Measurement Duration In Seconds (0-99999), starting now. .

Example if ctc measure is not already enabled

```
lunash:>sysconf ctc measurement show -d 3600

Measurement status: disabled
```

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

Example if ctc measure is already enabled

```
lunash:>sysconf ctc measurement show -d 3600

Measurement status: enabled

client            min         max         avg         class
192.168.10.16     608       10800        2671        default
192.168.10.17     984       41408        8267        default


Command Result : 0 (Success)
```

sysconf ctc show

Get CTC service information.

User Privileges

Users with the following privileges can perform this command:

- Admin
- Operator
- Monitor

Syntax

sysconf ctc show

Example

```
lunash:>sysconf ctc show

   Measurement status: enabled

   Measurement interval: 44

   ctc@eth0 is disabled


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

Argument(s)	Shortcut	Description
init	**i**	Activate automatic drift adjustments. See "sysconf drift init" on the next page.
reset	**r**	Reset all drift tracking data. See "sysconf drift reset" on page 575.
set	**se**	Manually set internal drift data. See "sysconf drift set" on page 576.
startmeasure	**star**	Set the time and start measuring. See "sysconf drift startmeasure" on page 577.
status	**stat**	Display the current drift data. See "sysconf drift status" on page 578.
stopmeasure	**sto**	Stop measuring and record the drift. See "sysconf drift stopmeasure" on page 579.

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.

User Privileges

Users with the following privileges can perform this command:

> Admin

> Operator

Syntax

sysconf drift init -currentprecisetime <hh:mm:ss>

Argument(s)	Shortcut	Description
-currentprecisetime <hh:mm:ss>	**-c**	Current best precise time in hh:mm:ss format.

Example

```
lunash:>sysconf drift init -currentprecisetime 09:21:00


   Measuring drift correction data on this appliance.

   Setting the time to 09:21:00 and initializing drift correction of 2 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:  Mon Mar  6 09:21:00 EST 2017


Command Result : 0 (Success)
```

sysconf drift reset

Reset drift and internal drift tracking data.

User Privileges

Users with the following privileges can perform this command:

- Admin
- Operator

Syntax

sysconf drift reset [**-force**]

Argument(s)	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.

User Privileges

Users with the following privileges can perform this command:

- Admin
- Operator

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.

User Privileges

Users with the following privileges can perform this command:

> Admin

> Operator

Syntax

sysconf drift startmeasure -currentprecisetime <hh:mm:ss>

Argument(s)	Shortcut	Description
-currentprecisetime <hh:mm:ss>	**-c**	Current best precise time in hh:mm:ss format.

Example

```
lunash:>sysconf drift startmeasure -currentprecisetime 12:37:00


   Setting the time to 12:37:00 and recording data for drift correction mechanism.

   Current date and time set to:  Wed Mar  1 12:37:00 EST 2017


Command Result : 0 (Success)
```

sysconf drift status

Display the status of the current drift data.

User Privileges

Users with the following privileges can perform this command:

- Admin
- Operator
- Monitor

Syntax

sysconf drift status

Example

```
lunash:>sysconf drift status


   Drift measurement started on:  Wed Mar  1 12:37:00 EST 2017
   Measurement has yet to be stopped.
   Current drift correction is:   3 seconds per day
   (Note that drift correction may be manually set.)


Command Result : 0 (Success)
```

sysconf drift stopmeasure

Stops measuring and records the drift.

User Privileges

Users with the following privileges can perform this command:

- Admin
- Operator

Syntax

sysconf drift stopmeasure -currentprecisetime <hh:mm:ss>

Argument(s)	Shortcut	Description
-currentprecisetime <hh:mm:ss>	**-c**	Current best precise time in hh:mm:ss format.

Example

```
lunash:>sysconf drift stopmeasure -currentprecisetime 09:18:00


   Measuring drift correction data on this appliance.

   Storing measured drift of 2 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

license
ntls
ssh

Argument(s)	Shortcut	Description
license	**l**	Display the fingerprint for the HSM serial number. See "sysconf fingerprint license" on the next page.
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 582.
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 Network HSM 7 appliance admin interface.) See "sysconf fingerprint ssh" on page 583.

sysconf fingerprint license

This command displays the fingerprint for the HSM serial number. You need this fingerprint to obtain the license string associated with capability and partition upgrades.

User Privileges

Users with the following privileges can perform this command:

- Admin
- Operator
- Monitor

Syntax

sysconf fingerprint license

Example

```
lunash:>sysconf fingerprint license


Fingerprint for Use With Entitlement Management System
------------------------------------------------------
HSM serial #66331 : *1368R7JF78AHLF2


Command Result : 0 (Success)
```

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.

User Privileges

Users with the following privileges can perform this command:

- Admin
- Operator
- Monitor

Syntax

sysconf fingerprint ntls

Argument(s)	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

```
lunash:>sysconf fingerprint ntls


NTLS server certificate fingerprint:
AD:18:EF:C1:A3:A4:B0:59:4A:DF:8D:EB:1E:D0:3C:02:C7:A5:2D:81


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.

User Privileges

Users with the following privileges can perform this command:

- Admin
- Operator
- Monitor

Syntax

sysconf fingerprint ssh

Argument(s)	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

```
lunash:>sysconf fingerprint ssh


SSH Server Public Keys

Type   Bits Fingerprint
------------------------------------------------------------

RSA    2048 SHA256:+Rdwts5NZKmRDmRbb18PNpsh+bIhPPxSSo4PQi/7XVo
DSA    2048 SHA256:9jSwYbRCeT4vUFp/uywspL2o7Qzd81I6OhlMp1ZH0u8
ECDSA   256 SHA256:1zJtU0ErS/z9tJtQ+UrcSxiGxVZVIGIYR8XtW7Druwo


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 587 for a list of the affected commands.

Syntax

sysconf forcesologin

disable
enable
show

Argument(s)	Shortcut	Description
disable	**d**	Disable SO login enforcement. See "sysconf forceSOLogin disable" on page 586*.
enable	**e**	Enable SO login enforcement. See "sysconf forceSOLogin enable" on page 587**.
show	**s**	Display the current SO login enforcement setting. See "sysconf forceSOLogin show" on page 589.

* On successful **hsm factoryReset** or **sysconf config factoryReset** (option "all") the Luna Network HSM 7 SO Login Enforcement feature is reset to "disabled".

** If the HSM is not initialized, then the Luna Network HSM 7 SO Login Enforcement feature cannot be enabled or disabled.

Most LunaSH commands, except time- and partition-specific ones do not require the HSM Security Officer to be logged in. The Luna Network HSM 7 SO Login Enforcement option functions as follows:

> Only the SO can enable Luna Network HSM 7 SO Login Enforcement.

> When enabled, the feature verifies that the HSM SO is logged in before authorizing the operations described below.

> Only the HSM SO can disable Luna Network HSM 7 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 delete**

> **client hostip map**

> **client hostip unmap**

> **client register**

> **client revokePartition**

ntls

> **ntls bind**

> **ntls certificate monitor disable**

> **ntls certificate monitor enable**

> **ntls certificate monitor trap trigger**

> **ntls information reset**

> **ntls ipcheck disable**

> **ntls ipcheck enable**

> **ntls tcp_keepalive set**

> **ntls threads set**

> **ntls timer set**

sysconf

> **sysconf config factoryReset**

> **sysconf regenCert**

 Copyright 2001-2025 Thales Group

sysconf forceSOLogin disable

Disable SO login enforcement.

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

The HSM must be initialized before you can execute this command. See "hsm init" on page 194 for more information.

> **NOTE** The SO login enforcement setting persists backup and restore operations.

User Privileges

Users with the following privileges can perform this command:

> Admin

Syntax

sysconf forceSOLogin disable

Example

```
lunash:>sysconf forceSOLogin disable


Command Result : 0 (Success)
```

sysconf forceSOLogin enable

Enable SO login enforcement. You must be logged in as the HSM Security Officer 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.

The HSM must be initialized before you can execute this command. See "hsm init" on page 194 for more information.

User Privileges

Users with the following privileges can perform this command:

> Admin

Affected Commands

When SO login enforcement is enabled, the following commands can be executed by the HSM SO only:

Client commands

> "client assignPartition" on page 94
> "client delete" on page 95
> "client hostip map" on page 103
> "client hostip unmap" on page 105
> "client register" on page 108
> "client revokePartition" on page 110

NTLS commands

> "ntls bind" on page 378
> "ntls certificate monitor disable" on page 382
> "ntls certificate monitor enable" on page 383
> "ntls certificate monitor trap trigger" on page 385
> "ntls information reset" on page 389
> "ntls ipcheck disable" on page 393
> "ntls ipcheck enable" on page 394
> "ntls tcp_keepalive set" on page 398
> "ntls threads set" on page 402
> "ntls timer set" on page 406

Sysconf commands

> "sysconf regenCert" on page 637

Syntax

sysconf forceSOLogin enable

Example

```
lunash:>sysconf forceSOLogin enable


Command Result : 0 (Success)
```

sysconf forceSOLogin show

Display the current SO login enforcement setting.

User Privileges

Users with the following privileges can perform this command:

> Admin

Syntax

sysconf forceSOLogin show

Example

```
lunash:>sysconf forceSOLogin show

HSM Administrator Login Enforcement is NOT enabled.

Command Result : 0 (Success)
```

sysconf installCert

Installs a signed certificate file as the appliance's server certificate (renaming to and replacing **server.pem**). The certificate must be signed, base64-encoded, and PEM-formatted.

> **NOTE** This feature requires Luna Network HSM 7 Appliance Software 7.7.0.

User Privileges

Users with the following privileges can perform this command:

> Admin

Syntax

sysconf installCert <filename>

Argument(s)	Shortcut	Description
<filename>		Specifies the filename of the signed certificate.

Example

```
lunash:>sysconf installCert signed_server.pem

Attempting to install signed_server.pem:
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            15:00:00:00:1e:e5:dd:d2:71:5e:0f:0c:9a:00:00:00:00:00:1e
    Signature Algorithm: sha1WithRSAEncryption
        Issuer: CN=OTT1-TITAN-CA
        Validity
            Not Before: May 28 16:47:09 2019 GMT
            Not After : May 28 16:57:09 2020 GMT
        Subject: C=CA, ST=ON, L=Ottawa, CN=myLuna
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (2048 bit)
                Modulus:
                    00:b1:46:cc:c8:70:70:81:89:a8:22:dd:ac:ce:8f:
                    73:c2:77:29:1f:b5:a2:49:de:d3:b3:03:1c:e2:ba:
                    6a:3e:dc:ba:61:d3:88:9c:9e:74:5c:82:9e:1e:64:
                    c7:22:54:e2:6d:99:66:42:9f:e5:b8:87:d6:d4:59:
                    89:0d:88:39:7c:37:ef:42:b3:51:f2:21:5f:eb:de:
                    ed:d6:08:84:af:9c:b7:c7:55:6c:0a:46:85:d9:0c:
                    5a:4d:cf:2d:21:79:fc:83:12:c3:d5:ec:de:4c:39:
                    4d:64:ff:07:28:7e:d0:ab:ff:b7:e6:fe:41:76:8b:
                    4b:4b:b1:14:f2:42:6c:4b:92:00:6b:81:1f:30:8e:
                    48:4d:91:e6:d6:c9:0b:ba:d3:df:6f:8d:0b:bf:01:
                    89:48:74:c5:3b:ab:f2:81:d3:fa:82:c8:eb:5c:ec:
                    ca:b7:9e:bf:7a:75:9d:73:9b:be:e3:fb:f5:74:22:
```

```
                    b6:2c:8e:d3:96:c1:53:5e:3e:97:ed:b1:9f:ba:0a:
                    6f:d4:04:fe:d1:3e:d6:9d:d5:f1:e4:35:05:f9:99:
                    a8:1b:66:37:a2:94:5d:76:a3:85:c4:63:3c:26:50:
                    ef:f2:34:76:09:a5:7e:99:95:41:2a:1c:1b:d1:5f:
                    dc:26:30:08:0f:ac:85:30:b3:6e:8f:43:43:f2:fb:
                    c5:cf
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            X509v3 Subject Key Identifier:
                E8:C5:DC:3F:F4:56:5C:AF:25:48:A7:24:DB:69:64:EC:1A:FB:A1:EE
            X509v3 Authority Key Identifier:
                keyid:90:6F:CA:8F:70:28:24:E5:21:6D:01:8C:D0:64:BF:6D:D9:8E:86:D7

            X509v3 CRL Distribution Points:

                Full Name:
                  URI:file:////ott1-titan/CertEnroll/OTT1-TITAN-CA.crl

            Authority Information Access:
                CA Issuers - URI:file:////ott1-titan/CertEnroll/ott1-titan_OTT1-TITAN-CA.crt

    Signature Algorithm: sha1WithRSAEncryption
         61:84:0d:a6:a0:2b:91:4b:82:52:5f:37:58:de:36:c5:52:38:
         f6:de:a8:c4:f6:a7:69:1c:1c:ba:32:ac:0e:d7:76:aa:6c:aa:
         97:41:4d:27:9a:6e:78:0c:b9:d3:76:c7:eb:09:52:2f:a7:4f:
         af:1e:6c:25:15:db:86:2d:63:dc:76:dc:34:ba:06:c7:6e:83:
         3c:4f:c9:b9:c5:94:9a:4c:be:a9:b5:2b:d2:f3:6c:62:f5:6e:
         8c:24:34:48:94:d8:af:b8:59:d0:65:26:7c:39:a1:86:d2:a3:
         e6:16:2a:1a:dc:d6:01:cd:30:cc:75:cf:b4:a2:43:4a:45:74:
         d6:3c:88:71:69:55:59:69:8f:88:51:ad:5b:8c:11:6d:78:b4:
         a5:39:4d:89:02:c5:35:8f:c5:d5:f0:a1:e2:2b:d0:71:be:3c:
         29:32:9f:ac:36:b5:2a:27:c7:64:cf:41:7e:db:da:bb:0f:9c:
         1d:cd:b4:74:ea:9f:31:11:fa:f8:5e:f8:67:c4:5e:39:2a:48:
         b7:9d:6d:0f:45:56:9b:b3:83:35:2e:c5:d1:c4:cd:2e:c7:69:
         0c:b6:98:4b:09:02:13:7c:06:73:8b:ee:ea:ff:ff:9a:c1:88:
         d7:4b:ed:f8:71:23:78:ee:76:be:de:e8:6f:b5:27:84:8b:03:
         6b:3d:91:53

'sysconf installCert' successful. The NTLS, STC and CBS services must be (re)started before
clients can connect.
    (Successfully installed signed_server.pem as server.pem)

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 license

Access the **sysconf license** commands to manage feature licensing for capability and partition upgrades.

Syntax

sysconf license

apply
list
revoke

Argument(s)	Shortcut	Description
apply	**a**	Apply a purchased upgrade license. See "sysconf license apply" on the next page.
list	**l**	List currently-applied upgrade licenses. See "sysconf license list" on page 594.
revoke	**r**	Revoke a purchased upgrade license. See "sysconf license revoke" on page 595.

sysconf license apply

This command applies a feature license entitlement for a purchased capability or partition upgrade.

User Privileges

Users with the following privileges can perform this command:

> Admin

Syntax

sysconf license apply -filename <filename> [**-force**]

Argument(s)	Shortcut	Description
-filename <filename>	**-fi**	The name of the file containing the license string.
-force	**-fo**	Force action (no prompting for confirmation).

Example

```
lunash:>sysconf license apply -filename kcdsa.lic -force

FwUpdate3 Application Version 2.5

SafeNet Firmware/Capability Update Utility

This is a destructive capability update
Proceed prompt bypassed
Update Result :0 (Success)

Command Result : 0 (Success)
```

sysconf license list

This command lists all currently-applied feature licenses.

User Privileges

Users with the following privileges can perform this command:

- Admin
- Monitor
- Operator

Syntax

sysconf license list

Example

```
lunash:>sysconf license list


#     FEATURE                       VERSION   QUANTITY
=====================================================
1     LUNA_PARTITIONS                   1.0         10
2     LUNA_PARTITIONS                   1.0         20
3     LUNA_PARTITIONS                   1.0         10

Command Result : 0 (Success)
```

sysconf license revoke

This command revokes a previously-applied feature license entitlement for a purchased capability or partition upgrade. Revoking a license allows you to transfer an upgrade from one HSM appliance to another.

> **NOTE** This self-service feature is not available in the current release. Contact Thales Customer Care to have a license revoked.
> UPDATE: This command is removed from Luna Network HSM 7 appliance software 7.9.0 onward.

User Privileges

Users with the following privileges can perform this command:

> Admin

Syntax

sysconf license revoke -feature <index> [**-force**]

Argument(s)	Shortcut	Description
-feature <index>	**-fe**	The index number (see "sysconf license list" on the previous page) of the license you wish to revoke.
-force	**-fo**	Force action (no prompting for confirmation).

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 tail
ntpdate
ntsAuth
show
status
symmetricauth

Argument(s)	Shortcut	Description
addserver	**ad**	Add NTP Server. See "sysconf ntp addserver" on page 598.
autokeyauth	**au**	NTP Autokey Authentication. See "sysconf ntp autokeyauth" on page 600.
deleteserver	**de**	Delete NTP Server. See "sysconf ntp deleteserver" on page 607.
disable	**di**	Disable NTP Service. See "sysconf ntp disable" on page 608.
enable	**e**	Enable NTP Service. See "sysconf ntp enable" on page 609.
listservers	**li**	List Configured NTP Servers. See "sysconf ntp listservers" on page 610.
log tail	**lo t**	NTP Log Command. See "sysconf ntp log tail" on page 611.
ntpdate	**n**	Set date and time using NTP. See "sysconf ntp ntpdate" on page 612.
ntsAuth	**n**	NTP NTS Authentication. See "sysconf ntp ntsAuth cert" on page 616.
show	**sh**	Show NTP Configuration. See "sysconf ntp show" on page 613.
status	**st**	Get NTP Service Status. See "sysconf ntp status" on page 614.

 Copyright 2001-2025 Thales Group

Argument(s)	Shortcut	Description
symmetricauth	**sy**	NTP Symmetric Key Authentication. See "sysconf ntp symmetricauth" on page 619.

sysconf ntp addserver

Add an NTP server. NTP will automatically synchronize with the highest-stratum server you add. If none of these servers are accessible, NTP will synchronize with the local clock, and may be subject to drift.

A DNS name server must be configured if you add an NTP server by hostname.

User Privileges

Users with the following privileges can perform this command:

- Admin
- Operator

Syntax

sysconf ntp addserver <hostname_or_ipaddress> [**-autokey** | **-key** <keyid>] [**-burst**] [**-iburst**] [**-prefer**] [**-version** <version>]

Argument(s)	Shortcut	Description
<hostname_or_ipaddress>		Specifies the hostname or IP address of the NTP Server.
-autokey	**-a**	Send and receive packets authenticated by the AutoKey scheme (not used with **-key** <keyid>).
-burst	**-b**	Send multiple packets when the server is reachable.
-iburst	**-i**	Send out bursts of 8 packets when the server is unreachable.
-key	**-k**	Specifies the NTP Authentication key ID (not used with AutoKey) **Range:** 1 to 65535
-prefer	**-p**	Set this server as the preferred server.
-version <version>	**-v**	Specifies the NTP version **Valid values**: 3 or 4

> **NOTE** To reduce the synchronization time, specify the **-iburst** option when adding an NTP server.
>
> lunash:> **sysconf ntp addserver** <hostname/IP> **-iburst**

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
```

```
Stopping 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  1310  9024   yes   yes  none    reject   reachable  2
  2  1311  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 authentication.

These autokeyAuth commands are removed from Luna Network HSM 7 appliance software version 7.8.5 onward. If your prior configuration did not already include a server using ntp authentication, your ntp configuration remains as-is. If you had configured an ntp server that used authentication, you will need to reconfigure. Use nts via the "sysconf ntp ntsAuth cert" on page 616 commands.

When you add a trusted NTP server, Luna Network HSM 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

Argument(s)	Shortcut	Description
clear	**c**	Delete all keys and certificates. See "sysconf ntp autokeyAuth clear" on the next page.
generate	**g**	Generate client keys and certificates (required to use AutoKey). See "sysconf ntp autokeyAuth generate" on page 602.
install	**i**	Install Autokey Identity Scheme IFF|GQ|MV (optional). See "sysconf ntp autokeyAuth install" on page 604.
list	**l**	Show Autokey keys and certificates. See "sysconf ntp autokeyAuth list" on page 605.
update	**u**	Update client certificates (a certificate usually has a ttl of one year, after which you must update to renew). See "sysconf ntp autokeyAuth update" on page 606.

sysconf ntp autokeyAuth clear

Delete all Autokey authentication keys and certificates.

These autokeyAuth commands are removed from Luna Network HSM 7 appliance software version 7.8.5 onward. If your prior configuration did not already include a server using ntp authentication, your ntp configuration remains as-is. If you had configured an ntp server that used authentication, you will need to reconfigure. Use nts via the "sysconf ntp ntsAuth cert" on page 616 commands.

User Privileges

Users with the following privileges can perform this command:

- Admin
- Operator

Syntax

sysconf ntp autokeyAuth clear [**-force**]

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

Example

```
lunash:>sysconf ntp autokeyAuth clear



WARNING !!  This command deletes all NTP Autokey keys and certificates.
If you are sure that you wish to proceed, then type 'proceed', otherwise type 'quit'.

> proceed
Proceeding...
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.

These autokeyAuth commands are removed from Luna Network HSM 7 appliance software version 7.8.5 onward. If your prior configuration did not already include a server using ntp authentication, your ntp configuration remains as-is. If you had configured an ntp server that used authentication, you will need to reconfigure. Use nts via the "sysconf ntp ntsAuth cert" on page 616 commands.

User Privileges

Users with the following privileges can perform this command:

> Admin

> Operator

Syntax

sysconf ntp autokeyAuth generate [**-certalg** <certalg>] [**-modulus** <modulus>] [**-signalg** <signalg>] [**-password** <ntpkey>]

Argument(s)	Shortcut	Description
-certalg <certalg>	**-c**	NTP Certificate Algorithm. **Valid values:** RSA-SHA1, DSA-SHA1 **Default:** RSA-SHA1
-modulus <modulus>	**-m**	NTP Modulus Size. Only 2048-bit keys are currently supported, so it is not necessary to include this option. **Default:** 2048
-password <ntpkey>	**-p**	NTP Symmetric Key Value
-signalg <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:>sysc 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 OpenSSL 1.0.1e-fips 11 Feb 2013
Using host sadoc78 group sadoc78
Generating RSA keys (2048 bits)...
RSA 0 43 77     1 2 6                          3 1 2
Generating new host file and link
ntpkey_host_sadoc78->ntpkey_RSAhost_sadoc78.3699032190
Generating RSA keys (2048 bits)...
RSA 0 2 974     1 2 12                         3 1 4
Generating new sign file and link
ntpkey_sign_sadoc78->ntpkey_RSAsign_sadoc78.3699032190
Generating new certificate sadoc78 RSA-SHA1
X509v3 Basic Constraints: critical,CA:TRUE
X509v3 Key Usage: digitalSignature,keyCertSign
Generating new cert file and link
ntpkey_cert_sadoc78->ntpkey_RSA-SHA1cert_sadoc78.3699032190

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.

These autokeyAuth commands are removed from Luna Network HSM 7 appliance software version 7.8.5 onward. If your prior configuration did not already include a server using ntp authentication, your ntp configuration remains as-is. If you had configured an ntp server that used authentication, you will need to reconfigure. Use nts via the "sysconf ntp ntsAuth cert" on page 616 commands.

User Privileges

Users with the following privileges can perform this command:

> Admin

> Operator

Syntax

sysconf ntp autokeyAuth install -idscheme <identityscheme> **-keyfile** <filename>

Argument(s)	Shortcut	Description
-idscheme <identityscheme>	**-i**	Specifies the NTP AutoKey Identity Scheme to install. **Valid values:** IFF, GQ, or MV
-keyfile <filename>	**-k**	Specifies the keyfile name.

sysconf ntp autokeyAuth list

List the NTP Autokey authentication keys.

These autokeyAuth commands are removed from Luna Network HSM 7 appliance software version 7.8.5 onward. If your prior configuration did not already include a server using ntp authentication, your ntp configuration remains as-is. If you had configured an ntp server that used authentication, you will need to reconfigure. Use nts via the "sysconf ntp ntsAuth cert" on page 616 commands.

User Privileges

Users with the following privileges can perform this command:

- Admin
- Operator

Syntax

sysconf ntp autokeyAuth list

Example

```
lunash:>sysc ntp autokeyAuth list


=========== Installed keys and certificates: ====================
ntpkey_RSA-SHA1cert_sadoc78.3699032190
ntpkey_cert_sadoc78 -> ntpkey_RSA-SHA1cert_sadoc78.3699032190
ntpkey_RSAsign_sadoc78.3699032190
ntpkey_sign_sadoc78 -> ntpkey_RSAsign_sadoc78.3699032190
ntpkey_RSAhost_sadoc78.3699032190
ntpkey_host_sadoc78 -> ntpkey_RSAhost_sadoc78.3699032190

=================== Certificate details: ========================
Certificate File: ntpkey_RSA-SHA1cert_sadoc78.3699032190
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number: 3699032190 (0xdc7ac07e)
    Signature Algorithm: sha1WithRSAEncryption
        Issuer: CN=sadoc78
        Validity
            Not Before: Mar 20 20:56:30 2017 GMT
            Not After : Mar 20 20:56:30 2018 GMT
        Subject: CN=sadoc78
        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.

These autokeyAuth commands are removed from Luna Network HSM 7 appliance software version 7.8.5 onward. If your prior configuration did not already include a server using ntp authentication, your ntp configuration remains as-is. If you had configured an ntp server that used authentication, you will need to reconfigure. Use nts via the "sysconf ntp ntsAuth cert" on page 616 commands.

User Privileges

Users with the following privileges can perform this command:

- Admin
- Operator

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 OpenSSL 1.0.1e-fips 11 Feb 2013
Using host sadoc78 group sadoc78
Using host key ntpkey_RSAhost_sadoc78.3699032190
Using sign key ntpkey_RSAsign_sadoc78.3699032190
Generating new certificate sadoc78 RSA-SHA1
X509v3 Basic Constraints: critical,CA:TRUE
X509v3 Key Usage: digitalSignature,keyCertSign
Generating new cert file and link
ntpkey_cert_sadoc78->ntpkey_RSA-SHA1cert_sadoc78.3699032190

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.

User Privileges

Users with the following privileges can perform this command:

- Admin
- Operator

Syntax

sysconf ntp deleteserver <hostname_or_ipaddress>

Argument(s)	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 time.nrc.ca deleted.
Stopping ntpd:                                     [  OK  ]

Starting ntpd:                                     [  OK  ]

Command Result : 0 (Success)
```

sysconf ntp disable

Disable and stop the NTP service.

User Privileges

Users with the following privileges can perform this command:

- Admin
- Operator

Syntax

sysconf ntp disable

Example

```
lunash:>sysconf ntp disable

NTP is disabled
Stopping ntpd:                                             [  OK  ]
NTP is stopped

Command Result : 0 (Success)
```

sysconf ntp enable

Enable and start the NTP service.

This command enables the service after it has been stopped, such as with **sysconf ntp disable**. This command is normally not needed with **sysconf ntp addserver**, which includes restarting of the NTP service.

User Privileges

Users with the following privileges can perform this command:

- Admin
- Operator

Syntax

sysconf ntp enable

Example

```
lunash:>sysconf ntp enable

NTP is enabled
Stopping 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  4000  9024   yes   yes  none    reject   reachable  2
  2  4001  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.

User Privileges

Users with the following privileges can perform this command:

- Admin
- Operator
- Monitor

Syntax

sysconf ntp listservers

Example

```
lunash:> sysconf ntp listservers

=================================================================
NTP Servers:
server time.nrc.ca
=================================================================

Command Result : 0 (Success)
```

sysconf ntp log tail

Display the NTP logs.

> **NOTE** This command has been removed from Luna Appliance Software 7.9.0 and newer, and is deprecated in previous releases. To display the NTP logs, use lunash:> "syslog tail" on page 762 **-logname ntp**.

User Privileges

Users with the following privileges can perform this command:

- Admin
- Operator

Syntax

sysconf ntp log tail [**-entries** <logentries>]

Argument(s)	Shortcut	Description
-entries <logentries>	**-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
20 Mar 00:08:54 ntpd[842]: 0.0.0.0 064d 0d kern PPS no signal
20 Mar 00:43:48 ntpd[842]: 0.0.0.0 065d 0d kern PPS no signal
20 Mar 01:28:25 ntpd[842]: 0.0.0.0 066d 0d kern PPS no signal
20 Mar 02:03:54 ntpd[842]: 0.0.0.0 067d 0d kern PPS no signal
20 Mar 02:39:02 ntpd[842]: 0.0.0.0 068d 0d kern PPS no signal
20 Mar 03:14:38 ntpd[842]: 0.0.0.0 069d 0d kern PPS no signal
20 Mar 03:49:00 ntpd[842]: 0.0.0.0 06ad 0d kern PPS no signal
20 Mar 04:41:50 ntpd[842]: 0.0.0.0 06bd 0d kern PPS no signal
20 Mar 05:33:49 ntpd[842]: 0.0.0.0 06cd 0d kern PPS no signal
20 Mar 06:27:09 ntpd[842]: 0.0.0.0 06dd 0d kern PPS no signal
20 Mar 07:02:59 ntpd[842]: 0.0.0.0 06ed 0d kern PPS no signal
20 Mar 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.

User Privileges

Users with the following privileges can perform this command:

- Admin
- Operator

Syntax

sysconf ntp ntpdate <hostname_or_ipaddress> [**-key** <keyid>] [**-version** <version>]

Argument(s)	Shortcut	Description
<hostname_or_ipaddress>		Specifies the hostname or IP address of the NTP server.
-key <keyid>	**-k**	NTP Authentication Keyid **Range:** 1 to 65535
-version <version>	**-v**	Specifies the NTP version **Valid values:** 3 or 4

Example

```
lunash:>sysconf ntp ntpdate time.nrc.ca


This command sets the date and time using ntp server "time.nrc.ca" if NTP daemon is not
running.

Current time before running ntpdate: Mon Mar 20 17:15:20 EDT 2017
Current time after running ntpdate: Mon Mar 20 17:15:35 EDT 2017

Command Result : 0 (Success)
```

sysconf ntp show

Display the NTP configuration.

User Privileges

Users with the following privileges can perform this command:

- Admin
- Operator
- Monitor

Syntax

sysconf ntp show

Example

```
lunash:>sysconf ntp show

---------------- NTP Version ----------------------------------------
ntpq 4.2.8p8@1.3265-o Wed Nov  9 19:44:21 UTC 2016 (1)
==================== NTP Configuration ==============================
restrict default kod limited nomodify notrap nopeer noquery ignore
restrict -6 default kod limited nomodify notrap nopeer noquery ignore
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.

Refer to "Parameters" below for a description of the parameters that are displayed after running **sysconf ntp status**.

> **TIP** The command **sysconf ntp status** sends packets to the configured NTP servers. The response time from the server using unreliable UDP protocol, especially over large distances, is random due to the network delay, server availability etc. If no response is received from the server, the command eventually times out after some attempts; this causes a ‘random’ delay in the command output. Five-to-ten seconds seems to be the timeout period if no response is received from the server. The default timeout is 5000 milliseconds. Note that since the command retries each query once after a timeout, the total waiting time for a timeout will be twice the timeout value set. For these reasons, you might see the command output begin, then pause for several seconds, before resuming. In other network configurations, and with "nearby" fast-responding NTP servers configured, you might never notice a pause.

> **NOTE** It can take a few minutes to synchronize the NTP server. Checking immediately might return an error.

Parameters

The following parameters are displayed after running **sysconf ntp status**:

Parameter	Description
remote	Name of the remote NTP server. A plus (+) before an NTP server name means that it is a good candidate for synchronization. More than one NTP server could be a good candidate. An asterisk (*) before an NTP server name means that the it is 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.
st	Stratum of the remote peer.
t	The type of peer. Can be one of the following: > local > unicast > multicast > broadcast
when	Time the last packet was received (in seconds).
poll	How frequently to query the server (in seconds).

Parameter	Description
reach	Octal bitmask of success or failure of the last 8 queries.
delay	Network round trip time (in milliseconds).
offset	Difference between the local clock and remote clock (in milliseconds)
jitter	Difference of successive time values from the server.

User Privileges

Users with the following privileges can perform this command:

- Admin
- Operator
- Monitor

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 ntsAuth cert

Access commands that allow you to manage Network Time Security for NTP. See also NTS (Network Time Security).

Syntax

sysconf ntp ntsAuth cert

add
clear
delete
list

Argument(s)	Shortcut	Description
add	**a**	Add a certificate for NTS authentication. See "sysconf ntp ntsAuth cert add" below.
clear	**c**	Clear all NTS registered certificates. See "sysconf ntp ntsAuth cert clear" on the next page.
delete	**d**	Delete a certificate for NTS authentication. See "sysconf ntp ntsAuth cert delete" on the next page.
list	**l**	List certificates registered for NTS servers. See "sysconf ntp ntsAuth cert list" on page 618.

sysconf ntp ntsAuth cert add

Adds certificate to trust store for NTS authentication. See also NTS (Network Time Security).

User Privileges

Users with the following privileges can perform this command:

> Admin

> Operator

Syntax

sysconf ntp ntsAuth cert add <filename>

Argument(s)	Shortcut	Description
.	.<filename>	Adds certificate for NTS authentication.

sysconf ntp ntsAuth cert clear

Clears all NTS registered certificates. See also NTS (Network Time Security).

User Privileges

Users with the following privileges can perform this command:

> Admin

> Operator

Syntax

sysconf ntp ntsAuth cert clear [**-force**]

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

Example

```
lunash:>sysconf ntp ntsAuth cert clear


WARNING !!  This command deletes all NTS registered certificates.
If you are sure that you wish to proceed, then type 'proceed', otherwise type 'quit'.

> proceed
Proceeding...


Command Result : 0 (Success)
```

sysconf ntp ntsAuth cert delete

Deletes certificate from trust store for NTS authentication. See also NTS (Network Time Security).

User Privileges

Users with the following privileges can perform this command:

> Admin

> Operator

Syntax

sysconf ntp ntsAuth cert delete <filename> **-force**

Argument(s)	Shortcut	Description
.	. <filename>	Deletes certificate for NTS authentication.
-force	**-f**	Force the action without prompting.

Example

```
lunash:>sysconf ntp ntsAuth cert delete myntscertfile

myntscertfile deleted

Command Result : 0 (Success)
```

sysconf ntp ntsAuth cert list

Lists certificates registered for NTS server. See also NTS (Network Time Security).

User Privileges

Users with the following privileges can perform this command:

- Admin
- Operator
- Monitor

Syntax

sysconf ntp ntsAuth cert list

Example

```
lunash:>sysconf ntp ntsAuth cert list

No certificates registered.

Command Result : 0 (Success)
```

sysconf ntp symmetricauth

Access commands that allow you to manage NTP symmetric keys.

Syntax

sysconf ntp symmetricauth

key
trustedkeys

Argument(s)	Shortcut	Description
key	**k**	Manage symmetric keys. See "sysconf ntp symmetricauth key" on the next page.
trustedkeys	**t**	Manage trusted symmetric keys. See "sysconf ntp symmetricauth trustedkeys" on page 626.

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

Argument(s)	Shortcut	Description
add	**a**	Add a symmetric authentication key. See "sysconf ntp symmetricAuth key add" on the next page.
clear	**c**	Delete all NTP symmetric authentication keys. See "sysconf ntp symmetricAuth key clear" on page 623.
delete	**d**	Delete an NTP symmetric authentication key. See "sysconf ntp symmetricAuth key delete" on page 624.
list	**l**	List all of the currently configured NTP symmetric keys. See "sysconf ntp symmetricAuth key list" on page 625.

sysconf ntp symmetricAuth key add

Add an NTP symmetric authentication key.

User Privileges

Users with the following privileges can perform this command:

> Admin

> Operator

Syntax

Syntax from Luna Network HSM 7 appliance version 7.9.0 onward

sysconf ntp symmetricAuth key add -id <keyid> **-algorithm** <keytype> **-value** <ntpkey>

Argument(s)	Shortcut	Description
-id <keyid>	**-i**	Specifies the key ID. **Range:** 1 to 65535
-algorithm <keytype>	**-a**	Specify one of SHA256,SHA384,SHA512,SHA3-224,SHA3-256,SHA3-384,SHA3-512,AES128,AES256)
-length <ntpkey>	**-l**	Specifies the key length (128-4096).

Syntax prior to Luna Network HSM 7 appliance version 7.9.0

sysconf ntp symmetricAuth key add -id <keyid> **-type** <keytype> **-value** <ntpkey>

Argument(s)	Shortcut	Description
-id <keyid>	**-i**	Specifies the key ID. **Range:** 1 to 65535
-type <keytype>	**-t**	Specifies the key type. **Valid values**: M,S,A,N From www.ntp.org: > An **A** key is just a sequence of up to eight ASCII characters (some characters with special meaning can't be used). > An **M** key is a sequence of up to 31 ASCII characters. > An **S** key is a 64 bit value with the low order bit of each byte being odd parity. > An **N** key is a 64 bit value with the high order bit of each byte being odd parity.

Argument(s)	Shortcut	Description
-value <ntpkey>	**-v**	Specifies the key value.

sysconf ntp symmetricAuth key clear

Delete all symmetric Authentication Keys.

User Privileges

Users with the following privileges can perform this command:

- Admin
- Operator

Syntax

sysconf ntp symmetricAuth key clear [**-force**]

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

Example

```
lunash:>sysconf ntp symmetricAuth key clear



WARNING !!  This command deletes all NTP symmetric keys.
If you are sure that you wish to proceed, then type 'proceed', otherwise type 'quit'.

> proceed
Proceeding...
You must restart NTP for the changes to take effect.

Command Result : 0 (Success)
```

sysconf ntp symmetricAuth key delete

Delete a single-named authentication key from the appliance's list.

User Privileges

Users with the following privileges can perform this command:

- Admin
- Operator

Syntax

sysconf ntp symmetricAuth key delete -id <keyid> **-force**

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

User Privileges

Users with the following privileges can perform this command:

- Admin
- Operator
- Monitor

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

Argument(s)	Shortcut	Description
add	**a**	Add a symmetric NTP authentication trusted key. See "sysconf ntp symmetricAuth trustedKeys add" on the next page.
clear	**c**	Delete all symmetric NTP authentication trusted keys. See "sysconf ntp symmetricAuth trustedKeys clear" on page 628.
delete	**d**	Delete an symmetric NTP authentication trusted key. See "sysconf ntp symmetricAuth trustedKeys delete" on page 629.
list	**l**	List all of the currently configured symmetric trusted NTP keys. See "sysconf ntp symmetricAuth trustedKeys list" on page 630.

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.

User Privileges

Users with the following privileges can perform this command:

- Admin
- Operator

Syntax

sysconf ntp symmetricAuth trustedKeys add -id <keyid>

Argument(s)	Shortcut	Description
-id <keyid>	**-i**	Specifies the ID of the key to add. **Range:** 1 to 65535

sysconf ntp symmetricAuth trustedKeys clear

Delete all Trusted Authentication Keys.

User Privileges

Users with the following privileges can perform this command:

> Admin

> Operator

Syntax

sysconf ntp symmetricAuth trustedKeys clear [**-force**]

Argument(s)	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.

User Privileges

Users with the following privileges can perform this command:

> Admin

> Operator

Syntax

sysconf ntp symmetricAuth trustedKeys delete -id <keyid> [**-force**]

Argument(s)	Shortcut	Description
-id <keyid>	**-i**	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.

User Privileges

Users with the following privileges can perform this command:

- Admin
- Operator
- Monitor

Syntax

sysconf ntp symmetricAuth trustedKeys list

Example

```
lunash:>sysconf ntp symmetricAuth trustedKeys list

current trustedkeys:

Command Result : 0 (Success)
```

sysconf radius

Manage the appliance-side configuration of appliance-user authentication via a RADIUS server.

Syntax

sysconf radius

addserver
deleteserver
disable
enable
show

Argument(s)	Shortcut	Description
addserver	**a**	Add a RADIUS server. See "sysconf radius addServer" on the next page.
deleteserver	**de**	Remove a RADIUS server. See "sysconf radius deleteServer" on page 633.
disable	**di**	Disable RADIUS for SSH. See "sysconf radius disable" on page 634.
enable	**e**	Enable RADIUS for SSH. See "sysconf radius enable" on page 635.
show	**s**	Show RADIUS configuration. See "sysconf radius show" on page 636.

For RADIUS configuration instructions, see Configuring RADIUS Authentication.

sysconf radius addServer

Identify a RADIUS server to the Luna Network HSM 7, specifying the server's hostname or IP.

> **NOTE** RADIUS must already be enabled, by means of command **sysconf radius enable**, before you can run this command to add a RADIUS server. In addition to enabling RADIUS, you must run the **sysconf radius addServer** command to identify the RADIUS server, as well as the **user radiusAdd** and **user role add** commands to create a user on this appliance with the desired name, and identify that role as requiring RADIUS to authenticate.

User Privileges

Users with the following privileges can perform this command:

> Admin

Syntax

sysconf radius addServer -server <hosthame> **-port** <port> **-timeout** <seconds>

Argument(s)	Shortcut	Description
-server <hosthame>	**-s**	Host name
-port <port>	**-p**	Network port **Range:** 0 to 65535
-timeout <seconds>	**-t**	Time in seconds **Range:** 1 to 300

Example

```
lunash:>sysconf radius addServer -server 192.20.15.182 -port 1812 -timeout 60


Enter the server secret:
Re-enter the server secret:


Command Result : 0 (Success)
```

sysconf radius deleteServer

Remove a RADIUS server from the Luna Network HSM 7, specifying the server's hostname or IP.

> **NOTE** This command can be run only while RADIUS is enabled on the Luna Network HSM 7.

User Privileges

Users with the following privileges can perform this command:

> Admin

Syntax

sysconf radius deleteServer -server <hostname>

Argument(s)	Shortcut	Description
-server <hostname>	**-s**	Host name of server to be deleted.

Example

```
lunash:>sysconf radius deleteServer -server 192.20.15.182


Command Result : 0 (Success)
```

sysconf radius disable

Disable RADIUS service on Luna Network HSM 7.

User Privileges

Users with the following privileges can perform this command:

> Admin

Syntax

sysconf radius disable

Example

```
lunash:>sysconf radius disable


Command Result : 0 (Success)
```

sysconf radius enable

Enable RADIUS service on Luna Network HSM 7.

> **NOTE** In addition to enabling RADIUS, you must run the **sysconf radius addserver** command to identify the RADIUS server, as well as the **user role radiusadd** and **user role add** commands to create a user on this appliance with the desired name, and identify that role as requiring RADIUS to authenticate.

User Privileges

Users with the following privileges can perform this command:

> Admin

Syntax

sysconf radius enable

Example

```
lunash:>sysconf radius enable


Command Result : 0 (Success)
```

sysconf radius show

Show the current RADIUS configuration and status.

User Privileges

Users with the following privileges can perform this command:

> Admin

Syntax

sysconf radius show

Example

```
lunash:>sysconf radius show

RADIUS for SSH is enabled with the following deployed servers:

                                                     server:port     timeout
                                                -------------  ----------
                                           192.20.15.182:1812          60



Command Result : 0 (Success)
```

sysconf regenCert

Generate or regenerate the Luna Network HSM 7 server certificate used for NTLS and save it to the appliance file system. Include the **-csr** option if you plan to have the resulting certificate signed by a Certificate Authority (CA).

This command stores the resulting private and public keys on the file system (hard disk) inside the Luna Network HSM 7 appliance.

User Privileges

Users with the following privileges can perform this command:

> Admin

Syntax

sysconf regenCert [<IPaddress>] [**-keytype** <keytype>] [**-keysize** <keysize>] [**-curve** <curve>] [**-csr**] [**-startdate** <startdate>] [**-days** <days>] [**-country** <country>] [**-state** <state>] [**-location** <location>] [**-organization** <organization>] [**-orgunit** <unit>] [**-email** <email_address>] [**-san** <SAN>] [**-force**]

Argument(s)	Shortcut	Description
<IPaddress>		Specifies the IP address to set as the CN of the server's NTLS certificate. If not specified, the CN will be the hostname of the Luna Network HSM 7 appliance, as specified by the **network hostname** command. See "network hostname" on page 325 for more information.
-country <country>	**-co**	The country where the client computer resides. This option accepts the following characters: `/0123456789ABCDEFGHIJKLMNOPQRSTUVWXYZ_abcdefghijklmnopqrstuvwxyz`
-csr	**-cs**	Create a Certificate Signing Request (CSR), a private key and unsigned client certificate. The certificate must be signed by a third party before being used to authenticate the Luna Network HSM 7. **NOTE** This option requires Luna Appliance Software 7.7.0 or newer.
-curve	**-cu**	Elliptic Curve name (ECC only): **Options:** secp256k1,secp384r1,secp521r1,prime256v1 **Default:** secp384r1) **NOTE** This option requires Luna Appliance Software 7.8.4 or newer.

Argument(s)	Shortcut	Description
-days <days>	**-d**	Specifies the number of days for which the new certificate will remain valid, starting on <startdate>. **Range:** 1-3653 **Default:** 3653 (10 years)
-email <email_address>	**-e**	An email address to contact the certificate creator. This option accepts the following characters: `@.0123456789ABCDEFGHIJKLMNOPQRSTUVWXYZ_abcdefghijklmnopqrstuvwxyz`
-force	**-f**	Force the action without prompting.
-keysize	**-keys**	RSA key size (RSA only): options are 2048,3072,4096 (default is 2048) **NOTE** This option requires Luna Appliance Software 7.8.4 or newer.
-keytype	**-keyt**	Key type: options are rsa, ecc, or ed25519 (default is RSA) **NOTE** This option requires Luna Appliance Software 7.8.4 or newer.
-location <location>	**-l**	The locality where the client computer resides. This option accepts the following characters: `/0123456789ABCDEFGHIJKLMNOPQRSTUVWXYZ_abcdefghijklmnopqrstuvwxyz`
-organization <organization>	**-orga**	The name of the organization that owns the client computer. This option accepts the following characters: `/-.:0123456789ABCDEFGHIJKLMNOPQRSTUVWXYZ_abcdefghijklmnopqrstuvwxyz`
-orgunit <unit>	**-orgu**	The business unit or department that owns the client computer. This option accepts the following characters: `/0123456789ABCDEFGHIJKLMNOPQRSTUVWXYZ_abcdefghijklmnopqrstuvwxyz`
-san <SAN>	**-sa**	Subject Alternate Names (SAN) for this appliance. This field must be set if clients intend to use IP/hostname verification. Specify a list of comma-separated IPs and domains associated with the appliance. This option accepts the following characters: `:.,0123456789ABCDEFGHIJKLMNOPQRSTUVWXYZ_abcdefghijklmnopqrstuvwxyz` Example: **-san IP:1.2.3.4,DNS:abc.com,**...

Argument(s)	Shortcut	Description
-startdate <startdate>	**-s**	Specifies the starting date upon which the certificate becomes valid, in the format YYYYMMDD. The default is 24 hours ago, to eliminate possible time zone mismatch issues if you need the certificate to be valid immediately anywhere in the world.
-state <state>	**-stat**	The state where the client computer resides. This option accepts the following characters: `/0123456789ABCDEFGHIJKLMNOPQRSTUVWXYZ_ abcdefghijklmnopqrstuvwxyz`

Example (prior to appliance software 7.8.4)

```
lunash:>sysconf regenCert


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. The NTLS, STC and CBS services 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)
```

Example (7.8.4 and newer)

```
lunash:>sysconf regenCert -keytype rsa -keysize 3072


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. The NTLS, STC and CBS services must be (re)started before
clients can connect.
                                WARNING: for -csr option, please install the signed cert before
restarting NTLS

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 reimage

Access commands that restore the appliance to the pre-installed baseline software image and the HSM firmware to the baseline version.

> **CAUTION!** Re-imaging to an older appliance software version might expose vulnerabilities that were fixed in newer releases.

User Privileges

Users with the following privileges can perform this command:

> Admin

Syntax

sysconf reimage

start
tarlog

Argument(s)	Shortcut	Description
start	**s**	Re-image the appliance and the HSM to the pre-installed baseline software/firmware versions. See "sysconf reimage start" on the next page.
tarlog	**t**	Retrieve the archived log file for the most recent re-imaging procedure. See "sysconf reimage tarlog" on page 646.

sysconf reimage start

Restore the appliance and the HSM to the pre-installed baseline software/firmware versions.

The baseline versions are:

> Luna Network HSM 7 Appliance Software 7.2.0

> Luna HSM Firmware 7.0.3

If you have installed the Re-Image Software 7.7.1 and Firmware 7.3.3 Patch, the baseline versions are:

> Luna Network HSM 7 Appliance Software 7.7.1

> Luna HSM Firmware 7.3.3

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

CAUTION! This command is destructive; all partitions and cryptographic objects will be destroyed, and the HSM must be re-initialized. The operation takes 15-20 minutes, and the appliance reboots twice. Do not reboot the appliance manually during this time. Ensure that you have a power backup in place before re-imaging the appliance.

Re-imaging to an older appliance software version might expose vulnerabilities that were fixed in newer releases.

Using Luna Appliance Software 7.9.0 or newer, the appliance re-image operation deletes all bonded interfaces and supporting network configurations. Those must be reconfigured, if they are needed, after the re-image operation is complete. If you are using bonded interfaces, run lunash:> "sysconf reimage start" above via a serial connection or a physical network interface (**eth0**/**eth1**/**eth2**/**eth3**) to avoid losing contact with the Luna Network HSM 7.

NOTE This feature requires that the Luna Network HSM 7 has been upgraded to minimum Luna HSM Firmware 7.3.0 and Luna Network HSM 7 Appliance Software 7.3.0 at one point.

The Appliance Re-image feature is not supported on HSMs that use Functionality Modules. If you have ever enabled **HSM policy 50: Allow Functionality Modules**, even if the policy is currently disabled, you cannot re-image the HSM appliance. See FM Deployment Constraints for details.

User Privileges

Users with the following privileges can perform this command:

> Admin

Syntax

sysconf reimage start [**-base**]

Argument(s)	Shortcut	Description
-base	**-b**	Restore the Luna Network HSM 7 to its original capability settings. With this option included, licenses such as partition packs are not preserved after the appliance re-image process. Purchased update licenses are still valid, and you can re-apply them (or apply them to a different Luna Network HSM 7) using the Thales Licensing Portal.

Example using Luna Appliance Software 7.9.0 or newer

```
lunash:>sysconf reimage start

   The HSM Administrator is logged in. Proceeding...

   To remove audit logs from the HSM, you must configure the Audit Logs feature.
   If you do not configure Audit Logs before the Appliance Re-image, the existing
   audit log history will be retained in the HSM.

   Type 'proceed' to continue the re-imaging process without configuring Audit Logs, or 'quit'
to cancel.
   > proceed
   Proceeding...

   WARNING: This operation will revert the Luna Network HSM to the baseline of software 7.2.0-
220 with firmware 7.0.3 !!!

         (1) This is a destructive operation that erases all partitions and key material.
         (2) Ensure that you have a valid backup of all your partitions.
         (3) After completion, you must re-initialize the HSM.
         (4) After completion, remote PED must be re-connected.
         (5) This operation takes 15-20 minutes. Make sure you have power backup in place.
         (6) This operation will delete all bonded interfaces and supporting network
configurations.
         (7) Access to the appliance will be unavailable. DO NOT restart the appliance during
this time.
         (8) The operation erases all appliance logs.
         (9) The Appliance Re-image operation will generate additional audit logs in the HSM.
         (10) The Appliance Re-image procedure includes multiple appliance reboot.
         (11) This operation CANNOT be undone.

   Type 'proceed' to continue, or 'quit' to cancel.
   > proceed
   Proceeding...

   Step 1 of 7: Backing up the appliance support information
   ...
   Done
   Step 2 of 7: Setting up the environment for the Appliance Re-image.
   ...
   Done
   Step 3 of 7: Extracting the packages
   ...
   This step may take a few minutes... \
   Done
```

```
   Step 4 of 7: Preparing the Luna Network HSM baseline installation scripts
   ...
   Done
   Step 5 of 7: Updating to the Luna Network HSM baseline firmware
   ...
   This step may take a few minutes... -
   Step 5.1 of 7: Prepare for Luna Network HSM licenses installation
   ...
   This step may take a few minutes... /
   Done
   Step 6 of 7: Installing Luna Network HSM Base licenses
   ...
   This step may take a few minutes... -

   Done
   Step 7 of 7: Factory reset Luna Network HSM
   ...
   The Luna Network HSM with baseline firmware version has been factory reset.
   Done

The Luna Network HSM  will restart multiple times to complete the baseline installation.
This process could take up to 15 more minutes beyond initial reboot.
Please wait for the operation to complete as interrupting the process could have adverse
effects.

Command Result : 0 (Success)
```

Example using Luna Appliance Software 7.8.5 or older

```
lunash:>sysconf reimage start

   The HSM Administrator is logged in. Proceeding...

   To remove audit logs from the HSM, you must configure the Audit Logs feature.
   If you do not configure Audit Logs before re-imaging, the existing audit log history will be
retained in the HSM.

   Type 'proceed' to continue the re-imaging process without configuring Audit Logs, or 'quit'
to cancel.
   > proceed
   Proceeding...

   WARNING: This operation will revert the Luna Network HSM to the baseline of software 7.2.0-
220 with firmware 7.0.3 !!!

         (1) This is a destructive operation that erases all partitions and key material.
         (2) Ensure that you have a valid backup of all your partitions.
         (3) After completion, you must re-initialize the HSM.
         (4) After completion, remote PED must be re-connected.
         (5) This operation takes 15-20 minutes. Make sure you have power backup in place.
         (6) Access to the appliance will be unavailable. DO NOT restart the appliance during
this time.
         (7) The operation erases all appliance logs.
         (8) The re-imaging operation will generate additional audit logs in the HSM.
         (9) The re-imaging procedure includes multiple appliance reboot.
         (10) This operation CANNOT be undone.

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

```
   > proceed
   Proceeding...

   Step 1 of 7: Backing up the appliance support information
   ...
   Done
   Step 2 of 7: Setting up the environment for the Appliance Re-image.
   ...
   Done
   Step 3 of 7: Extracting the packages
   ...
   This step may take a few minutes... \
   Done
   Step 4 of 7: Preparing the Luna Network HSM baseline installation scripts
   ...
   Done
   Step 5 of 7: Updating to the Luna Network HSM baseline firmware
   ...
   Done
   Step 6 of 7: Installing Luna Network HSM Base licenses
   ...
   This step may take a few minutes... \
   Done
   Step 7 of 7: Factory reset Luna Network HSM
   ...
   The Luna Network HSM with baseline firmware version has been factory reset.
   Done

The Luna Network HSM  will restart multiple times to complete the baseline installation.
This process could take 15-20 minutes.
Please wait for the operation to complete as interrupting the process could have adverse
effects.
```

sysconf reimage tarlog

Retrieve the archived log file produced during the last appliance re-image operation. After running **sysconf reimage tarlog**, the file **Baseline_Re_image_logs.**<timestamp>**.tar.gz** can be viewed in the **admin** user's files using lunash:> **"my file list" on page 306** and transferred to a client workstation with **pscp**/**sftp**.

User Privileges

Users with the following privileges can perform this command:

> Admin

Syntax

sysconf reimage tarlog

Example

```
lunash:>sysconf reimage tarlog

'hsm reimage tarlogs' successful

Use 'scp' from a client machine to get file named:
Baseline_Re_image_logs.20180614_14.40.40.tar.gz

Command Result : 0 (Success)
```

sysconf scp

Access commands that enable or disable scp on the system.

> **NOTE** SCP is deprecated in favor of SFTP. Adjust any scripts or procedures that currently rely on scp.

User Privileges

Users with the following privileges can perform these commands:

> Admin

> Operator

Syntax

sysconf scp

disable
enable
show

Argument(s)	Shortcut	Description
disable	**d**	Disable and stop scp service. See "sysconf scp disable" below.
enable	**e**	Enable and start scp service. See "sysconf scp enable" below.
show	**s**	Show if SCP is enabled or disabled on the system. See "sysconf scp show" on page 649.

sysconf scp disable

Disable and stop the SCP service.

This command was added with the introduction of SFTP (a more modern and secure protocol).

By default, for compatibility, scp is enabled.

> **NOTE** SCP is deprecated in favor of SFTP. Adjust any scripts or procedures that currently rely on scp.

User Privileges

Users with the following privileges can perform this command:

- Admin
- Operator

Syntax

sysconf scp disable

Examples

```
lunash:>sysconf scp disable

Command Result : 0 (Success)


lunash:>sysconf scp disable

   SCP is already disabled on the system.

Command Result : 0 (Success)
```

sysconf scp enable

Enable and start the SCP service.

This command was added with the introduction of SFTP (a more modern and secure protocol).

By default, for compatibility, scp is enabled.

> **NOTE** SCP is deprecated in favor of SFTP. Adjust any scripts or procedures that currently rely on scp.

User Privileges

Users with the following privileges can perform this command:

- Admin
- Operator

Syntax

sysconf scp enable

Examples

```
lunash:>sysconf scp enable

Command Result : 0 (Success)


lunash:>sysconf scp enable

   SCP is already enabled on the system.

Command Result : 0 (Success)
```

sysconf scp show

Show the current scp status.

> **NOTE** SCP is deprecated in favor of SFTP. Adjust any scripts or procedures that currently rely on scp.

User Privileges

Users with the following privileges can perform this command:

- Admin
- Operator
- Monitor

Syntax

sysconf scp show

Examples

```
lunash:>sysconf scp show

SCP is enabled

Command Result : 0 (Success)

lunash:>sysconf scp show

SCP is disabled

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

Argument(s)	Shortcut	Description
disable	**d**	Disable the SNMP service. See "sysconf snmp disable" on the next page.
enable	**e**	Enable the SNMP service. See "sysconf snmp enable" on page 652.
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 653.
show	**s**	Display SNMP service information. See "sysconf snmp show" on page 659.
trap	**t**	Access commands that allow you to view or configure the SNMP trap hosts. See "sysconf snmp trap" on page 660.
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 670.

sysconf snmp disable

Disable and stop the SNMP service.

User Privileges

Users with the following privileges can perform this command:

- Admin
- Operator

Syntax

sysconf snmp disable

Example

```
lunash:>sysconf snmp disable

SNMP is disabled
Starting snmpd:                                            [  OK  ]
SNMP is stopped

Command Result : 0 (Success)
```

sysconf snmp enable

Enable and start the SNMP service.

User Privileges

Users with the following privileges can perform this command:

- Admin
- Operator

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

Argument(s)	Shortcut	Description
add	**a**	Add a notification target . See "sysconf snmp notification add" on the next page.
clear	**c**	Delete all notification targets. See "sysconf snmp notification clear" on page 656.
delete	**d**	Delete a notification target. See "sysconf snmp notification delete" on page 657.
list	**l**	Display a list of the notification targets. See "sysconf snmp notification list" on page 658.

sysconf snmp notification add

Add a single notification destination to be notified via the SNMP service.

User Privileges

Users with the following privileges can perform this command:

- Admin
- Operator

Syntax

sysconf snmp notification add -ipaddress <ipaddress> **-authpassword** <password> **-privpassword** <password> **-secname** <userid> [**-authprotocol** <protocol>] [**-notifytype** {**trap** | **inform**}] [**-privprotocol** <protocol>] [**-udpport** <port>] [**-engineid** <engineid>]

Argument(s)	Shortcut	Description
-authpassword <password>	**-authpa**	Specifies the authentication password. The password may be 8-to-128 characters long.
-authprotocol <protocol>	**-authpr**	Specifies the authentication protocol. **Valid values:** SHA **Default:** SHA
-engineid <engineid>	**-e**	Specifies the SNMP v3 Engine ID in hex numbers. The **-engineid** parameter is user-defined; set any hex number, omitting the 0x or 0X. Luna Network HSM 7 does not support dynamic discovery of the EngineID, once configured; ensure that you save or remember this value.
-ipaddress <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 <type>	**-n**	Specifies the notification type. **Valid values:** **trap:** one-way unconfirmed notification **inform:** confirmed notification with retries **Default:** trap
-privpassword <password>	**-privpa**	Specifies the privacy password or encryption password. The password may be 8-to-128 characters long.
-privprotocol <protocol>	**-privpr**	Specifies the AES privacy protocol.

Argument(s)	Shortcut	Description
-secname <userid>	**-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 <port>	**-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

Example

```
lunash:>sysconf snmp notification add -ipaddress 10.124.0.87 -authpassword authPa$$w0rd -
privpassword privPa$$w0rd -secname admin -engineid 0029403200

SNMP notification target information added

Command Result : 0 (Success)
```

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 LunaSH 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.

User Privileges

Users with the following privileges can perform this command:

> Admin

> Operator

Syntax

sysconf snmp notification clear [**-force**]

Argument(s)	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
Proceeding...
SNMP notification target information cleared


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.

User Privileges

Users with the following privileges can perform this command:

- Admin
- Operator

Syntax

sysconf snmp notification delete -ipaddress <ipaddress> [**-udpport** <port>]

Argument(s)	Shortcut	Description
-ipaddress <ipaddress>	**-i**	Specifies the IP address of the notification target to delete.
-udpport <port>	**-u**	Specifies the UDP port of the notification target to delete. **Range:** 0-65535 **Default:** 162

Example

```
lunash:>sysconf snmp notification delete -ipaddress 192.20.11.64

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.

User Privileges

Users with the following privileges can perform this command:

- Admin
- Operator
- Monitor

Syntax

sysconf snmp notification list

Example

```
lunash:>sysconf snmp notification list


SNMP Notification Targets:
--------------------------
10.124.0.87:162 "0029403200" "admin"
192.20.11.64:162 "00473984504" "James"


Command Result : 0 (Success)
```

In this example, the output conveys the following information:

Field	Description
10.124.0.87 192.20.11.64	The IP addresses of the notification target hosts (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.
admin James	The "Security Names" (or user names) on whose behalf notifications are sent.
0029403200 00473984504	The SNMP v3 Engine ID (hex).

sysconf snmp show

Display SNMP service information.

User Privileges

Users with the following privileges can perform this command:

- Admin
- Operator
- Monitor

Syntax

sysconf snmp show

Example

```
lunash:>sysconf snmp show

SNMP is running
SNMP is enabled

Command Result : 0 (Success)
```

sysconf snmp trap

Access commands that allow you to view or configure SNMP trap hosts.

Syntax

sysconf snmp trap

clear
delete
disable
enable
set
show
test

Argument(s)	Shortcut	Description
clear	**c**	Clear SNMP trap host information. See "sysconf snmp trap clear" on the next page.
delete	**de**	Delete information for a specific SNMP trap host. See "sysconf snmp trap delete" on page 662.
disable	**di**	Disable and stop the Luna SNMP Trap Agent (lsta). See "sysconf snmp trap disable" on page 663.
enable	**e**	Enable and start the Luna SNMP Trap Agent (lsta). See "sysconf snmp trap enable" on page 664.
set	**se**	Set SNMP trap host information. See "sysconf snmp trap set" on page 665.
show	**sh**	Display SNMP trap host information. See "sysconf snmp trap show" on page 667.
test	**t**	Test SNMP trap notification. See "sysconf snmp trap test" on page 668.

sysconf snmp trap clear

Deletes all SNMP Trap Host Information.

> **NOTE** After running this command, you must restart the lsta service with the command **service restart lsta** for the configuration change to take effect.

User Privileges

Users with the following privileges can perform this command:

- Admin
- Operator

Syntax

sysconf snmp trap clear [**-force**]

Argument(s)	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
Proceeding...

Please use 'service restart lsta' for the new configuration to take effect.

Command Result : 0 (Success)
```

sysconf snmp trap delete

Delete information for a specific SNMP trap host.

> **NOTE** After running this command, you must restart the lsta service with the command **service restart lsta** for the configuration change to take effect.

User Privileges

Users with the following privileges can perform this command:

- Admin
- Operator

Syntax

sysconf snmp trap delete -host <hostname/IP> [**-force**]

Argument(s)	Shortcut	Description
-host <hostname/IP>	**-h**	Specifies the trap host name or IP address.
-force	**-f**	Force the action without prompting.

Example

```
lunash:>sysconf snmp trap delete -host mysnmphost

If you are sure that you wish to delete this snmp trap information, then enter 'proceed',
otherwise enter 'quit'.

> proceed
Proceeding...


Please use 'service restart lsta' for the new configuration to take effect.


Command Result : 0 (Success)
```

sysconf snmp trap disable

Disable and stop the Luna SNMP Trap Agent (lsta).

User Privileges

Users with the following privileges can perform this command:

- Admin
- Operator

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).

User Privileges

Users with the following privileges can perform this command:

- Admin
- Operator

Syntax

sysconf snmp trap enable

Example

```
lunash:>sysconf snmp trap enable

SNMP trap agent is enabled
Stopping syslog:                                           [  OK  ]
Starting syslog:                                           [  OK  ]
Starting lsta:                                             [  OK  ]

SNMP trap agent is started

Command Result : 0 (Success)
```

sysconf snmp trap set

Set SNMP trap host information. You can set multiple trap hosts by issuing this command for each host you wish to configure.

> **NOTE** After running this command, you must restart the lsta service with the command **service restart lsta** for the configuration change to take effect.

User Privileges

Users with the following privileges can perform this command:

- Admin
- Operator

Syntax

sysconf snmp trap set -host <hostname/IP> **-secname** <secname> **-engineid** <engineID> **-authprotocol** <protocol> **-authpwd** <password> **-privprotocol** <protocol> **-privpwd** <password>] [**-traptype** <type>]

Argument(s)	Shortcut	Description
-authprotocol <protocol>	**-authpr**	Specifies the SNMP v3 Authentication Protocol **Valid values:** SHA **Default:** SHA
-authpwd <password>	**-authpw**	Specifies the SNMP v3 Authentication password.
-engineid <engineID>	**-e**	Specifies the SNMP v3 Engine ID. The **-engineid** parameter is user-defined; set any hex number, omitting the 0x or 0X. Luna Network HSM 7 does not support dynamic discovery of the EngineID, once configured; ensure that you save or remember this value.
-host <hostname/IP>	**-h**	Specifies the trap host name or IP address.
-privprotocol <protocol>	**-privpr**	Specifies the SNMP v3 Privacy protocol. **Valid values:** AES **Default:** AES
-privpwd <password>	**-privpw**	Specifies the SNMP v3 Privacy Password.
-secname <secname>	**-s**	Specifies the SNMP v3 security name.

Argument(s)	Shortcut	Description
-traptype <type>	**-t**	Specify **trap** to record all sending attempts as successful. By default (**inform**), the appliance waits for a response from the target server before recording that the trap was sent successfully. **NOTE** This feature requires Luna Network HSM 7 Appliance Software 7.7.0 or newer. **Valid Values:** trap,inform **Default:** inform

Example

```
lunash:>sysconf snmp trap set -host mysnmphost -secname admin -engineid 800007c70300e05290ab60
-authprotocol SHA -authpwd p4$$w0rd -privprotocol AES -privpwd pr1vat3Pwd

Please use 'service restart lsta' for the new configuration to take effect.

Command Result : 0 (Success)
```

sysconf snmp trap show

Display SNMP trap host information.

User Privileges

Users with the following privileges can perform this command:

- Admin
- Operator
- Monitor

Syntax

sysconf snmp trap show

Example

```
lunash:>sysconf snmp trap show


  SNMP Trap Host                  : 192.168.13.117:162
  SNMP Trap Type                  : inform
  SNMP Version                    : 3
  SNMP v3 Security Name           : myuserpin
  SNMP v3 Engine ID               : 0x1234567890
  SNMP v3 Security Level          : authPriv
  SNMP v3 Authentication protocol : SHA
  SNMP v3 Privacy protocol        : AES

  SNMP Trap Host                  : mysnmphost:162
  SNMP Version                    : 3
  SNMP v3 Security Name           : admin
  SNMP v3 Engine ID               : 0x800007c70300e05290ab60
  SNMP v3 Security Level          : authPriv
  SNMP v3 Authentication protocol : SHA
  SNMP v3 Privacy protocol        : AES



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 About the Syslog and SNMP 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)
```

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 About the Syslog and SNMP Monitoring Guide.

User Privileges

Users with the following privileges can perform this command:

- Admin
- Operator

Syntax

sysconf snmp trap test -logfacility <logfacility> **-loglevel** <loglevel> **-process** <process> **-message** <message> [**-pid**]

Argument(s)	Shortcut	Description
-logfacility <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 <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

Argument(s)	Shortcut	Description
-process <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 <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

Argument(s)	Shortcut	Description
add	**a**	Add a user. See "sysconf snmp user add" on the next page.
clear	**c**	Delete all users. See "sysconf snmp user clear" on page 673.
delete	**d**	Delete a user. See "sysconf snmp user delete" on page 674.
list	**l**	List the currently configured users. See "sysconf snmp user list" on page 675.

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) access to all MIB objects.

> Notify (TRAP/INFORM) access to all MIB objects.

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**.

> **NOTE** If an SSH connection with a Luna Network HSM 7 appliance is terminated while the **sysconf snmp user add** command is in progress, it is not possible to reconnect immediately to re-run the command.

User Privileges

Users with the following privileges can perform this command:

> Admin

> Operator

Syntax

sysconf snmp user add -secname <secname> **-authpassword** <password> **-authprotocol** <protocol> **-privpassword** <password> **-privprotocol** <protocol>

Argument(s)	Shortcut	Description
-secname <secname>	**-s**	Specifies the security name. The name may be 1-to-31 characters; this is effectively the SNMPv3 term for "User name"
-authpassword <password>	**-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 <protocol>	**-authpr**	Specifies the authentication protocol. **Valid values:** SHA **Default:** SHA
-privpassword <password>	**-privpa**	Specifies the privacy password or encryption password. The password may be 8-to-128 characters (for better security, it should be different than the password specified for **authpassword**).
-privprotocol <protocol>	**-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 authPa$$w0rd -authprotocol SHA -
privpassword privPa$$w0rd -privprotocol AES

SNMP user account "admin" added

Command Result : 0 (Success)
```

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 authPa$$w0rd -x AES -X privPa$$w0rd myLuna1 .1
```

sysconf snmp user clear

Delete all users that are currently configured to use the SNMP command with this Luna Network HSM 7 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.

User Privileges

Users with the following privileges can perform this command:

- Admin
- Operator

Syntax

sysconf snmp user clear [**-force**]

Argument(s)	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
Proceeding...
SNMP user account information cleared


Command Result : 0 (Success)
```

sysconf snmp user delete

Delete a specific (named) user that is currently configured to use the SNMP command with this Luna Network HSM 7 appliance (allowed to access the SNMP agent).

User Privileges

Users with the following privileges can perform this command:

- Admin
- Operator

Syntax

sysconf snmp user delete -secname <userid>

Argument(s)	Shortcut	Description
-secname <userid>	**-s**	Specifies the user name of the user you want to delete.

Example

```
lunash:>sysconf snmp user delete -secname User

SNMP user account "User" 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 Network HSM 7 appliance.

User Privileges

Users with the following privileges can perform this command:

- Admin
- Operator
- Monitor

Syntax

sysconf snmp user list

Example

```
lunash:>sysconf snmp user list


SNMP Users:
-----------
admin
Jon


Command Result : 0 (Success)
```

sysconf ssh

Access commands that allow you to view or configure SSH options on the appliance.

Syntax

sysconf ssh

ciphers
client
device
ip
password
port
publickey
regenkeypair
show

Argument(s)	Shortcut	Description
ciphers	**ci**	View and configure list of ciphers available and ciphers configured for SSH negotiation. See "sysconf ssh ciphers" on the next page.
client	**cl**	Manage an allowlist of permitted SSH clients. See "sysconf ssh client" on page 688.
device	**d**	Set the SSH device restriction policy. See "sysconf ssh device" on page 702.
ip	**i**	Set the SSH IP restriction policy. See "sysconf ssh ip" on page 703.
password	**pa**	Enable or disable password authentication. See "sysconf ssh password" on page 704.
port	**po**	Set the SSHD listen port number (22, 1024-65535). See "sysconf ssh port" on page 707.
publickey	**pu**	View or configure SSH public keys. See "sysconf ssh publickey" on page 708.
regenkeypair	**r**	Regenerate the SSH key pair. See "sysconf ssh regenKeyPair" on page 711.
show	**s**	Display the currently set SSH restriction policies. See "sysconf ssh show" on page 712.

sysconf ssh ciphers

View and configure the ciphers that can be used when negotiating SSH connections.

Commands added with Luna Network HSM 7 appliance software version 7.8.0.

Syntax

sysconf ssh ciphers

Argument(s)	Shortcut	Description
reset	**reset**	Reset the list of configured SSH ciphers back to the default entries. See "sysconf ssh ciphers reset" on page 679.
set	**se**	Set the configured SSH ciphers. See "sysconf ssh ciphers set" on page 681.
show	**sh**	Shows the list of available ciphers, and the list of configured SSH ciphers. See "sysconf ssh ciphers show" on page 684.

SSH Ciphers before Luna Network HSM 7.8.0

> **NOTE** The table below compiles ssh ciphers as available for Luna Network HSM 7 appliances **prior to version 7.8.0** when the **sysconf ciphers** commands became available.

SSH algorithms	Appliance software 7.2.0	Appliance software 7.3.0	Appliance software 7.4.0	Appliance software 7.7.0	Appliance software 7.7.1
kex	curve25519-sha256@libssh.org ecdh-sha2-nistp256 ecdh-sha2-nistp384 ecdh-sha2-nistp521 diffie-hellman-group-exchange-sha256 diffie-hellman-group16-sha512 diffie-hellman-group18-sha512 diffie-hellman-group14-sha256 diffie-hellman-group14-sha1	curve25519-sha256 curve25519-sha256@libssh.org ecdh-sha2-nistp256 ecdh-sha2-nistp384 ecdh-sha2-nistp521 diffie-hellman-group-exchange-sha256 diffie-hellman-group16-sha512 diffie-hellman-group18-sha512 diffie-hellman-group14-sha256 diffie-hellman-group14-sha1	curve25519-sha256 curve25519-sha256@libssh.org ecdh-sha2-nistp256 ecdh-sha2-nistp384 ecdh-sha2-nistp521 diffie-hellman-group-exchange-sha256 diffie-hellman-group16-sha512 diffie-hellman-group18-sha512 diffie-hellman-group14-sha256 diffie-hellman-group14-sha1	curve25519-sha256 curve25519-sha256@libssh.org ecdh-sha2-nistp256 ecdh-sha2-nistp384 ecdh-sha2-nistp521 diffie-hellman-group-exchange-sha256 diffie-hellman-group16-sha512 diffie-hellman-group18-sha512 diffie-hellman-group14-sha256 diffie-hellman-group14-sha1	curve25519-sha256 curve25519-sha256@libssh.org ecdh-sha2-nistp256 ecdh-sha2-nistp384 ecdh-sha2-nistp521 diffie-hellman-group-exchange-sha256 diffie-hellman-group16-sha512 diffie-hellman-group18-sha512 diffie-hellman-group14-sha256
server_host_key	ssh-rsa rsa-sha2-512 rsa-sha2-256 ecdsa-sha2-nistp256	ssh-rsa rsa-sha2-512 rsa-sha2-256 ecdsa-sha2-nistp256	ssh-rsa rsa-sha2-512 rsa-sha2-256 ecdsa-sha2-nistp256	ssh-rsa rsa-sha2-512 rsa-sha2-256 ecdsa-sha2-nistp256 ssh-ed25519	ssh-rsa rsa-sha2-512 rsa-sha2-256 ecdsa-sha2-nistp256 ssh-ed25519

SSH algorithms	Appliance software 7.2.0	Appliance software 7.3.0	Appliance software 7.4.0	Appliance software 7.7.0	Appliance software 7.7.1
encryption	aes192-ctr aes256-ctr	aes192-ctr aes256-ctr	aes192-ctr aes256-ctr	aes192-ctr aes256-ctr	aes192-ctr aes256-ctr
mac	hmac-sha1 hmac-sha2-256 hmac-sha2-512	hmac-sha1 hmac-sha2-256 hmac-sha2-512	hmac-sha1 hmac-sha2-256 hmac-sha2-512	hmac-sha1 hmac-sha2-256 hmac-sha2-512	umac-64-etm@openssh.com umac-128-etm@openssh.com hmac-sha2-256-etm@openssh.com hmac-sha2-512-etm@openssh.com umac-64@openssh.com umac-128@openssh.com hmac-sha2-256 hmac-sha2-512
compression	none zlib@openssh.com	none zlib@openssh.com	none zlib@openssh.com	none zlib@openssh.com	none zlib@openssh.com

sysconf ssh ciphers reset

Resets the SSH ciphers for the appliance to default settings.

User Privileges

Users with the following privileges can perform this command:

- Admin
- Operator

Syntax

sysconf ssh ciphers reset

Example resetting a configured list of ciphers

```
llunash:>sysconf ssh ciphers reset

This operation will reset the SSH cipher(s) to use the following default cipher(s):

Configured Ciphers
------------------
aes192-ctr
aes256-ctr

This operation will restart the SSH service.
Type 'proceed' to reset SSH cipher(s) to default settings and restart the SSH service, or
'quit'
    to quit now. > proceed

Stopping sshd:                                             [  OK  ]

Starting sshd:                                             [  OK  ]


Command Result : 0 (Success)
```

sysconf ssh ciphers set

Sets the SSH ciphers for the appliance.

Command added with Luna Network HSM 7 appliance software version 7.8.0.

If **-list** is provided alone, the SSH ciphers list in the command becomes the new list, replacing any that were previously configured.

If the **-add** option is provided, then the **-add** list is appended to the currently configured SSH ciphers list.
If the **-remove** option is provided, then the **-remove** list is removed from the currently configured ciphers.

Removing all ciphers is not possible; one must remain configured.

The client-side priority preference takes precedence during SSH cipher negotiation.

User Privileges

Users with the following privileges can perform this command:

> Admin

> Operator

Syntax

sysconf sh ciphers set -list <cipher list>[**-add** | **-remove**] [**-force**]

Argument(s)	Shortcut	Description
-add	**-a**	Add to the Configured SSH Ciphers List
-list <cipher list>	**-l**	Colon Separated List of Ciphers • when used with **-add** this is the list of ciphers that will be appended below any currently-configured ciphers; • when used with **-remove** this is the list of ciphers that will be removed from the currently-configured ciphers; • when used with no option, this is the list of ciphers that will replace all currently-configured ciphers
-remove	**-r**	Remove from the Configured SSH Ciphers List
-force	**-f**	Force the action.

Example setting a list of ciphers

```
lunash:>sysconf ssh ciphers set -list aes192-ctr:aes256-ctr:aes128-ctr

This operation will set the SSH cipher(s) to use the following cipher(s):

Configured Ciphers
------------------
aes192-ctr
```

```
aes256-ctr
aes128-ctr

This operation will restart the SSH service.
Type 'proceed' to set SSH cipher(s) and restart the SSH service, or 'quit'
    to quit now. > proceed

Stopping sshd:                                             [  OK  ]

Starting sshd:                                             [  OK  ]

Command Result : 0 (Success)
```

Example adding ciphers to an existing list

```
lunash:>sysconf ssh ciphers set -list aes128-cbc:aes256-cbc -add

This operation will set the SSH cipher(s) to use the following cipher(s):

Configured Ciphers
------------------
aes192-ctr
aes256-ctr
aes128-ctr
aes128-cbc
aes256-cbc

This operation will restart the SSH service.
Type 'proceed' to set SSH cipher(s) and restart the SSH service, or 'quit'
    to quit now. > proceed

Stopping sshd:                                             [  OK  ]

Starting sshd:                                             [  OK  ]

Command Result : 0 (Success)
```

Example removing ciphers from an existing list

```
lunash:>sysconf ssh ciphers set -list aes192-ctr:aes128-ctr:aes128-cbc -remove

This operation will set the SSH cipher(s) to use the following cipher(s):

Configured Ciphers
------------------
aes256-ctr
aes256-cbc

This operation will restart the SSH service.
Type 'proceed' to set SSH cipher(s) and restart the SSH service, or 'quit'
    to quit now. > proceed

Stopping sshd:                                             [  OK  ]

Starting sshd:                                             [  OK  ]

Command Result : 0 (Success)
```

Examples of incorrect usage

Attempting to set or add improper ciphers

```
lunash:>sysconf ssh ciphers set -list invalid-cipherA:deprecated-cipherB:made-up-cipherC

Error: The following SSH cipher(s) are invalid:
invalid-cipherA
deprecated-cipherB
made-up-cipherC

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

Attempting to remove ciphers that are not already among those configured

```
lunash:>sysconf ssh ciphers set -list aes192-ctr:arcfour -remove

Error: Cannot remove the following SSH cipher(s), as they are not currently configured:
aes192-ctr
arcfour

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

Attempting to remove all ciphers, leaving none configured

```
lunash:>sysconf ssh ciphers set -list aes256-ctr:aes256-cbc -remove

Error: Cannot remove all currently configured SSH ciphers.

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

sysconf ssh ciphers show

Shows the available and configured SSH ciphers for the appliance.
Command added with Luna Network HSM 7 appliance software version 7.8.0.

> **TIP** If your HSM appliance software version is earlier than 7.8.0, we suggest How to enumerate ssh cipher lists available to your network appliance if "ciphers show" command is not available in your version.

User Privileges

Users with the following privileges can perform this command:

- Admin
- Operator
- Monitor

Syntax

sysconf ssh ciphers show

Example

```
lunash:>sysconf ssh ciphers show

The following cipher(s) are available to configure SSH:

Available Ciphers
--------------------------------------------------
3des-cbc
blowfish-cbc
cast128-cbc
arcfour
arcfour128
arcfour256
aes128-cbc
aes192-cbc
aes256-cbc
rijndael-cbc@lysator.liu.se
aes128-ctr
aes192-ctr
aes256-ctr
aes128-gcm@openssh.com
aes256-gcm@openssh.com
chacha20-poly1305@openssh.com

The selected SSH cipher(s) are used by the SSH service
SSH is using the following cipher(s):

Configured Ciphers
------------------
aes192-ctr
aes256-ctr
```

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

SSH Ciphers before Luna Network HSM 7.8.0

> **NOTE** The table below compiles ssh ciphers as available for Luna Network HSM 7 appliances **prior to version 7.8.0** when the **sysconf ciphers** commands became available.

SSH algorithms	Appliance software 7.2.0	Appliance software 7.3.0	Appliance software 7.4.0	Appliance software 7.7.0	Appliance software 7.7.1
kex	curve25519-sha256@libssh.org ecdh-sha2-nistp256 ecdh-sha2-nistp384 ecdh-sha2-nistp521 diffie-hellman-group-exchange-sha256 diffie-hellman-group16-sha512 diffie-hellman-group18-sha512 diffie-hellman-group14-sha256 diffie-hellman-group14-sha1	curve25519-sha256 curve25519-sha256@libssh.org ecdh-sha2-nistp256 ecdh-sha2-nistp384 ecdh-sha2-nistp521 diffie-hellman-group-exchange-sha256 diffie-hellman-group16-sha512 diffie-hellman-group18-sha512 diffie-hellman-group14-sha256 diffie-hellman-group14-sha1	curve25519-sha256 curve25519-sha256@libssh.org ecdh-sha2-nistp256 ecdh-sha2-nistp384 ecdh-sha2-nistp521 diffie-hellman-group-exchange-sha256 diffie-hellman-group16-sha512 diffie-hellman-group18-sha512 diffie-hellman-group14-sha256 diffie-hellman-group14-sha1	curve25519-sha256 curve25519-sha256@libssh.org ecdh-sha2-nistp256 ecdh-sha2-nistp384 ecdh-sha2-nistp521 diffie-hellman-group-exchange-sha256 diffie-hellman-group16-sha512 diffie-hellman-group18-sha512 diffie-hellman-group14-sha256 diffie-hellman-group14-sha1	curve25519-sha256 curve25519-sha256@libssh.org ecdh-sha2-nistp256 ecdh-sha2-nistp384 ecdh-sha2-nistp521 diffie-hellman-group-exchange-sha256 diffie-hellman-group16-sha512 diffie-hellman-group18-sha512 diffie-hellman-group14-sha256

SSH algorithms	Appliance software 7.2.0	Appliance software 7.3.0	Appliance software 7.4.0	Appliance software 7.7.0	Appliance software 7.7.1
server_host_key	ssh-rsa rsa-sha2-512 rsa-sha2-256 ecdsa-sha2-nistp256	ssh-rsa rsa-sha2-512 rsa-sha2-256 ecdsa-sha2-nistp256	ssh-rsa rsa-sha2-512 rsa-sha2-256 ecdsa-sha2-nistp256	ssh-rsa rsa-sha2-512 rsa-sha2-256 ecdsa-sha2-nistp256 ssh-ed25519	ssh-rsa rsa-sha2-512 rsa-sha2-256 ecdsa-sha2-nistp256 ssh-ed25519
encryption	aes192-ctr aes256-ctr	aes192-ctr aes256-ctr	aes192-ctr aes256-ctr	aes192-ctr aes256-ctr	aes192-ctr aes256-ctr
mac	hmac-sha1 hmac-sha2-256 hmac-sha2-512	hmac-sha1 hmac-sha2-256 hmac-sha2-512	hmac-sha1 hmac-sha2-256 hmac-sha2-512	hmac-sha1 hmac-sha2-256 hmac-sha2-512	umac-64-etm@openssh.com umac-128-etm@openssh.com hmac-sha2-256-etm@openssh.com hmac-sha2-512-etm@openssh.com umac-64@openssh.com umac-128@openssh.com hmac-sha2-256 hmac-sha2-512
compression	none zlib@openssh.com	none zlib@openssh.com	none zlib@openssh.com	none zlib@openssh.com	none zlib@openssh.com

sysconf ssh client

Configure and manage SSH access control at the HSM appliance, by creating an allowlist of IP addresses that are permitted to connect. These commands are optional, and can be used if you wish to apply an additional layer in your network security with respect to HSM appliances.

> **NOTE** This command is available using Luna Network HSM 7 Appliance Software 7.7.1 and newer.
>
> Your network administrator remains responsible for all the standard network security configuration and management actions required by your security regime.

IP addresses are added, singly or in groups, this creates or expands a list of exclusively permitted host IPs that are applicable to a given Luna Network HSM 7 appliance user ID.

- When the list exists, only member host IP addresses are permitted; all others are excluded.
- If the list does not exist for a user ID on the appliance, then any IP address can potentially connect via SSH.
- When no allowlist exists for user ID, the Client Access Status shows as "All clients" next to that user ID.
- Current list members can be deleted individually, or the entire list can be deleted. Or allowlists for all user IDs can be cleared at once.

> **NOTE** These commands do not have any awareness whether the provided host IP represents a valid Luna client. The command applies a general IP-based SSH access filtering. It is up to you to ensure that you are using a correct host IP address in each instance, such as you would have separately configured for NTLS or STC client connections - see Client-Partition Connections.

Syntax

sysconf ssh client

add
clear
delete
list
showRejectedClients

Subcommand(s)	Shortcut	Description
add	**a**	Adds a client IP to the list. When the list has one member or more, any IP not included, is refused when attempting SSH connection. See "sysconf ssh client add" on page 690.
clear	**c**	Deletes all the currently permitted IP addresses from the list associated with every user ID. Allows any IP to connect via SSH. See "sysconf ssh client clear" on page 694.

Subcommand(s)	Shortcut	Description
delete	**d**	Deletes a single client host IP or a comma-separated list of host IP addresses from the allowlist of permitted addresses for a named Luna Network HSM 7 appliance user ID. See "sysconf ssh client delete" on page 697.
list	**l**	List configured client IPs. See "sysconf ssh client list" on page 700.
showRejectedClients	**t**	Show the most recent log entries regarding rejected client IPs. See "sysconf ssh client showRejectedClients" on page 701.

sysconf ssh client add

Register an SSH client.

> **NOTE** This command is available using Luna Network HSM 7 Appliance Software 7.7.1 and newer.

This command limits access to the HSM via SSH, by applying an allowlist of clients for a user. New IP addresses (comma-delimited if more than one) are added to the existing list, or a list is created.

> **NOTE** For multiple IP address entry, surround the list with quotation marks and separate list members with comma delimiters. Spaces are optional for readability, and are ignored.

If the list already includes an IP address that is being added, that address is ignored and any new ones are added to the list.

Invalid entries are flagged and the command exits.

User Privileges

Users with the following privileges can perform this command:

- Admin
- Operator

Syntax

sysconf ssh client add -userId <username> **-host** <multipleipaddresses> **-force**

Argument(s)	Shortcut	Description
-host <multipleipaddresses>	**-h**	SSH client IP(s) to register. Use ',' as a delimiter.
-userId <username>	**-u**	User Name
-force	**-f**	Force the action with no prompting.

Example with single new IP address

```
lunash:>sysconf ssh client list
User ID              Client Access status
---------------------------------------------
audit                All clients
admin                All clients
monitor              All clients
operator             All clients
Alice                All clients

Command Result : 0 (Success)
```

```
lunash:>sysconf ssh client list add -userId Alice -h 10.124.79.145

Alice will forfeit ssh access from any hosts not
configured with this Luna Network HSM.

If you are sure that you wish to proceed, then type 'proceed',
otherwise type 'quit'

> proceed
Proceeding...

INFO: Restarting sshd service is recommended to apply updated
      ssh access configuration.

Command Result : 0 (Success)


lunash:>sysconf ssh client list

User ID              Client Access status
---------------------------------------------
audit                All clients
admin                All clients
monitor              All clients
operator             All clients
Alice                10.124.79.145

Command Result : 0 (Success)

lunash:>
```

User ID "Alice" existed in the list (was registered) and that user ID could be accessed on the appliance from any host. The command in the example adds a single host IP that now becomes the only IP from which that user ID can be accessed on this appliance via SSH. The other user IDs in the list (audit, admin, monitor, and operator) remain wide open and can be accessed via SSH from any host IP, unless you have imposed other restrictions in your network configuration, external to the Luna Network HSM 7 appliance.

Example with multiple new IP addresses

```
lunash:>sysconf ssh client list

User ID              Client Access status
---------------------------------------------
audit                All clients
admin                All clients
monitor              All clients
operator             All clients
Alice                10.124.79.145

Command Result : 0 (Success)

lunash:>sysconf ssh client add -userId Alice -host "10.124.145.18, 10.124.145.19,
10.124.145.20"

Alice will forfeit ssh access from any hosts not
configured with this Luna Network HSM.
```

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

> proceed
Proceeding...

INFO: Restarting sshd service is recommended to apply updated
      ssh access configuration.

Command Result : 0 (Success)


lunash:>sysconf ssh client list

User ID              Client Access status
---------------------------------------------
audit                All clients
admin                All clients
monitor              All clients
operator             All clients
Alice                10.124.79.145 10.124.145.18 10.124.145.19 10.124.145.20

Command Result : 0 (Success)
```

User ID "Alice" existed in the list (was registered) and that client could access the appliance from just a single host IP. The command in the example adds more host IPs such that the original host as well as three new ones become the only host IPs from which that client can access this appliance via SSH. The host IPs listed in the command happened to include the pre-existing one. That was not necessary to retain the pre-existing host IP, but also does not conflict. The other user IDs in the list remain wide open and can be accessed via SSH from any host IP, unless you have imposed other restrictions in your network configuration, external to the Luna Network HSM 7 appliance.

Example with multiple new IP addresses with extra spaces

```
lunash:>sysconf ssh client list

User ID              Client Access status
---------------------------------------------
audit                All clients
admin                All clients
monitor              All clients
operator             All clients
Alice                10.124.79.145 10.124.145.18 10.124.145.19 10.124.145.20

Command Result : 0 (Success)

lunash:>sysconf ssh client add -userId Alice -host " 10.124.145.21, 10.124.145.22 ,
10.124.145.23  "

Alice will forfeit ssh access from any hosts not
configured with this Luna Network HSM.

If you are sure that you wish to proceed, then type 'proceed',
otherwise type 'quit'

> proceed
Proceeding...
```

```
INFO: Restarting sshd service is recommended to apply updated
      ssh access configuration.

Command Result : 0 (Success)
lunash:>sysconf ssh client list

User ID              Client Access status
---------------------------------------------
audit                All clients
admin                All clients
monitor              All clients
operator             All clients
Alice                10.124.79.145 10.124.145.18 10.124.145.19 10.124.145.20 10.124.145.21
10.124.145.22 10.124.145.23

Command Result : 0 (Success)
```

User ID "Alice" existed in the list (was registered) and that client could access the appliance from any of four registered host IPs, but no other host IP could connect over SSH for that client user ID. The command in the example adds a three more host IPs that expand the list to seven host IPs from which that client can access this appliance via SSH. The existing host IPs are retained; it was not necessary to specify them again, when adding new ones. If they had been included, they would have been ignored. The quotation marks enclosing the full list of new host IPs are optional, the commas that separate the IPs being added are required, but the spaces are ignored. The other user IDs in the list remain wide open and can be accessed via SSH from any host IP, unless you have imposed other restrictions in your network configuration, external to the Luna Network HSM 7 appliance.

sysconf ssh client clear

Clears the allowlist of client host IP addresses for one user Id or for all user IDs.Clients at specified IPs will be no longer subjected to SSH access restriction for the user specified. If no other SSH filter entry exists for any other user from a given IP address, then any user can have SSH access from the IP.

> **NOTE** This command is available using Luna Network HSM 7 Appliance Software 7.7.1 and newer.

User Privileges

Users with the following privileges can perform this command:

- Admin
- Operator

Syntax

sysconf ssh client clear [-all] [-userId <username>] **-force**

Argument(s)	Shortcut	Description
-all	**-a**	Set default ssh access for all users
-userId <username>	**-u**	User Name
-force	**-f**	Force the action with no prompting.

Example clearing a single user ID

```
lunash:>sysconf ssh client list

User ID              Client Access status
---------------------------------------------
audit                10.124.79.145
admin                All clients
monitor              All clients
operator             All clients
Alice                10.124.79.145 10.124.145.18

Command Result : 0 (Success)


lunash:>sysconf ssh client clear -userid audit

audit will be given SSH access permission from all hosts.

If you are sure that you wish to proceed, then type 'proceed',
```

```
otherwise type 'quit'

> proceed
Proceeding...

INFO: Restarting sshd service is recommended to apply updated
      ssh access configuration.

Command Result : 0 (Success)


lunash:>sysconf ssh client list

User ID              Client Access status
---------------------------------------------
audit                All clients
admin                All clients
monitor              All clients
operator             All clients
Alice                10.124.79.145 10.124.145.18

Command Result : 0 (Success)

lunash:>
```

Example clearing all user IDs' host SSH accessibility

```
lunash:>sysconf ssh client list

User ID             Client Access status
--------------------------------------------
audit               10.124.79.145
admin               All clients
monitor             All clients
operator            All clients
Alice               10.124.79.145 10.124.145.18

Command Result : 0 (Success)


lunash:>sysconf ssh client clear -all

All users will be given default SSH access permission.

If you are sure that you wish to proceed, then type 'proceed',
otherwise type 'quit'

> proceed
Proceeding...

INFO: Restarting sshd service is recommended to apply updated
      ssh access configuration.

Command Result : 0 (Success)
```

```
lunash:>sysconf ssh client list

User ID              Client Access status
---------------------------------------------
audit                All clients
admin                All clients
monitor              All clients
operator             All clients
Alice                All clients

Command Result : 0 (Success)

lunash:>
```

sysconf ssh client delete

Delete or unregister a client host-IP address from the SSH access permission list for a specified Network HSM appliance user ID.

> **NOTE** This command is available using Luna Network HSM 7 Appliance Software 7.7.1 and newer.

IP addresses are removed from the existing list.

- If you delete a subset of IPs already registered, then SSH access remains limited to access from those IPs still explicitly included in the allowlist.
- When you remove all IP entries from the list for a specific user ID, it reverts to "All clients"; that is, you allow a user to SSH from any workstation.

> **NOTE** For multiple IP address entry, surround the list with quotation marks and separate list members with comma delimiters. Spaces are optional for readability, and are ignored.

Invalid entries are flagged and the command exits.

User Privileges

Users with the following privileges can perform this command:

- Admin
- Operator

Syntax

sysconf ssh client delete -ip <multipleipaddresses> **-force**

Argument(s)	Shortcut	Description
-host <multipleaddresses>	**-h**	SSH client host IP(s) to unregister. Use ',' as a delimiter.
-userid	**-u**	User name
-force	**-f**	Force the action with no prompting.

Example deleting/unregistering one IP address

```
lunash:>sysconf ssh client list

User ID              Client Access status
---------------------------------------------
audit                All clients
```

```
admin                All clients
monitor              All clients
operator             All clients
Alice                10.124.79.145 10.124.145.18 10.124.145.19 10.124.145.20 10.124.145.21
10.124.145.22 10.124.145.23

Command Result : 0 (Success)

[local_host] lunash:>sysconf ssh client delete -userid Alice -host 10.124.145.23

Alice will forfeit ssh access from all hosts specified here:
10.124.145.23

If you are sure that you wish to proceed, then type 'proceed',
otherwise type 'quit'

> proceed
Proceeding...

INFO: Restarting sshd service is recommended to apply updated
      ssh access configuration.

Command Result : 0 (Success)


lunash:>sysconf ssh client list

User ID              Client Access status
---------------------------------------------
audit                All clients
admin                All clients
monitor              All clients
operator             All clients
Alice                10.124.79.145 10.124.145.18 10.124.145.19 10.124.145.20 10.124.145.21
10.124.145.22

Command Result : 0 (Success)

lunash:>
```

User "Alice" on the appliance could be accessed from any of seven host IP addresses. The command removes (unregisters) one of them. The six remaining host IP addresses are now the only ones from which user ID "Alice" can be accessed over SSH. The other user IDs in the list remain wide open and can be accessed via SSH from any host IP.

Example deleting/unregistering multiple IP addresses

```
lunash:>sysconf ssh client list


User ID              Client Access status
---------------------------------------------
audit                All clients
admin                All clients
monitor              All clients
```

```
operator             All clients
Alice                10.124.79.145 10.124.145.18 10.124.145.19 10.124.145.20 10.124.145.21
10.124.145.22

Command Result : 0 (Success)

lunash:>sysconf ssh client delete -userid Alice -host 10.124.145.21,10.124.145.22

Alice will forfeit ssh access from all hosts specified here:
10.124.145.21 10.124.145.22

If you are sure that you wish to proceed, then type 'proceed',
otherwise type 'quit'

> proceed
Proceeding...

INFO: Restarting sshd service is recommended to apply updated
      ssh access configuration.

Command Result : 0 (Success)

lunash:>sysconf ssh client list

User ID              Client Access status
---------------------------------------------
audit                All clients
admin                All clients
monitor              All clients
operator             All clients
Alice                10.124.79.145 10.124.145.18 10.124.145.19 10.124.145.20

Command Result : 0 (Success)
```

User "Alice" on the appliance could be accessed from any of six host IP addresses. The command removes (unregisters) two of them. The four remaining host IP addresses are now the only ones from which user ID "Alice" can be accessed over SSH. The other user IDs in the list remain wide open and can be accessed via SSH from any host IP.

sysconf ssh client list

List registered SSH client(s). This is the allowlist. While any addresses are on this list for a given user ID, no other addresses can make SSH connections to the appliance for that user ID. "All clients" means that access to that user ID is wide open from any host IP, unless you have other access controls on your network, external to the HSM appliance.

> **NOTE** This command is available using Luna Network HSM 7 Appliance Software 7.7.1 and newer.

User Privileges

Users with the following privileges can perform this command:

- Admin
- Operator
- Monitor

Syntax

sysconf ssh client list

Example

```
lunash:>sysconf ssh client list

User ID              Client Access status
---------------------------------------------
audit                All clients
admin                All clients
monitor              All clients
operator             All clients
Alice                10.124.79.145


Command Result : 0 (Success)
```

sysconf ssh client showRejectedClients

List the most recent clients that have made failed attempts at SSH connection. Rejection is for a user from a specified IP address.

> **NOTE** This command is available using Luna Network HSM 7 Appliance Software 7.7.1 and newer.

If you register at least one client, this forces all other clients to be rejected. Rejection of a client can be due to one of following reasons:

- Incoming client IP is not registered with the appliance.
- The client's actual IP might have been registered, but the remote client IP has been subject to address translation (NAT) and the resulting incoming IP is different from the actual client. This IP is not registered with the appliance.

User Privileges

Users with the following privileges can perform this command:

- Admin
- Operator

Syntax

sysconf ssh client showRejectedClients

Example

```
lunash:>sysconf ssh client showRejectedClients

2020 Dec 23 11:24:19 Alice from 10.124.79.145

Command Result : 0 (Success)

lunash:>
```

sysconf ssh device

Restrict the appliance/HSM administrative traffic (over SSH) to a specific Ethernet device. Use this command if you want to segregate administrative traffic (SSH) from client (NTLS) traffic. This command is an alternative to the command "sysconf ssh ip" on the next page, 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 378, which binds client (NTLS) traffic to a specific IP or device name on your Luna Network HSM 7.

User Privileges

Users with the following privileges can perform this command:

> Admin

> Operator

Syntax

sysconf ssh device <netdevice>

Argument(s)	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. **eth2**: Restrict SSH connections to the eth2 interface. **eth3**: Restrict SSH connections to the eth3 interface.

Example

```
lunash:>sysconf ssh device eth0

Success:  SSH now restricted to ethernet device eth0 (IP address 192.20.11.78).
          Restarting ssh service.

Stopping sshd:                                             [  OK  ]

Starting sshd:                                             [  OK  ]


Command Result : 0 (Success)
```

sysconf ssh ip

Restrict the appliance/HSM administrative traffic (over SSH) to the indicated IP address (bound to one of the Luna Network HSM 7's Ethernet ports). Use this command where you need to segregate administrative traffic from client (NTLS) traffic. This command is an alternative to the command "sysconf ssh device" on the previous page, 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 378, which binds client (NTLS) traffic to a specific IP or device name on your Luna Network HSM 7.

User Privileges

Users with the following privileges can perform this command:

- Admin
- Operator

Syntax

sysconf ssh ip <ipaddress>

Argument(s)	Description
<ipaddress>	Specifies the IP address associated with the Luna Network HSM 7 network interface device to which you want to restrict the SSH service. **Valid Values:** > Any specific IPv4 or IPv6 address > **0.0.0.0** (unrestricted IPv4) > **::** (unrestricted IPv6)

Example

```
lunash:>sysconf ssh ip 192.20.11.78

Success:  SSH now restricted to ethernet device eth0 (IP address 192.20.11.78).
          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 SSH password authentication.

Syntax

sysconf ssh password

disable
enable

Argument(s)	Shortcut	Description
disable	**d**	Disable SSH password authentication. See "sysconf ssh password disable" on the next page.
enable	**e**	Enable SSH password authentication. See "sysconf ssh password enable" on page 706.

sysconf ssh password disable

Disable SSH password authentication.

User Privileges

Users with the following privileges can perform this command:

- Admin
- Operator

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.

User Privileges

Users with the following privileges can perform this command:

- Admin
- Operator

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.

User Privileges

Users with the following privileges can perform this command:

> Admin

Syntax

sysconf ssh port <port>

Argument(s)	Description
<port>	Specifies the SSHD listen port number. **Range:** 22 or 1024-65535 **Default:** 22

Example

```
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

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 310.

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 Network HSM 7 appliance without knowing the LunaSH admin password!

Syntax

sysconf ssh publickey

disable
enable

Argument(s)	Shortcut	Description
disable	**di**	Disable SSH public key authentication. See "sysconf ssh publickey disable" on the next page.
enable	**e**	Enable SSH public key authentication. See "sysconf ssh publickey enable" on page 710.

sysconf ssh publickey disable

Disable SSH public key authentication.

User Privileges

Users with the following privileges can perform this command:

- Admin
- Operator

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 Network HSM 7 appliance without knowing the LunaSH admin password!

User Privileges

Users with the following privileges can perform this command:

- Admin
- Operator

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.

User Privileges

Users with the following privileges can perform this command:

> Admin

> Operator

Syntax

sysconf ssh regenKeyPair [**-curvesize** <curvesize>]

Argument(s)	Shortcut	Description
-curvesize	**-c**	Elliptic Curve size. Valid Values: **256** (default), **384**, **512** **NOTE** This option requires Luna Appliance Software 7.8.4 or newer.

NOTE Only the **-curvesize** option is provided with this command; **-keysize** is not, since RSA keypairs are not permitted for SSH connections.

Example

```
lunash:> sysconf ssh regenKeyPair -curvesize 384


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  ]


Starting sshd:                                                [  OK  ]
Command Result : 0 (Success)
```

sysconf ssh show

Display the currently configured SSH restrictions.

User Privileges

Users with the following privileges can perform this command:

- Admin
- Operator
- Monitor

Syntax

sysconf ssh show

Example

```
lunash:>sysconf ssh show

SSHD configuration:

SSHD Listen Port 22


SSH is restricted to ethernet device eth0 (ip address 192.20.11.78).
SSH is unrestricted for all IPv4 addresses.

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 time zone 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 time zone.

You can determine the current date/time setting using the **status date** command.

User Privileges

Users with the following privileges can perform this command:

- Admin
- Operator

Syntax

sysconf time <time> [<date>]

Argument(s)	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 13:58 20170301

Wed Mar  1 13:58:00 EST 2017


Command Result : 0 (Success)
```

sysconf timezone

Show and set the time zone for the appliance's clock. This command allows the administrator to check and set the system time zone.

Syntax

sysconf timezone

set
show
list

Argument(s)	Shortcut	Description
list	**l**	Displays a list of accepted time zone codes and regions. See "sysconf timezone list" on the next page.
set	**se**	Set time zone. See "sysconf timezone set" on page 716.
show	**sh**	Shows the current time zone setting. See "sysconf timezone show" on page 717.

sysconf timezone list

Displays a list of accepted time zone codes and regions.

User Privileges

Users with the following privileges can perform this command:

- Admin
- Operator
- Monitor

Syntax

sysconf timezone list <region>

Argument(s)	Description
<region>	Specifying a <region> parameter will produce a list of time zones associated with that region. See Setting the Time Zone for more information on correct time zone abbreviations.

Example

```
lunash:>sysconf timezone list Kentucky

Available time zones:

posix/America/Kentucky
posix/America/Kentucky/Monticello
posix/America/Kentucky/Louisville
America/Kentucky
America/Kentucky/Monticello
America/Kentucky/Louisville
right/America/Kentucky
right/America/Kentucky/Monticello
right/America/Kentucky/Louisville

Command Result : 0 (Success)
```

sysconf timezone set

Set time zone.

User Privileges

Users with the following privileges can perform this command:

> Admin

> Operator

Syntax

sysconf timezone set <time_zone>

Argument(s)	Shortcut	Description
<time_zone>	**se**	Set time zone. For a list of accepted time zone abbreviations, use the command **sysconf timezone list**, or see https://en.wikipedia.org/wiki/List_of_tz_database_time_zones.

Example

```
lunash:>sysconf timezone set EST5EDT
Time zone set to EST5EDT
```

sysconf timezone show

Shows the current time zone setting. This changes depending on whether Daylight Saving Time is in effect. See Setting the Time Zone for more information.

User Privileges

Users with the following privileges can perform this command:

- Admin
- Operator
- Monitor

Syntax

sysconf timezone show

Example

```
lunash:>sysconf timezone show
EST
```

sysconf tls ciphers

View or modify the list of ciphers that the Luna Network HSM 7 appliance's TLS service negotiates with a contacting entity. This allows you to change the order of the default list, which determines the preference order when TLS is negotiating, or to exclude some of the supported ciphers from the negotiations, if desired. When the Luna Network HSM 7 appliance is negotiating with a Client, the client cipher options are open (but see Note below), and the appliance choices prevail.

> **NOTE** This feature requires minimum Luna Network HSM 7 Appliance Software 7.2.0 and Luna HSM Client 7.2.0.

Syntax

sysconf tls ciphers

reset
set
show

Argument(s)	Shortcut	Description
reset	**r**	Reset to the default ciphers. See "sysconf tls ciphers reset" on the next page.
set	**se**	Set the list of ciphers from which TLS can choose when negotiating session security. See "sysconf tls ciphers set" on page 722.
show	**sh**	Show the current list of ciphers available for TLS, or export the current settings as a template. See "sysconf tls ciphers show" on page 727.

sysconf tls ciphers reset

Reset the current list of TLS ciphers to the default list.

> **NOTE** This feature requires minimum Luna Network HSM 7 Appliance Software 7.2.0 and Luna HSM Client 7.2.0.

User Privileges

Users with the following privileges can perform this command:

> Admin

Syntax

sysconf tls ciphers reset [**-force**]

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

Example (Luna Network HSM 7 version 7.8.3 and newer)

```
lunash:>sysconf tls ciphers reset

This operation will reset the TLS cipher suites to use the following default cipher suites:
Cipher suites are listed from highest to lowest priority.

Configured Ciphers (highest priority at top)
--------------------------------------------------
TLS_AES_256_GCM_SHA384        TLSv1.3  Kx=any   Au=any  Enc=AESGCM(256)             Mac=AEAD
TLS_CHACHA20_POLY1305_SHA256  TLSv1.3  Kx=any   Au=any  Enc=CHACHA20/POLY1305(256)  Mac=AEAD
TLS_AES_128_GCM_SHA256        TLSv1.3  Kx=any   Au=any  Enc=AESGCM(128)             Mac=AEAD
ECDHE-RSA-AES256-GCM-SHA384   TLSv1.2  Kx=ECDH  Au=RSA  Enc=AESGCM(256)             Mac=AEAD
DHE-RSA-AES256-GCM-SHA384     TLSv1.2  Kx=DH    Au=RSA  Enc=AESGCM(256)             Mac=AEAD
ECDHE-RSA-AES128-GCM-SHA256   TLSv1.2  Kx=ECDH  Au=RSA  Enc=AESGCM(128)             Mac=AEAD
DHE-RSA-AES128-GCM-SHA256     TLSv1.2  Kx=DH    Au=RSA  Enc=AESGCM(128)             Mac=AEAD
ECDHE-RSA-AES256-SHA384       TLSv1.2  Kx=ECDH  Au=RSA  Enc=AES(256)                Mac=SHA384
DHE-RSA-AES256-SHA256         TLSv1.2  Kx=DH    Au=RSA  Enc=AES(256)                Mac=SHA256
ECDHE-RSA-AES128-SHA256       TLSv1.2  Kx=ECDH  Au=RSA  Enc=AES(128)                Mac=SHA256
DHE-RSA-AES128-SHA256         TLSv1.2  Kx=DH    Au=RSA  Enc=AES(128)                Mac=SHA256
AES256-GCM-SHA384             TLSv1.2  Kx=RSA   Au=RSA  Enc=AESGCM(256)             Mac=AEAD
AES128-GCM-SHA256             TLSv1.2  Kx=RSA   Au=RSA  Enc=AESGCM(128)             Mac=AEAD
AES256-SHA256                 TLSv1.2  Kx=RSA   Au=RSA  Enc=AES(256)                Mac=SHA256
AES128-SHA256                 TLSv1.2  Kx=RSA   Au=RSA  Enc=AES(128)                Mac=SHA256

This operation will restart the TLS related services (NTLS, STCD, CBS).
Type 'proceed' to reset TLS cipher suites to default settings and restart TLS related services,
or 'quit'
    to quit now. > proceed
```

```
Restarting NTLS, STC and CBS services.... Done

Command Result : 0 (Success)
```

Example of resetting prior to Luna Network HSM 7 version 7.8.3

(This example shows the current list, the reset operation, and then the active list after reset.)

```
lunash:>sysconf tls ciphers show

The following cipher suites are available to configure TLS:

Available Ciphers
--------------------------------------------------
ECDHE-RSA-AES256-GCM-SHA384  TLSv1.2  Kx=ECDH  Au=RSA  Enc=AESGCM(256)  Mac=AEAD
ECDHE-RSA-AES256-SHA384      TLSv1.2  Kx=ECDH  Au=RSA  Enc=AES(256)     Mac=SHA384
DHE-RSA-AES256-GCM-SHA384    TLSv1.2  Kx=DH    Au=RSA  Enc=AESGCM(256)  Mac=AEAD
DHE-RSA-AES256-SHA256        TLSv1.2  Kx=DH    Au=RSA  Enc=AES(256)     Mac=SHA256
AES256-GCM-SHA384            TLSv1.2  Kx=RSA   Au=RSA  Enc=AESGCM(256)  Mac=AEAD
AES256-SHA256                TLSv1.2  Kx=RSA   Au=RSA  Enc=AES(256)     Mac=SHA256
ECDHE-RSA-AES128-GCM-SHA256  TLSv1.2  Kx=ECDH  Au=RSA  Enc=AESGCM(128)  Mac=AEAD
ECDHE-RSA-AES128-SHA256      TLSv1.2  Kx=ECDH  Au=RSA  Enc=AES(128)     Mac=SHA256
DHE-RSA-AES128-GCM-SHA256    TLSv1.2  Kx=DH    Au=RSA  Enc=AESGCM(128)  Mac=AEAD
DHE-RSA-AES128-SHA256        TLSv1.2  Kx=DH    Au=RSA  Enc=AES(128)     Mac=SHA256
AES128-GCM-SHA256            TLSv1.2  Kx=RSA   Au=RSA  Enc=AESGCM(128)  Mac=AEAD
AES128-SHA256                TLSv1.2  Kx=RSA   Au=RSA  Enc=AES(128)     Mac=SHA256

The selected TLS cipher suites are used by the NTLS, STC outer tunnel, RBS, Ped vector
Server/Client features
TLS is using the following cipher suites:
Cipher suites are listed from highest to lowest priority.

Configured Ciphers (highest priority at top)
--------------------------------------------------
ECDHE-RSA-AES256-GCM-SHA384  TLSv1.2  Kx=ECDH  Au=RSA  Enc=AESGCM(256)  Mac=AEAD
ECDHE-RSA-AES256-SHA384      TLSv1.2  Kx=ECDH  Au=RSA  Enc=AES(256)     Mac=SHA384


Command Result : 0 (Success)



lunash:>sysconf tls ciphers reset

This operation will reset the TLS cipher suites to use the following default cipher suites:
Cipher suites are listed from highest to lowest priority.

Configured Ciphers (highest priority at top)
--------------------------------------------------
ECDHE-RSA-AES256-GCM-SHA384  TLSv1.2  Kx=ECDH  Au=RSA  Enc=AESGCM(256)  Mac=AEAD
ECDHE-RSA-AES256-SHA384      TLSv1.2  Kx=ECDH  Au=RSA  Enc=AES(256)     Mac=SHA384
DHE-RSA-AES256-GCM-SHA384    TLSv1.2  Kx=DH    Au=RSA  Enc=AESGCM(256)  Mac=AEAD
DHE-RSA-AES256-SHA256        TLSv1.2  Kx=DH    Au=RSA  Enc=AES(256)     Mac=SHA256
AES256-GCM-SHA384            TLSv1.2  Kx=RSA   Au=RSA  Enc=AESGCM(256)  Mac=AEAD
AES256-SHA256                TLSv1.2  Kx=RSA   Au=RSA  Enc=AES(256)     Mac=SHA256
ECDHE-RSA-AES128-GCM-SHA256  TLSv1.2  Kx=ECDH  Au=RSA  Enc=AESGCM(128)  Mac=AEAD
ECDHE-RSA-AES128-SHA256      TLSv1.2  Kx=ECDH  Au=RSA  Enc=AES(128)     Mac=SHA256
DHE-RSA-AES128-GCM-SHA256    TLSv1.2  Kx=DH    Au=RSA  Enc=AESGCM(128)  Mac=AEAD
```

```
DHE-RSA-AES128-SHA256        TLSv1.2  Kx=DH    Au=RSA  Enc=AES(128)     Mac=SHA256
AES128-GCM-SHA256            TLSv1.2  Kx=RSA   Au=RSA  Enc=AESGCM(128)  Mac=AEAD
AES128-SHA256                TLSv1.2  Kx=RSA   Au=RSA  Enc=AES(128)     Mac=SHA256

This operation will restart the TLS related services (NTLS, STCD, CBS).
Type 'proceed' to reset TLS cipher suites to default settings and restart TLS related services,
or 'quit'
    to quit now. > proceed

Restarting NTLS, STC and CBS services.... Done

Command Result : 0 (Success)



lunash:>sysconf tls ciphers show

The following cipher suites are available to configure TLS:

Available Ciphers
--------------------------------------------------
ECDHE-RSA-AES256-GCM-SHA384  TLSv1.2  Kx=ECDH  Au=RSA  Enc=AESGCM(256)  Mac=AEAD
ECDHE-RSA-AES256-SHA384      TLSv1.2  Kx=ECDH  Au=RSA  Enc=AES(256)     Mac=SHA384
DHE-RSA-AES256-GCM-SHA384    TLSv1.2  Kx=DH    Au=RSA  Enc=AESGCM(256)  Mac=AEAD
DHE-RSA-AES256-SHA256        TLSv1.2  Kx=DH    Au=RSA  Enc=AES(256)     Mac=SHA256
AES256-GCM-SHA384            TLSv1.2  Kx=RSA   Au=RSA  Enc=AESGCM(256)  Mac=AEAD
AES256-SHA256                TLSv1.2  Kx=RSA   Au=RSA  Enc=AES(256)     Mac=SHA256
ECDHE-RSA-AES128-GCM-SHA256  TLSv1.2  Kx=ECDH  Au=RSA  Enc=AESGCM(128)  Mac=AEAD
ECDHE-RSA-AES128-SHA256      TLSv1.2  Kx=ECDH  Au=RSA  Enc=AES(128)     Mac=SHA256
DHE-RSA-AES128-GCM-SHA256    TLSv1.2  Kx=DH    Au=RSA  Enc=AESGCM(128)  Mac=AEAD
DHE-RSA-AES128-SHA256        TLSv1.2  Kx=DH    Au=RSA  Enc=AES(128)     Mac=SHA256
AES128-GCM-SHA256            TLSv1.2  Kx=RSA   Au=RSA  Enc=AESGCM(128)  Mac=AEAD
AES128-SHA256                TLSv1.2  Kx=RSA   Au=RSA  Enc=AES(128)     Mac=SHA256

The selected TLS cipher suites are used by the NTLS, STC outer tunnel, RBS, Ped vector
Server/Client features
TLS is using the following cipher suites:
Cipher suites are listed from highest to lowest priority.

Configured Ciphers (highest priority at top)
--------------------------------------------------
ECDHE-RSA-AES256-GCM-SHA384  TLSv1.2  Kx=ECDH  Au=RSA  Enc=AESGCM(256)  Mac=AEAD
ECDHE-RSA-AES256-SHA384      TLSv1.2  Kx=ECDH  Au=RSA  Enc=AES(256)     Mac=SHA384
DHE-RSA-AES256-GCM-SHA384    TLSv1.2  Kx=DH    Au=RSA  Enc=AESGCM(256)  Mac=AEAD
DHE-RSA-AES256-SHA256        TLSv1.2  Kx=DH    Au=RSA  Enc=AES(256)     Mac=SHA256
AES256-GCM-SHA384            TLSv1.2  Kx=RSA   Au=RSA  Enc=AESGCM(256)  Mac=AEAD
AES256-SHA256                TLSv1.2  Kx=RSA   Au=RSA  Enc=AES(256)     Mac=SHA256
ECDHE-RSA-AES128-GCM-SHA256  TLSv1.2  Kx=ECDH  Au=RSA  Enc=AESGCM(128)  Mac=AEAD
ECDHE-RSA-AES128-SHA256      TLSv1.2  Kx=ECDH  Au=RSA  Enc=AES(128)     Mac=SHA256
DHE-RSA-AES128-GCM-SHA256    TLSv1.2  Kx=DH    Au=RSA  Enc=AESGCM(128)  Mac=AEAD
DHE-RSA-AES128-SHA256        TLSv1.2  Kx=DH    Au=RSA  Enc=AES(128)     Mac=SHA256
AES128-GCM-SHA256            TLSv1.2  Kx=RSA   Au=RSA  Enc=AESGCM(128)  Mac=AEAD
AES128-SHA256                TLSv1.2  Kx=RSA   Au=RSA  Enc=AES(128)     Mac=SHA256


Command Result : 0 (Success)
```

sysconf tls ciphers set

Set the list of ciphers that the Network HSM appliance's TLS service uses to negotiate connection security for a session.

> **NOTE** This feature requires minimum Luna Network HSM 7 Appliance Software 7.2.0 and Luna HSM Client 7.2.0.

You can change the list of TLS ciphers by listing them in the LunaSH command line in the order of desired priority (**-list**), or by creating a file containing this list and transferring it to the appliance **admin** files (**-applytemplate**). The following rules apply to both methods:

> You can use valid OpenSSL arguments to simplify your specifications, such as:
  - **kECDHE** (cipher suites using ephemeral ECDH key agreement, in default order)
  - **kDHE** (cipher suites using ephemeral DH key agreement, in default order)
  - **kRSA** (cipher suites using RSA key exchange, in default order)
  - **ALL** (all not-otherwise-specified ciphers, in default order)

> Ciphers or arguments in the list must be separated by colons (**:**).
  For example:

```
ECDHE-RSA-AES256-SHA384:ECDHE-RSA-AES256-GCM-SHA384:ALL
```

> The list/template can contain a maximum of 255 characters, including colon separators. To avoid reaching this character limit:
  - Specify only the ciphers you intend to use. It is not necessary to include the entire list.
  - If you do wish to include the entire list, specify the most important ciphers first, and then use the ALL option to complete the list in the default remaining order.

User Privileges

Users with the following privileges can perform this command:

> Admin

Syntax

sysconf tls ciphers set {**-list** <cipher_list> | **-applytemplate** <file name>} [**-force**]

Argument(s)	Shortcut	Description
-applytemplate <file name>	**-a**	File name of a template file to apply. Either a template file with **-applytemplate**, or a command line list with **-list** must be applied.

Argument(s)	Shortcut	Description
-list <cipher list>	**-l**	Colon-separated list of ciphers to apply. Either a template file with **-list**, or a command line list with **-applytemplate** must be applied.
-force	**-f**	Force the action without prompting.

Example (Luna Appliance Software 7.8.3 and newer) using a list with a modifier to exclude a group of ciphers

Exclude all TLSv1.2

```
lunash:>sysconf tls ciphers set -list ALL:!TLSv1.2

This operation will set the TLS cipher suites to use the following cipher suites:
Cipher suites are listed from highest to lowest priority.

Configured Ciphers (highest priority at top)
---------------------------------------------------
TLS_AES_256_GCM_SHA384        TLSv1.3  Kx=any  Au=any  Enc=AESGCM(256)             Mac=AEAD
TLS_CHACHA20_POLY1305_SHA256  TLSv1.3  Kx=any  Au=any  Enc=CHACHA20/POLY1305(256)  Mac=AEAD
TLS_AES_128_GCM_SHA256        TLSv1.3  Kx=any  Au=any  Enc=AESGCM(128)             Mac=AEAD

This operation will restart the TLS related services (NTLS, STCD, CBS).
Type 'proceed' to set ciphers suites and restart TLS related services, or 'quit'
    to quit now. > proceed

Restarting NTLS, STC and CBS services.... Done

Command Result : 0 (Success)
```

Exclude all TLSv1.3

```
lunash:>sysconf tls ciphers set -list ALL:!TLSv1.3

This operation will set the TLS cipher suites to use the following cipher suites:
Cipher suites are listed from highest to lowest priority.

Configured Ciphers (highest priority at top)
---------------------------------------------------
ECDHE-RSA-AES256-GCM-SHA384  TLSv1.2  Kx=ECDH  Au=RSA  Enc=AESGCM(256)  Mac=AEAD
DHE-RSA-AES256-GCM-SHA384    TLSv1.2  Kx=DH    Au=RSA  Enc=AESGCM(256)  Mac=AEAD
ECDHE-RSA-AES128-GCM-SHA256  TLSv1.2  Kx=ECDH  Au=RSA  Enc=AESGCM(128)  Mac=AEAD
DHE-RSA-AES128-GCM-SHA256    TLSv1.2  Kx=DH    Au=RSA  Enc=AESGCM(128)  Mac=AEAD
ECDHE-RSA-AES256-SHA384      TLSv1.2  Kx=ECDH  Au=RSA  Enc=AES(256)     Mac=SHA384
DHE-RSA-AES256-SHA256        TLSv1.2  Kx=DH    Au=RSA  Enc=AES(256)     Mac=SHA256
ECDHE-RSA-AES128-SHA256      TLSv1.2  Kx=ECDH  Au=RSA  Enc=AES(128)     Mac=SHA256
DHE-RSA-AES128-SHA256        TLSv1.2  Kx=DH    Au=RSA  Enc=AES(128)     Mac=SHA256
AES256-GCM-SHA384            TLSv1.2  Kx=RSA   Au=RSA  Enc=AESGCM(256)  Mac=AEAD
AES128-GCM-SHA256            TLSv1.2  Kx=RSA   Au=RSA  Enc=AESGCM(128)  Mac=AEAD
AES256-SHA256                TLSv1.2  Kx=RSA   Au=RSA  Enc=AES(256)     Mac=SHA256
AES128-SHA256                TLSv1.2  Kx=RSA   Au=RSA  Enc=AES(128)     Mac=SHA256
```

```
This operation will restart the TLS related services (NTLS, STCD, CBS).
Type 'proceed' to set ciphers suites and restart TLS related services, or 'quit'
    to quit now. > proceed

Restarting NTLS, STC and CBS services.... Done

Command Result : 0 (Success)
```

Example (Luna Appliance Software 7.8.3 and newer) using a template file

```
lunash:>sysconf tls ciphers set -applyTemplate tls_template.txt

This operation will set the TLS cipher suites to use the following cipher suites:
Cipher suites are listed from highest to lowest priority.

Configured Ciphers (highest priority at top)
--------------------------------------------------
TLS_AES_256_GCM_SHA384        TLSv1.3  Kx=any   Au=any  Enc=AESGCM(256)             Mac=AEAD
TLS_CHACHA20_POLY1305_SHA256  TLSv1.3  Kx=any   Au=any  Enc=CHACHA20/POLY1305(256)  Mac=AEAD
TLS_AES_128_GCM_SHA256        TLSv1.3  Kx=any   Au=any  Enc=AESGCM(128)             Mac=AEAD
ECDHE-RSA-AES256-GCM-SHA384   TLSv1.2  Kx=ECDH  Au=RSA  Enc=AESGCM(256)             Mac=AEAD
DHE-RSA-AES256-GCM-SHA384     TLSv1.2  Kx=DH    Au=RSA  Enc=AESGCM(256)             Mac=AEAD
ECDHE-RSA-AES128-GCM-SHA256   TLSv1.2  Kx=ECDH  Au=RSA  Enc=AESGCM(128)             Mac=AEAD
DHE-RSA-AES128-GCM-SHA256     TLSv1.2  Kx=DH    Au=RSA  Enc=AESGCM(128)             Mac=AEAD
ECDHE-RSA-AES256-SHA384       TLSv1.2  Kx=ECDH  Au=RSA  Enc=AES(256)                Mac=SHA384
DHE-RSA-AES256-SHA256         TLSv1.2  Kx=DH    Au=RSA  Enc=AES(256)                Mac=SHA256
ECDHE-RSA-AES128-SHA256       TLSv1.2  Kx=ECDH  Au=RSA  Enc=AES(128)                Mac=SHA256
DHE-RSA-AES128-SHA256         TLSv1.2  Kx=DH    Au=RSA  Enc=AES(128)                Mac=SHA256
AES256-GCM-SHA384             TLSv1.2  Kx=RSA   Au=RSA  Enc=AESGCM(256)             Mac=AEAD
AES128-GCM-SHA256             TLSv1.2  Kx=RSA   Au=RSA  Enc=AESGCM(128)             Mac=AEAD
AES256-SHA256                 TLSv1.2  Kx=RSA   Au=RSA  Enc=AES(256)                Mac=SHA256
AES128-SHA256                 TLSv1.2  Kx=RSA   Au=RSA  Enc=AES(128)                Mac=SHA256

This operation will restart the TLS related services (NTLS, STCD, CBS).
Type 'proceed' to set ciphers suites and restart TLS related services, or 'quit'
    to quit now. > proceed

Restarting NTLS, STC and CBS services.... Done



Command Result : 0 (Success)
```

Example using a template file prior to Luna Appliance Software 7.8.3

```
lunash:>sysconf tls ciphers set -applyTemplate top-six

This operation will set the TLS cipher suites to use the following cipher suites:
Cipher suites are listed from highest to lowest priority.

Configured Ciphers (highest priority at top)
--------------------------------------------------
ECDHE-RSA-AES256-GCM-SHA384  TLSv1.2  Kx=ECDH  Au=RSA  Enc=AESGCM(256)  Mac=AEAD
ECDHE-RSA-AES256-SHA384      TLSv1.2  Kx=ECDH  Au=RSA  Enc=AES(256)     Mac=SHA384
DHE-RSA-AES256-GCM-SHA384    TLSv1.2  Kx=DH    Au=RSA  Enc=AESGCM(256)  Mac=AEAD
DHE-RSA-AES256-SHA256        TLSv1.2  Kx=DH    Au=RSA  Enc=AES(256)     Mac=SHA256
AES256-GCM-SHA384            TLSv1.2  Kx=RSA   Au=RSA  Enc=AESGCM(256)  Mac=AEAD
AES256-SHA256                TLSv1.2  Kx=RSA   Au=RSA  Enc=AES(256)     Mac=SHA256
```

```
This operation will restart the TLS related services (NTLS, STCD, CBS).
Type 'proceed' to set ciphers suites and restart TLS related services, or 'quit'
    to quit now. > proceed

Restarting NTLS, STC and CBS services.... Done

Command Result : 0 (Success)

lunash:>sysconf tls ciphers show

The following cipher suites are available to configure TLS:

Available Ciphers
--------------------------------------------------
ECDHE-RSA-AES256-GCM-SHA384  TLSv1.2  Kx=ECDH  Au=RSA  Enc=AESGCM(256)  Mac=AEAD
ECDHE-RSA-AES256-SHA384      TLSv1.2  Kx=ECDH  Au=RSA  Enc=AES(256)     Mac=SHA384
DHE-RSA-AES256-GCM-SHA384    TLSv1.2  Kx=DH    Au=RSA  Enc=AESGCM(256)  Mac=AEAD
DHE-RSA-AES256-SHA256        TLSv1.2  Kx=DH    Au=RSA  Enc=AES(256)     Mac=SHA256
AES256-GCM-SHA384            TLSv1.2  Kx=RSA   Au=RSA  Enc=AESGCM(256)  Mac=AEAD
AES256-SHA256                TLSv1.2  Kx=RSA   Au=RSA  Enc=AES(256)     Mac=SHA256
ECDHE-RSA-AES128-GCM-SHA256  TLSv1.2  Kx=ECDH  Au=RSA  Enc=AESGCM(128)  Mac=AEAD
ECDHE-RSA-AES128-SHA256      TLSv1.2  Kx=ECDH  Au=RSA  Enc=AES(128)     Mac=SHA256
DHE-RSA-AES128-GCM-SHA256    TLSv1.2  Kx=DH    Au=RSA  Enc=AESGCM(128)  Mac=AEAD
DHE-RSA-AES128-SHA256        TLSv1.2  Kx=DH    Au=RSA  Enc=AES(128)     Mac=SHA256
AES128-GCM-SHA256            TLSv1.2  Kx=RSA   Au=RSA  Enc=AESGCM(128)  Mac=AEAD
AES128-SHA256                TLSv1.2  Kx=RSA   Au=RSA  Enc=AES(128)     Mac=SHA256

The selected TLS cipher suites are used by the NTLS, STC outer tunnel, RBS, Ped vector
Server/Client features
TLS is using the following cipher suites:
Cipher suites are listed from highest to lowest priority.

Configured Ciphers (highest priority at top)
--------------------------------------------------
ECDHE-RSA-AES256-GCM-SHA384  TLSv1.2  Kx=ECDH  Au=RSA  Enc=AESGCM(256)  Mac=AEAD
ECDHE-RSA-AES256-SHA384      TLSv1.2  Kx=ECDH  Au=RSA  Enc=AES(256)     Mac=SHA384
DHE-RSA-AES256-GCM-SHA384    TLSv1.2  Kx=DH    Au=RSA  Enc=AESGCM(256)  Mac=AEAD
DHE-RSA-AES256-SHA256        TLSv1.2  Kx=DH    Au=RSA  Enc=AES(256)     Mac=SHA256
AES256-GCM-SHA384            TLSv1.2  Kx=RSA   Au=RSA  Enc=AESGCM(256)  Mac=AEAD
AES256-SHA256                TLSv1.2  Kx=RSA   Au=RSA  Enc=AES(256)     Mac=SHA256


Command Result : 0 (Success)
```

Example using a command-line list prior to Luna Appliance Software 7.8.3

```
lunash:>sysconf tls ciphers set -list ECDHE-RSA-AES256-GCM-SHA384:ECDHE-RSA-AES256-SHA384

This operation will set the TLS cipher suites to use the following cipher suites:
Cipher suites are listed from highest to lowest priority.

Configured Ciphers (highest priority at top)
--------------------------------------------------
ECDHE-RSA-AES256-GCM-SHA384  TLSv1.2  Kx=ECDH  Au=RSA  Enc=AESGCM(256)  Mac=AEAD
ECDHE-RSA-AES256-SHA384      TLSv1.2  Kx=ECDH  Au=RSA  Enc=AES(256)     Mac=SHA384

This operation will restart the TLS related services (NTLS, STCD, CBS).
```

```
Type 'proceed' to set ciphers suites and restart TLS related services, or 'quit'
    to quit now. > proceed

Restarting NTLS, STC and CBS services.... Done

Command Result : 0 (Success)

lunash:>sysconf tls ciphers show

The following cipher suites are available to configure TLS:

Available Ciphers
--------------------------------------------------
ECDHE-RSA-AES256-GCM-SHA384  TLSv1.2  Kx=ECDH  Au=RSA  Enc=AESGCM(256)  Mac=AEAD
ECDHE-RSA-AES256-SHA384      TLSv1.2  Kx=ECDH  Au=RSA  Enc=AES(256)     Mac=SHA384
DHE-RSA-AES256-GCM-SHA384    TLSv1.2  Kx=DH    Au=RSA  Enc=AESGCM(256)  Mac=AEAD
DHE-RSA-AES256-SHA256        TLSv1.2  Kx=DH    Au=RSA  Enc=AES(256)     Mac=SHA256
AES256-GCM-SHA384            TLSv1.2  Kx=RSA   Au=RSA  Enc=AESGCM(256)  Mac=AEAD
AES256-SHA256                TLSv1.2  Kx=RSA   Au=RSA  Enc=AES(256)     Mac=SHA256
ECDHE-RSA-AES128-GCM-SHA256  TLSv1.2  Kx=ECDH  Au=RSA  Enc=AESGCM(128)  Mac=AEAD
ECDHE-RSA-AES128-SHA256      TLSv1.2  Kx=ECDH  Au=RSA  Enc=AES(128)     Mac=SHA256
DHE-RSA-AES128-GCM-SHA256    TLSv1.2  Kx=DH    Au=RSA  Enc=AESGCM(128)  Mac=AEAD
DHE-RSA-AES128-SHA256        TLSv1.2  Kx=DH    Au=RSA  Enc=AES(128)     Mac=SHA256
AES128-GCM-SHA256            TLSv1.2  Kx=RSA   Au=RSA  Enc=AESGCM(128)  Mac=AEAD
AES128-SHA256                TLSv1.2  Kx=RSA   Au=RSA  Enc=AES(128)     Mac=SHA256

The selected TLS cipher suites are used by the NTLS, STC outer tunnel, RBS, Ped vector
Server/Client features
TLS is using the following cipher suites:
Cipher suites are listed from highest to lowest priority.

Configured Ciphers (highest priority at top)
--------------------------------------------------
ECDHE-RSA-AES256-GCM-SHA384  TLSv1.2  Kx=ECDH  Au=RSA  Enc=AESGCM(256)  Mac=AEAD
ECDHE-RSA-AES256-SHA384      TLSv1.2  Kx=ECDH  Au=RSA  Enc=AES(256)     Mac=SHA384


Command Result : 0 (Success)
```

sysconf tls ciphers show

Show the current list of ciphers from which the Network HSM appliance's TLS service can negotiate connection security for a session.

> **NOTE** This feature requires minimum Luna Network HSM 7 Appliance Software 7.2.0 and Luna HSM Client 7.2.0.

User Privileges

Users with the following privileges can perform this command:

- Admin
- Operator
- Monitor

Syntax

sysconf tls ciphers show [**-exportTemplate** <file name>]

Argument(s)	Shortcut	Description
-exportTemplate <filename>	**-a**	Output the current TLS cipher settings to a Template file.

Example with no argument (Luna Network HSM 7 appliance software 7.8.3 and newer)

```
lunash:>sysconf tls ciphers show

The following cipher suites are available to configure TLS:

Available Ciphers
--------------------------------------------------
TLS_AES_256_GCM_SHA384         TLSv1.3  Kx=any   Au=any  Enc=AESGCM(256)              Mac=AEAD
TLS_CHACHA20_POLY1305_SHA256   TLSv1.3  Kx=any   Au=any  Enc=CHACHA20/POLY1305(256)  Mac=AEAD
TLS_AES_128_GCM_SHA256         TLSv1.3  Kx=any   Au=any  Enc=AESGCM(128)              Mac=AEAD
ECDHE-RSA-AES256-GCM-SHA384    TLSv1.2  Kx=ECDH  Au=RSA  Enc=AESGCM(256)              Mac=AEAD
DHE-RSA-AES256-GCM-SHA384      TLSv1.2  Kx=DH    Au=RSA  Enc=AESGCM(256)              Mac=AEAD
ECDHE-RSA-AES128-GCM-SHA256    TLSv1.2  Kx=ECDH  Au=RSA  Enc=AESGCM(128)              Mac=AEAD
DHE-RSA-AES128-GCM-SHA256      TLSv1.2  Kx=DH    Au=RSA  Enc=AESGCM(128)              Mac=AEAD
ECDHE-RSA-AES256-SHA384        TLSv1.2  Kx=ECDH  Au=RSA  Enc=AES(256)                 Mac=SHA384
DHE-RSA-AES256-SHA256          TLSv1.2  Kx=DH    Au=RSA  Enc=AES(256)                 Mac=SHA256
ECDHE-RSA-AES128-SHA256        TLSv1.2  Kx=ECDH  Au=RSA  Enc=AES(128)                 Mac=SHA256
DHE-RSA-AES128-SHA256          TLSv1.2  Kx=DH    Au=RSA  Enc=AES(128)                 Mac=SHA256
AES256-GCM-SHA384              TLSv1.2  Kx=RSA   Au=RSA  Enc=AESGCM(256)              Mac=AEAD
AES128-GCM-SHA256              TLSv1.2  Kx=RSA   Au=RSA  Enc=AESGCM(128)              Mac=AEAD
AES256-SHA256                  TLSv1.2  Kx=RSA   Au=RSA  Enc=AES(256)                 Mac=SHA256
AES128-SHA256                  TLSv1.2  Kx=RSA   Au=RSA  Enc=AES(128)                 Mac=SHA256

The selected TLS cipher suites are used by the NTLS, STC outer tunnel, RBS, Ped vector
Server/Client features
```

```
TLS is using the following cipher suites:
Cipher suites are listed from highest to lowest priority.

Configured Ciphers (highest priority at top)
--------------------------------------------------
TLS_AES_256_GCM_SHA384        TLSv1.3  Kx=any   Au=any  Enc=AESGCM(256)             Mac=AEAD
TLS_CHACHA20_POLY1305_SHA256  TLSv1.3  Kx=any   Au=any  Enc=CHACHA20/POLY1305(256)  Mac=AEAD
TLS_AES_128_GCM_SHA256        TLSv1.3  Kx=any   Au=any  Enc=AESGCM(128)             Mac=AEAD
ECDHE-RSA-AES256-GCM-SHA384   TLSv1.2  Kx=ECDH  Au=RSA  Enc=AESGCM(256)             Mac=AEAD
DHE-RSA-AES256-GCM-SHA384     TLSv1.2  Kx=DH    Au=RSA  Enc=AESGCM(256)             Mac=AEAD
ECDHE-RSA-AES128-GCM-SHA256   TLSv1.2  Kx=ECDH  Au=RSA  Enc=AESGCM(128)             Mac=AEAD
DHE-RSA-AES128-GCM-SHA256     TLSv1.2  Kx=DH    Au=RSA  Enc=AESGCM(128)             Mac=AEAD
ECDHE-RSA-AES256-SHA384       TLSv1.2  Kx=ECDH  Au=RSA  Enc=AES(256)                Mac=SHA384
DHE-RSA-AES256-SHA256         TLSv1.2  Kx=DH    Au=RSA  Enc=AES(256)                Mac=SHA256
ECDHE-RSA-AES128-SHA256       TLSv1.2  Kx=ECDH  Au=RSA  Enc=AES(128)                Mac=SHA256
DHE-RSA-AES128-SHA256         TLSv1.2  Kx=DH    Au=RSA  Enc=AES(128)                Mac=SHA256
AES256-GCM-SHA384             TLSv1.2  Kx=RSA   Au=RSA  Enc=AESGCM(256)             Mac=AEAD
AES128-GCM-SHA256             TLSv1.2  Kx=RSA   Au=RSA  Enc=AESGCM(128)             Mac=AEAD
AES256-SHA256                 TLSv1.2  Kx=RSA   Au=RSA  Enc=AES(256)                Mac=SHA256
AES128-SHA256                 TLSv1.2  Kx=RSA   Au=RSA  Enc=AES(128)                Mac=SHA256


Command Result : 0 (Success)
```

Example with no argument (prior to Luna Network HSM 7 appliance software 7.8.3)

```
lunash:>sysconf tls ciphers show

The following cipher suites are available to configure TLS:

Available Ciphers
--------------------------------------------------
ECDHE-RSA-AES256-GCM-SHA384  TLSv1.2  Kx=ECDH  Au=RSA  Enc=AESGCM(256)  Mac=AEAD
ECDHE-RSA-AES256-SHA384      TLSv1.2  Kx=ECDH  Au=RSA  Enc=AES(256)     Mac=SHA384
DHE-RSA-AES256-GCM-SHA384    TLSv1.2  Kx=DH    Au=RSA  Enc=AESGCM(256)  Mac=AEAD
DHE-RSA-AES256-SHA256        TLSv1.2  Kx=DH    Au=RSA  Enc=AES(256)     Mac=SHA256
AES256-GCM-SHA384            TLSv1.2  Kx=RSA   Au=RSA  Enc=AESGCM(256)  Mac=AEAD
AES256-SHA256                TLSv1.2  Kx=RSA   Au=RSA  Enc=AES(256)     Mac=SHA256
ECDHE-RSA-AES128-GCM-SHA256  TLSv1.2  Kx=ECDH  Au=RSA  Enc=AESGCM(128)  Mac=AEAD
ECDHE-RSA-AES128-SHA256      TLSv1.2  Kx=ECDH  Au=RSA  Enc=AES(128)     Mac=SHA256
DHE-RSA-AES128-GCM-SHA256    TLSv1.2  Kx=DH    Au=RSA  Enc=AESGCM(128)  Mac=AEAD
DHE-RSA-AES128-SHA256        TLSv1.2  Kx=DH    Au=RSA  Enc=AES(128)     Mac=SHA256
AES128-GCM-SHA256            TLSv1.2  Kx=RSA   Au=RSA  Enc=AESGCM(128)  Mac=AEAD
AES128-SHA256                TLSv1.2  Kx=RSA   Au=RSA  Enc=AES(128)     Mac=SHA256

The selected TLS cipher suites are used by the NTLS, STC outer tunnel, RBS, Ped vector
Server/Client features
TLS is using the following cipher suites:
Cipher suites are listed from highest to lowest priority.

Configured Ciphers (highest priority at top)
--------------------------------------------------
ECDHE-RSA-AES256-GCM-SHA384  TLSv1.2  Kx=ECDH  Au=RSA  Enc=AESGCM(256)  Mac=AEAD
ECDHE-RSA-AES256-SHA384      TLSv1.2  Kx=ECDH  Au=RSA  Enc=AES(256)     Mac=SHA384
DHE-RSA-AES256-GCM-SHA384    TLSv1.2  Kx=DH    Au=RSA  Enc=AESGCM(256)  Mac=AEAD
DHE-RSA-AES256-SHA256        TLSv1.2  Kx=DH    Au=RSA  Enc=AES(256)     Mac=SHA256
AES256-GCM-SHA384            TLSv1.2  Kx=RSA   Au=RSA  Enc=AESGCM(256)  Mac=AEAD
AES256-SHA256                TLSv1.2  Kx=RSA   Au=RSA  Enc=AES(256)     Mac=SHA256
```

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

Example exporting a template

```
lunash:>sysconf tls ciphers show -exportTemplate tls_template.txt

The following cipher suites are available to configure TLS:

Available Ciphers
--------------------------------------------------
TLS_AES_256_GCM_SHA384        TLSv1.3  Kx=any   Au=any  Enc=AESGCM(256)             Mac=AEAD
TLS_CHACHA20_POLY1305_SHA256  TLSv1.3  Kx=any   Au=any  Enc=CHACHA20/POLY1305(256)  Mac=AEAD
TLS_AES_128_GCM_SHA256        TLSv1.3  Kx=any   Au=any  Enc=AESGCM(128)             Mac=AEAD
ECDHE-RSA-AES256-GCM-SHA384   TLSv1.2  Kx=ECDH  Au=RSA  Enc=AESGCM(256)             Mac=AEAD
DHE-RSA-AES256-GCM-SHA384     TLSv1.2  Kx=DH    Au=RSA  Enc=AESGCM(256)             Mac=AEAD
ECDHE-RSA-AES128-GCM-SHA256   TLSv1.2  Kx=ECDH  Au=RSA  Enc=AESGCM(128)             Mac=AEAD
DHE-RSA-AES128-GCM-SHA256     TLSv1.2  Kx=DH    Au=RSA  Enc=AESGCM(128)             Mac=AEAD
ECDHE-RSA-AES256-SHA384       TLSv1.2  Kx=ECDH  Au=RSA  Enc=AES(256)                Mac=SHA384
DHE-RSA-AES256-SHA256         TLSv1.2  Kx=DH    Au=RSA  Enc=AES(256)                Mac=SHA256
ECDHE-RSA-AES128-SHA256       TLSv1.2  Kx=ECDH  Au=RSA  Enc=AES(128)                Mac=SHA256
DHE-RSA-AES128-SHA256         TLSv1.2  Kx=DH    Au=RSA  Enc=AES(128)                Mac=SHA256
AES256-GCM-SHA384             TLSv1.2  Kx=RSA   Au=RSA  Enc=AESGCM(256)             Mac=AEAD
AES128-GCM-SHA256             TLSv1.2  Kx=RSA   Au=RSA  Enc=AESGCM(128)             Mac=AEAD
AES256-SHA256                 TLSv1.2  Kx=RSA   Au=RSA  Enc=AES(256)                Mac=SHA256
AES128-SHA256                 TLSv1.2  Kx=RSA   Au=RSA  Enc=AES(128)                Mac=SHA256

The selected TLS cipher suites are used by the NTLS, STC outer tunnel, RBS, Ped vector
Server/Client features
TLS is using the following cipher suites:
Cipher suites are listed from highest to lowest priority.

Configured Ciphers (highest priority at top)
--------------------------------------------------
TLS_AES_256_GCM_SHA384        TLSv1.3  Kx=any   Au=any  Enc=AESGCM(256)             Mac=AEAD
TLS_CHACHA20_POLY1305_SHA256  TLSv1.3  Kx=any   Au=any  Enc=CHACHA20/POLY1305(256)  Mac=AEAD
TLS_AES_128_GCM_SHA256        TLSv1.3  Kx=any   Au=any  Enc=AESGCM(128)             Mac=AEAD
ECDHE-RSA-AES256-GCM-SHA384   TLSv1.2  Kx=ECDH  Au=RSA  Enc=AESGCM(256)             Mac=AEAD
DHE-RSA-AES256-GCM-SHA384     TLSv1.2  Kx=DH    Au=RSA  Enc=AESGCM(256)             Mac=AEAD
ECDHE-RSA-AES128-GCM-SHA256   TLSv1.2  Kx=ECDH  Au=RSA  Enc=AESGCM(128)             Mac=AEAD
DHE-RSA-AES128-GCM-SHA256     TLSv1.2  Kx=DH    Au=RSA  Enc=AESGCM(128)             Mac=AEAD
ECDHE-RSA-AES256-SHA384       TLSv1.2  Kx=ECDH  Au=RSA  Enc=AES(256)                Mac=SHA384
DHE-RSA-AES256-SHA256         TLSv1.2  Kx=DH    Au=RSA  Enc=AES(256)                Mac=SHA256
ECDHE-RSA-AES128-SHA256       TLSv1.2  Kx=ECDH  Au=RSA  Enc=AES(128)                Mac=SHA256
DHE-RSA-AES128-SHA256         TLSv1.2  Kx=DH    Au=RSA  Enc=AES(128)                Mac=SHA256
AES256-GCM-SHA384             TLSv1.2  Kx=RSA   Au=RSA  Enc=AESGCM(256)             Mac=AEAD
AES128-GCM-SHA256             TLSv1.2  Kx=RSA   Au=RSA  Enc=AESGCM(128)             Mac=AEAD
AES256-SHA256                 TLSv1.2  Kx=RSA   Au=RSA  Enc=AES(256)                Mac=SHA256
AES128-SHA256                 TLSv1.2  Kx=RSA   Au=RSA  Enc=AES(128)                Mac=SHA256

Generated cipher template file "tls_template.txt"



Command Result : 0 (Success)
```

sysconf user

Configure Luna Network HSM 7 appliance account management

> **CAUTION!** This feature is not supported for use with Clusters; do not enable it on any Luna Network HSM 7 that is a member of a cluster.

> **NOTE** This command requires Luna Appliance Software 7.9.0 or newer.

User Privileges

Users with the following privileges can perform these commands:

> Admin

Syntax

sysconf user

login
password
show

Subcommand(s)	Shortcut	Description
login	**l**	Configures login failure handling. See **"sysconf user login" on the next page**.
password	**p**	User password policies; configures password length, expiry, and history. See **"sysconf user password" on page 733**.
show	**s**	View the account management (password and login policies) configuration. See **"sysconf user show" on page 740**.

sysconf user login

Configures login rate limiting. A user account is locked temporarily upon consecutive failed logins within the set interval. The locked account is unlocked after the specified unlock/release interval.

> **CAUTION!** This feature is not supported for use with Clusters; do not enable it on any Luna Network HSM 7 that is a member of a cluster.

> **NOTE** This command requires Luna Appliance Software 7.9.0 or newer.

User Privileges

Users with the following privileges can perform this command:

> Admin

Syntax

sysconf user login [**-attempt** <number>] [**-release** <number>] [**-interval** <number>] [**-disable**]

Argument(s)	Shortcut	Description
-attempt <# allowed failed attempts>	**-a**	The maximum number of login failure attempts (within the allowed interval) before account lockout. Default = 3
-interval <window length>	**-i**	Failure detection interval or window; this is the span, in seconds, during which failed logins are counted (1-86400). The interval starts with a detected failed login. If more failed attempts occur during the interval, they are added to the count. If the count reaches the maximum allowed failed attempts, the account is locked out for a period determined by the **-release** parameter. If the window/interval expires without the lockout threshold of bad attempts being reached. The count is cleared and any new failed attempt starts the count again, and launches a new **-interval**. Default = 900 seconds
-release <lock release period>	**-r**	Lockout release. Time, in seconds, to unlock account after the lockout is triggered (1-86400). Default = 600 seconds
-disable	**-d**	Disables the policy. View the current settings with "sysconf user show" on page 740.

Example setting login policy to specific values

```
lunash:>sysconf user login -a 10 -r 3600 -i 900

Restarting ssh...

Login policy set successfully.

Command Result : 0 (Success)
lunash:>sysconf user show


Password policies:
======================
History : 3
Expire after : 90 days
Minimum length : 8 characters
Deny attempts : 10
Release interval : 3600 seconds
Detection window : 900 seconds

Command Result : 0 (Success)
```

Example disabling the login policy

```
lunash:>sysconf user login -disable

Restarting ssh...

Login policy disabled.

Command Result : 0 (Success)
lunash:>sysconf user show


Password policies:
======================
History : 3
Expire after : 90 days
Minimum length : 8 characters
Login policy : disabled

Command Result : 0 (Success)
```

sysconf user password

Configures password parameters of days until a new password expires, the number of previous passwords that are remembered when setting a new password, and the minimum length of a new password.

> **CAUTION!** This feature is not supported for use with Clusters; do not enable it on any Luna Network HSM 7 that is a member of a cluster.

> **NOTE** This command requires Luna Appliance Software 7.9.0 or newer.

User Privileges

Users with the following privileges can perform this command:

> Admin

Syntax

sysconf user password

expire
history
length

Argument(s)	Shortcut	Description
expire	**e**	The number of days, after a password change, that the password expires.If the user then attempts login after the current password has expired, they are prompted to set a new password before they can complete logging in. See **"sysconf user password expire" on the next page**.
history	**h**	Configures password history limit. When this is active, if a user attempts to set a password that matches any of the previous 'n' passwords, the user is prompted again to provide a new password. See **" sysconf user password history" on page 736**.
length	**l**	The minimum permitted number of characters in a user account password (8-30). See **"sysconf user password length" on page 738**.

sysconf user password expire

Configures login failure rate limiting. A user account is locked temporarily upon consecutive failed logins within the set interval. The locked account is unlocked after the specified unlock/release interval.

> **CAUTION!** This feature is not supported for use with Clusters; do not enable it on any Luna Network HSM 7 that is a member of a cluster.

> **NOTE** This command requires Luna Appliance Software 7.9.0 or newer.

User Privileges

Users with the following privileges can perform this command:

> Admin

Syntax

sysconf user password expire [<number>] [**-disable**]

Argument(s)	Shortcut	Description
<# days to pw expiry>	.	The number of days, after a password change, that the password expires. .If the user then attempts login after the current password has expired, they are prompted to set a new password before they can complete logging in. (1 - 365) Default = 90 Says 99999 days if expiry has not been set.
-disable	**-d**	Disables the password expiration policy. View the current settings with "sysconf user show" on page 740.

Example setting password expiry to a specific number of days

```
lunash:>sysconf user password expire 33

User password expiration set to 33 days successfully.

Command Result : 0 (Success)
lunash:>sysconf user show


Password policies:
=====================
History : 3
Expire after : 33 days
Minimum length : 8 characters
Deny attempts : 3
Release interval : 120 seconds
```

```
Detection window : 120 seconds

Command Result : 0 (Success)
```

Example setting password expiry to the default value

```
lunash:>sysconf user password expire

User password expiration set to 90 days successfully.

Command Result : 0 (Success)
lunash:>sysconf user show


Password policies:
=====================
History : 3
Expire after : 90 days
Minimum length : 8 characters
Deny attempts : 3
Release interval : 120 seconds
Detection window : 120 seconds

Command Result : 0 (Success)
```

Example of disabling password expiry

```
lunash:>sysconf user password expire -disable

User password expiration disabled.

Command Result : 0 (Success)
[docslab] lunash:>sysconf user show


Password policies:
=====================
History : 3
Expire after : disabled
Minimum length : 8 characters
Deny attempts : 3
Release interval : 120 seconds
Detection window : 120 seconds

Command Result : 0 (Success)
```

sysconf user password history

Configures password history limit. Once set, the user will be prompted to provide a new password if the one given during a password change has been used in the last 'n' attempts.

> **CAUTION!** This feature is not supported for use with Clusters; do not enable it on any Luna Network HSM 7 that is a member of a cluster.

> **NOTE** This command requires Luna Appliance Software 7.9.0 or newer.

User Privileges

Users with the following privileges can perform this command:

> Admin

Syntax

sysconf user password -history [<number>] [**-disable**]

Argument(s)	Shortcut	Description
<# previous passwords remembered>	.	Configures password history limit. When this is active, if a user attempts to set a password that matches any of the previous 'n' passwords, the user is prompted again to provide a new password. (1 - 10) Default = 4 Use **-disable** instead of a number to disable the password history setting.
-disable	**-d**	Disables the password history policy. View the current settings with "sysconf user show" on page 740.

Example

```
lunash:>sysconf user password history 3

Password history set to 3 successfully.

Command Result : 0 (Success)
lunash:>sysconf user show


Password policies:
====================
History : 3
Expire after : 99999 days
Minimum length : 8 characters
Deny attempts : 3
Release interval : 120 seconds
```

```
Detection window : 120 seconds

Command Result : 0 (Success)
```

sysconf user password length

Configures the minimum acceptable length of a new password.

> **CAUTION!** This feature is not supported for use with Clusters; do not enable it on any Luna Network HSM 7 that is a member of a cluster.

> **NOTE** This command requires Luna Appliance Software 7.9.0 or newer.

User Privileges

Users with the following privileges can perform this command:

> Admin

Syntax

sysconf user password -length [<number>]

Argument(s)	Shortcut	Description
<# minimum new password length>	.	Configures the minimum number of characters acceptable for a new password. (8 - 30) Default = 8 For security reasons, it is not possible to disable this policy, only to change it. View the current settings with "sysconf user show" on page 740.

Example (set password length to a specific number)

Specify any number between 8 and 30.

```
lunash:>sysconf user password length 10

Minimum password length set to 10 characters

Command Result : 0 (Success)
lunash:>sysconf user show


Password policies:
=====================
History : 3
Expire after : 33 days
Minimum length : 10 characters
Deny attempts : 3
Release interval : 120 seconds
Detection window : 120 seconds

Command Result : 0 (Success)
```

Example (set password length to the default)

Issue the command without a number.

```
lunash:>sysconf user password length

Minimum password length set to 8 characters

Command Result : 0 (Success)
lunash:>sysconf user show


Password policies:
====================
History : 3
Expire after : 33 days
Minimum length : 8 characters
Deny attempts : 3
Release interval : 120 seconds
Detection window : 120 seconds

Command Result : 0 (Success)
```

Disable password length enforcement

For security reasons, it is not possible to disable this policy, only to change it.

sysconf user show

Shows the configured password and login policies.

> **CAUTION!** This feature is not supported for use with Clusters; do not enable it on any Luna Network HSM 7 that is a member of a cluster.

> **NOTE** This command requires Luna Appliance Software 7.9.0 or newer.

User Privileges

Users with the following privileges can perform this command:

> Admin

Syntax

sysconf user show

Example

```
lunash:>sysconf user show


User account management summary
-------------------------------
-------------------------------

History : 3
Expire after : 10 days

Deny attemtpts : 10
Unlock interval : 3600 seconds
Failure interval : 900 seconds


Command Result : 0 (Success)
```

syslog

Access the syslog commands used to manage the system logs.

> **NOTE** Syslog uses system time. If you change the time zone setting for the appliance while syslog is running, syslog continues to log entries based on the old time zone until you restart the syslog service.

Syntax

syslog

cleanup
export
period
remotehost
rotate
rotations
severity
show
tail
tarlogs

Argument(s)	Shortcut	Description
cleanup	**c**	Delete log files. See "syslog cleanup" on the next page.
export	**e**	Export syslog. See "syslog export" on page 743.
period	**p**	Set the syslog period. See "syslog period" on page 744.
remotehost	**re**	Configure Syslog remote hosts. See "syslog remotehost" on page 746.
rotate	**rotate**	Rotate log files. See "syslog rotate" on page 745.
rotations	**rotati**	Set syslog rotations. See "syslog rotations" on page 759
severity	**se**	Log severity. See "syslog severity set" on page 760.
show	**sh**	Get Syslog configuration. See "syslog show" on page 761.
tail	**tai**	Get last entries of log. See "syslog tail" on page 762.
tarlogs	**tar**	Archive log files. See "syslog tarlogs" on page 764.

syslog cleanup

Delete log files. Using this command following **syslog rotate** causes all grow-able log files to be deleted.

User Privileges

Users with the following privileges can perform this command:

> Admin

Syntax

syslog cleanup [**-force**]

Argument(s)	Shortcut	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.
If you are sure that you wish to proceed, then type 'proceed', otherwise type 'quit'.

> proceed
Proceeding...
Creating tarlogs then deleting all log files...

The tar file containing logs is now available via sftp as filename "logs_cleanup_20250301_
1443.tgz".
Please copy "logs_cleanup_20250301_1443.tgz" to a client machine with scp.

Deleting log files ...
restart the rsyslogd service if it's running
Stopping syslog:                                           [  OK  ]

Starting syslog:                                           [  OK  ]


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 **sftp** 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 Network HSM 7 appliance.

User Privileges

Users with the following privileges can perform this command:

- Admin
- Operator

Syntax

syslog export

Example

```
lunash:>syslog export


System log files successfully prepared for secure transfer.
Use sftp from a client machine to get the file named: "syslog"


Command Result : 0 (Success)
```

 Copyright 2001-2025 Thales Group

syslog period

Set the time between syslog rotations.

User Privileges

Users with the following privileges can perform this command:

- Admin
- Operator

Syntax

syslog period <syslogperiod>

Argument(s)	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.

User Privileges

Users with the following privileges can perform this command:

- Admin
- Operator

Syntax

syslog rotate

Example

```
lunash:>syslog rotate


Command Result : 0 (Success)
```

syslog remotehost

Access the **syslog remotehost** commands to manage the syslog remote hosts. (See Remote System Logging)

Syntax

syslog remotehost

add
cert
clear
delete
list

Argument(s)	Shortcut	Description
add	**a**	Add a remote host. See "syslog remotehost add" on the next page.
cert	**ce**	Add or delete CA and Client certificates. See "syslog remotehost cert" on page 749.
clear	**cl**	Delete All Remote Logging Servers. See "syslog remotehost clear" on page 756.
delete	**d**	Delete a remote host. See "syslog remotehost delete" on page 757.
list	**l**	List all syslog remote hosts. See "syslog remotehost list" on page 758.

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.

> **NOTE** Attempting to add the same host, port configuration as the audit user (another LNH user) results in an error.

User Privileges

Users with the following privileges can perform this command:

- Admin
- Operator

Syntax

syslog remotehost add -host <hostname/IP> [**-protocol** <protocol>] [**-port** <port>][**-mode** <authmode>] [**-name** <commonname>] [**-tls**]

Argument(s)	Shortcut	Description
-host <hostname/IP>	**-h**	Specifies the hostname or the IP address of the remote computer system that will be accepting and storing the syslogs.
-protocol <protocol>	**-pr**	Specifies the network protocol. **Valid values:** tcp,udp, relp RELP protocol is not available when server mode is selected The **-name** option is required when the protocol is **relp**
-port <port>	**-po**	Remote Logging Server port number. **Range:** 0-65535 **Default:** 514
-mode <authmode>	**-m**	Authentication mode. **Valid values:** server, mutual
-name <commonname>	**-n**	Server common name. The **-name** option is required when the protocol is **relp**
-tls	**-t**	Setup host with tls.

Example

```
lunash:>syslog remotehost add -host 192.12.1.123

Stopping syslog:                                           [  OK  ]

Starting syslog:                                           [  OK  ]

192.12.1.123 added successfully
Make sure the rsyslog service on 192.12.1.123 is properly configured to receive the logs

Command Result : 0 (Success)
```

Example Configuring Remote Server with Server-authentication, TCP, and Self-signed Certs on Non-default Port

```
lunash:>syslog remotehost cert installca server_self_cert.pem
Attempting to install server_self_cert.pem
CA certificate installed successfully.
The syslog service needs to be (re)started before a secure connection can be established.

Command Result : 0 (Success)

lunash:>syslog remotehost add -host 192.168.140.45 -protocol tcp -port 30004 -mode server -tls
Stopping syslog:                                           [  OK  ]
Starting syslog:                                           [  OK  ]
192.168.140.45 added successfully
Make sure the rsyslog service on 192.168.140.45 is properly configured to receive the logs

Command Result : 0 (Success)

lunash:>syslog remotehost list
Remote logging server(s):
=========================
[192.168.140.45]:30004, tcp, tls

Command Result : 0 (Success)
```

syslog remotehost cert

Access the **syslog remotehost cert** commands to manage the syslog remote host certificates. (See Syslog Encryption)

Syntax

syslog remotehost cert

delete
deleteCA
gen
install
installCA

Argument(s)	Shortcut	Description
delete	**d**	Delete an HSM certificate. See "syslog remotehost cert delete" on the next page.
deleteCA	**deleteC**	Delete a CA certificate. See "syslog remotehost cert deleteCA" on page 751.
gen	**g**	Generates a CSR or client certificate. See "syslog remotehost cert gen" on page 752.
install	**i**	Installs the HSM certificate. See "syslog remotehost cert install" on page 754.
installCA	**installC**	Installs the CA certificate. See "syslog remotehost cert installCA" on page 755.

.

syslog remotehost cert delete

Delete the HSM certificate.

User Privileges

Users with the following privileges can perform this command:

> Admin

> Operator

Syntax

syslog remotehost cert delete [**-force**]

Argument(s)	Shortcut	Description
-force	**-f**	Deletes the installed certificate without warning the user if it already exists.

Example

```
lunash:>syslog remotehost cert delete -force


Command Result : 0 (Success)
```

syslog remotehost cert deleteCA

Delete the CA certificate.

User Privileges

Users with the following privileges can perform this command:

> Admin

> Operator

Syntax

syslog remotehost deleteCA [**-force**]

Argument(s)	Shortcut	Description
-force	**-f**	Deletes the installed CA certificate without warning the user if it already exists.

Example

```
lunash:>syslog remotehost cert deleteCA -force


Command Result : 0 (Success)
```

syslog remotehost cert gen

Generates a private key and CSR.

or

Generates a private key and self-signed certificate.

> **CAUTION!** The **syslog remotehost cert gen** command and the **audit remotehost cert gen** command affect the same certificate, in the same file system location within the Luna Network HSM 7appliance. If either the *admin* user or the *audit* user makes a change to an existing certificate, it affects both:
>
> > the encrypted remote logging of appliance events and
> >
> > the encrypted remote logging of cryptographic module events.
>
> Before using the **...cert gen** command, in either context (*admin* and syslog remotehost, or *audit* and audit remotehost) use the respective **...cert status** command to see whether a shared certificate is already configured.

User Privileges

Users with the following privileges can perform this command:

> Admin
>
> Operator

Syntax

syslog remotehost cert gen [<ipaddress>] [**-startdate** <startdate>] [**-days** <days>] [**-country** <iso_country_code>] [**-state** <name_of_state_province_region>] [**-location** <city_name>] [**-organization** <organization_legal_name>] [**-orgunit** <division_within_org>] [**-email** <contact_email_address>] [**-san** <SAN>] [**-keysize** <size>] [**-keytype** <key_type>] [**-curve** <curve_name>] [**-csr**][**-force**]

Argument(s)	Shortcut	Description
.	. <ipaddress>	Generates a CSR, or the self-signed client certificate client_syslog.pem in the file-space of the user that generated the cert Default: 1.2.3.4
-startdate <startdate>	**-star**	Certificate start date(not available with -csr) (0-99991231).
-days <days>	**-d**	Certificate validity days (1-3653)
-country <country code>	**-co**	The country in which your organization is located, entered as a two-letter ISO code.
-state <State/Region/Province (full name)>	**-stat**	The state or region in which your organization is located. (Example Québec)

Argument(s)	Shortcut	Description
-location <city name>	**-l**	The city in which your organization is located.
-organization	**-orga**	The full legal name of your organization, including suffixes such as LLC, Corp, etc.
-orgunit	**-orgu**	The division in your organization that deals with this certificate.
-email	**-e**	Email address used to contact the owner.
-san <subject alternative name>	**-sa**	In addition to the FQDN if you intend to support other subdomains
-keysize <size>	**-keys**	RSA key size: Default: 2048 (choose among 2048,3072,4096)
-keytype <keytype>	**-keyt**	Key type (ecc,rsa) Default: rsa
-curve <curve_name>	**-cu**	Elliptic Curve name Supported values: secp256k1, secp384r1, secp521r1, prime256v1 Default: secp384r1
-csr	**-cs**	Generate CSR - client certificate request file `client_syslog_csr.csr` in the file-space of the user that generated the cert request
-force	**-f**	Deletes the installed certificate without warning the user if it already exists.

An error is shown if CSR generation fails, or if certificate generation fails.

Disallowed option combinations

Do not included the **-curve** option if the **-keytype** is "rsa".

Do not included the **-keysize** option if the **-keytype** is "ecc".

Example

```
lunash:>syslog remotehost cert gen 10.124.79.157 -csr -startdate 20230410 -days 10 -country CA
-state ON -organization Thales -orgunit dis -location OT -email example@thales.com

CSR generated successully.
Command Result : 0 (Success)
.
```

syslog remotehost cert install

Install the HSM certificate.

User Privileges

Users with the following privileges can perform this command:

> Admin

> Operator

Syntax

syslog remotehost cert install <filename> [**-force**]

Argument(s)	Shortcut	Description
. <filename>	**.**	Filename of the received CA-signed HSM certificate to install.
-force	**-f**	Forces the action for scripting.

Example

```
lunash:>syslog remotehost cert install client_sign.pem

Attempting to install client_sign.pem

HSM certificate installed successfully.
The syslog service needs to be (re)started before a secure connection can be enabled.


Command Result : 0 (Success)
```

(In the above example, client_sign.pem is the signed CSR of the HSM.)

syslog remotehost cert installCA

Install the CA certificate.

User Privileges

Users with the following privileges can perform this command:

> Admin

> Operator

Syntax

syslog remotehost cert installCA <filename> [**-force**]

Argument(s)	Shortcut	Description
. <filename>	**.**	Filename of the received CA certificate to install.
-force	**-f**	Forces the action for scripting.

Example

```
lunash:>syslog remotehost cert installCA -force


Command Result : 0 (Success)
```

syslog remotehost clear

Delete all remote logging servers.

User Privileges

Users with the following privileges can perform this command:

> Admin

> Operator

Syntax

syslog remotehost clear [**-force**]

Argument(s)	Shortcut	Description
-force	**-f**	Force the action; useful for scripting.

Example

```
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

Stopping syslog:                                          [  OK  ]

Starting syslog:                                          [  OK  ]


Command Result : 0 (Success)
```

syslog remotehost delete

Delete a remote host receiving the logs. Use **syslog remotehost list** to see which systems are receiving the logs.

User Privileges

Users with the following privileges can perform this command:

- Admin
- Operator

Syntax

syslog remotehost delete -host <hostname/IP> [**port**<port>]

Argument(s)	Shortcut	Description
-host <hostname/IP>	**-h**	Specifies the hostname or the IP address of the remote computer system to delete from the list.
-port <hostname/IP>	**-p**	Specifies the port number of the remote computer system to delete from the list.

Example

```
lunash:>syslog remotehost delete -host 192.20.9.144

    WARNING!  This action will delete the remote server configuration for 192.20.9.144
    If you are sure that you wish to proceed, then type 'proceed, otherwise type 'quit'

    > proceed
    Proceeding...


Stopping syslog:                                           [  OK  ]

Starting syslog:                                           [  OK  ]


Command Result : 0 (Success)
```

syslog remotehost list

List the syslog remote hosts.

User Privileges

Users with the following privileges can perform this command:

- Admin
- Operator

Syntax

syslog remotehost list

Example

```
lunash:>syslog remotehost list

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

  192.20.9.160:6767, tls
  192.20.11.158:514, tcp
  192.20.11.155:514, udp


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.

User Privileges

Users with the following privileges can perform this command:

- Admin
- Operator

Syntax

syslog rotations <#_of_rotations>

Argument(s)	Description
<#_of_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)
```

syslog severity set

Set the log service severity threshold for events to be logged.

> **NOTE** This feature requires minimum Luna Network HSM 7 Appliance Software 7.2.0.

User Privileges

Users with the following privileges can perform this command:

> Admin

Syntax

syslog severity set -logname <logname> **-loglevel** <loglevel> [**-host** <hostname/IP>]

Argument(s)	Shortcut	Description
-loglevel <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,all **NOTE:** These values are arranged from those which produce the fewest to the most log entries. Each level includes all the levels above it. For example, setting the log level to **critical** will gather all **emergency**, **alert**, and **critical** events.
-logname <logname>	**-logn**	The name of the log file to which you want to apply severity levels. **Valid values:** lunalogs,clusterlogs,messages,cron,secure,boot)
-host <hostname/IP>	**-h**	The remote host that will receive the logs. Add new hosts with "syslog remotehost add" on page 747. The hosts must be configured to receive logs.

Example

```
lunash:>syslog severity set -logname lunalogs -loglevel crit

This command sets the severity level of lunalogs local log messages.
Only messages with the severity equal to or higher than the new
log level: "crit" will be logged.

Stopping syslog:                                           [  OK  ]

Starting syslog:                                           [  OK  ]

Command Result : 0 (Success)
```

syslog show

Display the current log rotation configuration and log levels. Optionally, show a list of the log files.

User Privileges

Users with the following privileges can perform this command:

- Admin
- Operator
- Monitor

Syntax

syslog show [**-files**]

Argument(s)	Shortcut	Description
-files	**-f**	Show a list of all log files, in addition to the current log configuration.

Example

In the example below, the asterisks indicate that ALL events are logged and that this setting is not user configurable.

```
lunash:>syslog show


Syslog configuration

   Rotations:         12

   Rotation Period:   weekly

   Log disk full policy:    tarlogs_cleanup

Local Configured Log Levels:
----------------------------
lunalogs:           info
messages:           *
cron:               notice
secure:             *
boot:               *
clusterlogs:        info

Note: '*' means all log levels.



Command Result : 0 (Success)
```

syslog tail

Display the last entries of the syslog. If no number is included, the command displays the entire syslog.

User Privileges

Users with the following privileges can perform this command:

- Admin
- Operator
- Monitor

Syntax

syslog tail -logname <logname> [**-entries** <#entries>] [**-search** <string>]

Argument(s)	Shortcut	Description
-entries <#entries>	**-e**	Specifies the number of entries to display. If this parameter is not specified, the entire log is displayed. **Range:** 0-4294967295
-logname <logname>	**-l**	Specifies the log name. **Valid values:** lunalogs,messages,secure,ntp,snmp,clusterlogs **NOTE:** The **hsm** option is not available in this release. To see HSM-specific logs, use the **messages** option.
-search <string>	**-s**	Search for the specified string. **NOTE:** To search the logs for HSM Alarm messages, for example, include this option with the string "ALM".

Example

```
lunash:>syslog tail -logname lunalogs -entries 8

2017 Mar  1 14:27:54 local_host  local5 info  hsm[32081]: STC policy is set to "OFF" on
partition 66331 : Unknown ResultCode value
2017 Mar  1 14:27:55 local_host  local5 info  hsm[32120]: STC policy is set to "OFF" on
partition 66331 : Unknown ResultCode value
2017 Mar  1 14:29:53 local_host  local5 info  hsm[3948]: STC policy is set to "OFF" on
partition 66331 : Unknown ResultCode value
2017 Mar  1 14:29:59 local_host  local5 info  lunash [29529]: info : 0 : Command: syslog
remotehost add  : admin : 10.124.0.87/61470
2017 Mar  1 14:30:37 local_host  local5 info  hsm[5511]: STC policy is set to "OFF" on
partition 66331 : Unknown ResultCode value
2017 Mar  1 14:30:48 local_host  local5 info  lunash [29529]: info : 0 : Command: syslog
remotehost list  : admin : 10.124.0.87/61470
2017 Mar  1 14:33:10 local_host  local5 info  lunash [29529]: info : 0 : Command: syslog
severity set  : admin : 10.124.0.87/61470
2017 Mar  1 14:33:47 local_host  local5 info  lunash [29529]: info : 0 : Command: syslog
```

```
severity set -logname lunalogs -loglevel crit : admin : 10.124.0.87/61470

Command Result : 0 (Success)
```

Error message when using -logname hsm

```
lunash:>syslog tail -logname hsm

HSM log does not exist

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

syslog tarlogs

Archives log files to logs.tar file in the current user's temporary directory. A single logs.tgz file allows you to obtain all the logs in one operation.

User Privileges

Users with the following privileges can perform this command:

- Admin
- Operator
- Monitor

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 backup

Access the **token backup** commands for operating a Luna Backup HSM connected to a USB port on the Luna Network HSM 7 appliance. These commands are not intended for use with remotely-connected backup devices using a Remote Backup Server (RBS).

An external Luna Backup HSM can be USB-connected to a Luna Network HSM 7 appliance for local backup/restore operations.

Luna Network HSM 7 does not pass Luna PED operations and data through to an externally-connected Luna Backup HSM from a Luna PED connected locally to the Luna Network HSM 7.

If the Backup HSM is multifactor quorum-authenticated, then the options for Luna PED connection are:

> local SCP-PED connection directly to the Backup HSM (Luna Backup HSM G5 only)

> Remote PED connection, passed through the Luna Network HSM 7 (Luna Backup HSM G5, Luna Backup HSM 7 v1 or v2, requires minimum Luna Network HSM 7 Appliance Software 7.7.0, use procedure for Luna Backup HSM 7 Connected to Luna Network HSM 7 Using Remote Multifactor Quorum Authentication)

Syntax

token backup

factoryreset
init
list
login
logout
partition
show
update

Argument(s)	Shortcut	Description
factoryreset	**f**	Reset a Luna Backup HSM to factory default settings. See "token backup factoryReset" on page 767.
init	**i**	Initializes the Backup HSM with the specified serial number and prepares it to receive backup data. See "token backup init" on page 769.
list	**li**	List all connected Backup HSMs. See "token backup list" on page 771.
login	**logi**	Log in to the Backup HSM as SO. See "token backup login" on page 772.
logout	**logo**	Log out the Backup HSM SO. See "token backup logout" on page 773.

Argument(s)	Shortcut	Description
partition	**p**	Access the token backup partition commands to manage your backup partitions. See "token backup partition" on page 774.
show	**s**	Get Backup HSM information. See "token backup show" on page 781.
update	**u**	Backup HSM firmware update commands. See "token backup update" on page 784.

token backup factoryReset

Reset a Luna Backup HSM 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: Comparison of Destruction/Denial Actions

An external Luna Backup HSM can be USB-connected to a Luna Network HSM 7 appliance for local backup/restore operations.

Luna Network HSM 7 does not pass Luna PED operations and data through to an externally-connected Luna Backup HSM from a Luna PED connected locally to the Luna Network HSM 7.

If the Backup HSM is multifactor quorum-authenticated, then the options for Luna PED connection are:

> local SCP-PED connection directly to the Backup HSM (Luna Backup HSM G5 only)

> Remote PED connection, passed through the Luna Network HSM 7 (Luna Backup HSM G5, Luna Backup HSM 7 v1 or v2, requires minimum Luna Network HSM 7 Appliance Software 7.7.0, use procedure for Luna Backup HSM 7 Connected to Luna Network HSM 7 Using Remote Multifactor Quorum Authentication)

User Privileges

Users with the following privileges can perform this command:

> Admin

> Operator

Syntax

token backup factoryReset -serial <serialnum> **[-force**]

Argument(s)	Shortcut	Description
-serial <serialnum>	**-s**	Specifies the Backup HSM serial number.
-force	**-f**	Force the action without prompting.

Example

```
lunash:>token backup factoryReset -serial 496771

CAUTION:  Are you sure you wish to reset this backup token to
          factory default settings? All data will be erased.

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

'token backup factoryReset' successful.
```

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

token backup init

Initializes the Backup HSM 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 password-authenticated Luna Backup HSMs, the domain and HSM SO password are prompted, and your input is obscured by asterisk (*) symbols. For multifactor quorum-authenticated HSMs, any typed values for domain or password are ignored and you are prompted for Luna PED operations with PED keys.

An external Luna Backup HSM can be USB-connected to a Luna Network HSM 7 appliance for local backup/restore operations.

Luna Network HSM 7 does not pass Luna PED operations and data through to an externally-connected Luna Backup HSM from a Luna PED connected locally to the Luna Network HSM 7.

If the Backup HSM is multifactor quorum-authenticated, then the options for Luna PED connection are:

> local SCP-PED connection directly to the Backup HSM (Luna Backup HSM G5 only)

> Remote PED connection, passed through the Luna Network HSM 7 (Luna Backup HSM G5, Luna Backup HSM 7 v1 or v2, requires minimum Luna Network HSM 7 Appliance Software 7.7.0, use procedure for Luna Backup HSM 7 Connected to Luna Network HSM 7 Using Remote Multifactor Quorum Authentication)

User Privileges

Users with the following privileges can perform this command:

> Admin

> Operator

Syntax

token backup init -label <label> **-serial** <serialnum> **[-domain** <domain>] [**-tokenadminpw** <password>] [**-force**]

Argument(s)	Shortcut	Description
-domain <domain>	**-d**	Backup partition domain (required for password-authenticated HSMs, ignored for multifactor quorum-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 <label>	**-l**	Backup partition label.
-serial <serialnum>	**-s**	Luna Backup HSM serial number.
-tokenadminpw <password>	**-t**	Backup HSM SO password (required for password-authenticated HSMs, ignored for multifactor quorum-authenticated - if you prefer to not type it in the clear, on the command line, it is prompted later).

Example

```
lunash:>token backup init -label sa7docbackup -serial 496771

  Please enter a password for the Token Administrator:
  > ********

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

  Please enter a cloning domain used when initializing this HSM:
  > *********

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

CAUTION:  Are you sure you wish to initialize the backup
          token named:   sa7docbackup
          Type 'proceed' to continue, or 'quit' to quit now.
          > proceed

'token backup init' successful.

Command Result : 0 (Success)
```

token backup list

Display a list all of the Luna Backup HSMs connected to the system, their firmware versions, and 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.

User Privileges

Users with the following privileges can perform this command:

- Admin
- Operator
- Monitor

Syntax

token backup list

Example

```
lunash:>token backup list

  Token Details:
  ============
  Token Label:                        sa78backup
  Slot:                               1
  Serial #:                           496771
  Firmware:                           6.27.0
  HSM Model:                          G5Backup


Command Result : 0 (Success)
```

token backup login

Log into the backup HSM as HSM SO. This command is used immediately before performing a firmware update on a backup token.

Remember to always log out of the Backup HSM using the **token backup logout** command.

An external Luna Backup HSM can be USB-connected to a Luna Network HSM 7 appliance for local backup/restore operations.

Luna Network HSM 7 does not pass Luna PED operations and data through to an externally-connected Luna Backup HSM from a Luna PED connected locally to the Luna Network HSM 7.

If the Backup HSM is multifactor quorum-authenticated, then the options for Luna PED connection are:

> local SCP-PED connection directly to the Backup HSM (Luna Backup HSM G5 only)

> Remote PED connection, passed through the Luna Network HSM 7 (Luna Backup HSM G5, Luna Backup HSM 7 v1 or v2, requires minimum Luna Network HSM 7 Appliance Software 7.7.0, use procedure for Luna Backup HSM 7 Connected to Luna Network HSM 7 Using Remote Multifactor Quorum Authentication)

User Privileges

Users with the following privileges can perform this command:

> Admin

> Operator

Syntax

token backup login -serial <serialnum> [**-password** <password>]

Argument(s)	Shortcut	Description
-serial <serialnum>	**-s**	Specifies the serial number of the Backup HSM.
-password <password>	**-p**	Specifies the Backup HSM SO's password. If this option is not specified, LunaSH prompts for the password entry.

Example

```
lunash:>token backup login -serial 496771


  Please enter Token Administrator's password:
  > ********

'token backup login' successful.


Command Result : 0 (Success)
```

token backup logout

Log out the Luna Backup HSM SO from the Backup HSM.

User Privileges

Users with the following privileges can perform this command:

> Admin

> Operator

Syntax

token backup logout -serial <serialnum>

Argument(s)	Shortcut	Description
-serial <serialnum>	**-s**	Specifies the serial number of the Backup HSM.

Example

```
lunash:>token backup logout -serial 496771


'token logout' successful.


Command Result : 0 (Success)
```

token backup partition

Access the token backup partition commands to manage your backup partitions.

An external Luna Backup HSM can be USB-connected to a Luna Network HSM 7 appliance for local backup/restore operations.

Luna Network HSM 7 does not pass Luna PED operations and data through to an externally-connected Luna Backup HSM from a Luna PED connected locally to the Luna Network HSM 7.

If the Backup HSM is multifactor quorum-authenticated, then the options for Luna PED connection are:

> local SCP-PED connection directly to the Backup HSM (Luna Backup HSM G5 only)

> Remote PED connection, passed through the Luna Network HSM 7 (Luna Backup HSM G5, Luna Backup HSM 7 v1 or v2, requires minimum Luna Network HSM 7 Appliance Software 7.7.0, use procedure for Luna Backup HSM 7 Connected to Luna Network HSM 7 Using Remote Multifactor Quorum Authentication)

Syntax

token backup partition

delete
list
show

Argument(s)	Shortcut	Description
delete	**d**	Delete a backup partition. See "token backup partition delete" on the next page
list	**l**	List the backup partitions. See "token backup partition list" on page 777.
show	**s**	List the objects on a backup partition. See "token backup partition show" on page 778.

token backup partition delete

Delete a backup partition on the Luna Backup HSM. To use the **token backup partition delete** command you must be logged in to the Backup HSM as HSM SO.

An external Luna Backup HSM can be USB-connected to a Luna Network HSM 7 appliance for local backup/restore operations.

Luna Network HSM 7 does not pass Luna PED operations and data through to an externally-connected Luna Backup HSM from a Luna PED connected locally to the Luna Network HSM 7.

If the Backup HSM is multifactor quorum-authenticated, then the options for Luna PED connection are:

> local SCP-PED connection directly to the Backup HSM (Luna Backup HSM G5 only)

> Remote PED connection, passed through the Luna Network HSM 7 (Luna Backup HSM G5, Luna Backup HSM 7 v1 or v2, requires minimum Luna Network HSM 7 Appliance Software 7.7.0, use procedure for Luna Backup HSM 7 Connected to Luna Network HSM 7 Using Remote Multifactor Quorum Authentication)

User Privileges

Users with the following privileges can perform this command:

> Admin

> Operator

Syntax

token backup partition delete -partition <partition_name> **-serial** <serialnum> [**-force**]

Argument(s)	Shortcut	Description
-force	**-f**	Specifies that the backup partition is erased without prompting the user for a confirmation of this destructive command.
-partition <partition_name>	**-p**	Specifies the name of the backup partition to delete. Obtain the backup partition name by using the **token backup partition list** command.
-serial <serialnum>	**-s**	Specifies the serial number of the backup partition to delete. Obtain the backup partition serial number by using the **token backup partition list** command.

Example

```
lunash:>token backup partition delete -partition sa78par1backup -serial 496771


CAUTION:  Are you sure you wish to delete the partition named:
            sa78par1backup
          Type 'proceed' to delete the partition, or 'quit'
          to quit now.
          > proceed
```

```
'token backup partition delete' successful.

Command Result : 0 (Success)
```

token backup partition list

Display a list of the backup partitions on the specified Luna Backup HSM. The serial number and name of each partition is displayed. Login as HSM SO is not needed for execution of this command.

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."

User Privileges

Users with the following privileges can perform this command:

- Admin
- Operator
- Monitor

Syntax

token backup partition list -serial <serialnum>

Argument(s)	Shortcut	Description
-serial <serialnum>	**-s**	Specifies the serial number of the Backup HSM.

Example

```
lunash:>token backup partition list -serial 496771


                                                        Storage (bytes)
                                                 ----------------------------
 Partition    Name                       Objects     Total      Used      Free
 ==========================================================================
 496771005  sa78par1backup                     6      9480      9348       132
 496771010  sa78par2backup                    12     18960     18696       264


Command Result : 0 (Success)
```

token backup partition show

Display a list of objects on the backup partition.

> **NOTE** A backed-up SMK does not appear as an object on the backup partition; find its OUID under `Partition SMK OUIDs` (see example below).

User Privileges

Users with the following privileges can perform this command:

- Admin
- Operator
- Monitor

Syntax

token backup partition show -partition [<partitionName>] **-serial** <serialnum> **-password** <backup_token/hsm_userPassword>

Argument(s)	Shortcut	Description
-password <tokenpartitionpassword>	**-pas**	Specifies the password of the backup 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 <tokenpartitionname>	**-par**	Specifies the name of the backup 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 <tokenserialnumber>	**-s**	The serial number of the backup partition for which to display information. By default information about all partitions is shown. Obtain the partition name by using the **partition list** command.

V1 Partition SMK Example

```
lunash:>token backup partition show -serial 999999 -partition clusterSMKbackup


  Please enter the user password for the token:
  > ********

   Partition Name:                          clusterSMKbackup
   Partition SN:                               1659497773253
   Partition Label:                         clusterSMKbackup
   Partition Version:                                     0
   Storage (Bytes): Total=0, Used=0, Free=0
   No objects are currently stored in this partition.
```

```
   Partition SMK OUIDs:
                SMK-FW4: Not Initialized
                SMK-FW6: Not Initialized
                SMK-FW7-FM: Not Initialized
                SMK-FW7-Rollover: Not Initialized
                SMK-FW7-Primary: 50000000110000011b030100

Command Result : 0 (Success)
```

V0 or pre-7.7.0 Partition Example

```
lunash:>token backup partition show -serial 999999 -partition objectparBU



  Please enter the user password for the token:
  > ********

   Partition Name:                                objectparBU
   Partition SN:                                1659497773254
   Partition Label:                               objectparBU
   Partition Version:                                       0
   Storage (Bytes): Total=9640, Used=9640, Free=0
   Number objects:  10

   Object Label:  MT RSA 2048-bit Public KeyGen
   Object Type:   Public Key
   Object Handle: 1954

   Object Label:  MT RSA 2048-bit Private KeyGen
   Object Type:   Private Key
   Object Handle: 1951

   Object Label:  MT RSA 2048-bit Public KeyGen
   Object Type:   Public Key
   Object Handle: 1950

   Object Label:  MT RSA 2048-bit Private KeyGen
   Object Type:   Private Key
   Object Handle: 1922

   Object Label:  MT RSA 2048-bit Public KeyGen
   Object Type:   Public Key
   Object Handle: 1921

   Object Label:  MT RSA 2048-bit Private KeyGen
   Object Type:   Private Key
   Object Handle: 1918

   Object Label:  MT RSA 2048-bit Public KeyGen
   Object Type:   Public Key
   Object Handle: 893

   Object Label:  MT RSA 2048-bit Private KeyGen
   Object Type:   Private Key
   Object Handle: 868

   Object Label:  MT RSA 2048-bit Public KeyGen
```

```
   Object Type:   Public Key
   Object Handle: 866

   Object Label:  MT RSA 2048-bit Private KeyGen
   Object Type:   Private Key
   Object Handle: 591

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

Command Result : 0 (Success)
```

token backup show

Displays the label and firmware version for the specified Luna Backup HSM.

> **CAUTION!** Wait at least 20 seconds before you run the **token backup show** command after performing a backup token 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 disconnect and reconnect the Backup HSM and then rerun the **token backup show** command.

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."

User Privileges

Users with the following privileges can perform this command:

- Admin
- Operator
- Monitor

Syntax

token backup show -serial <serialnum>

Argument(s)	Shortcut	Description
-serial <serialnum>	**-s**	The serial number of the Luna Backup HSM.

Luna Backup HSM 7 Example

```
lunash:>token backup show -serial 132525


   Token Details:
   ============
   Token Label:                        BackupTest
   Serial #:                           132525
   Firmware:                           7.3.2
   HSM Model:                          Luna G7
   Authentication Method:              Password
   Token Admin login status:           Not Logged In
   Token Admin login attempts left:    3 before Token zeroization!

   Partition Information:
```

```
   =======================
   Partitions licensed on token:       100
   Partitions created on token:        2
   ----------------------
   Partition: 132525004,     Name: backup1
   Partition: 13252552391,     Name: user_20200717161026

   Token Storage Information:
   ==========================
   Maximum Token Storage Space (Bytes):   33816576
   Space In Use (Bytes):                  30086384
   Free Space Left (Bytes):               3730192

   License Information:
   ====================
   621000121-000      G7 BU 32M Base CUF December 7 2018


Command Result : 0 (Success)
```

> **NOTE** Starting with Luna Backup HSM 7 Firmware 7.7.1, this command reports 679584 bytes of overhead under Space in Use after initialization.

Luna Backup HSM G5 Example

```
lunash:>token backup show -serial 496771


   Token Details:
   ============
   Token Label:                        sa78backup
   Serial #:                           496771
   Firmware:                           6.27.0
   HSM Model:                          G5Backup
   Authentication Method:              Password
   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:        2
   ----------------------
   Partition: 496771005,     Name: sa78par1backup
   Partition: 496771010,     Name: sa78par2backup

   Token Storage Information:
   ==========================
   Maximum Token Storage Space (Bytes):   16252928
   Space In Use (Bytes):                  32752
   Free Space Left (Bytes):               16220176

   License Information:
   ====================
   001111-012      G5 Backup Config - 001111-012
   004444-012      Test BackupToken RemotePed - 004444-012
   004444-006      Test BackupToken Partitions 20 Update - 4444-006
```

```
   004444-009      Test BackupToken HSM Storage 15.5 Meg - 004444-009
   004444-008      Test BackupToken External MTK Update 2 - 004444-008


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.

Syntax

token backup update

capability
firmware
show

Argument(s)	Shortcut	Description
capability	**c**	Update the capabilities for a Luna Backup HSM. See "token backup update capability" on the next page. **NOTE** This command is deprecated as capability upgrades are included in firmware updates. See "token backup update firmware" on page 787.
firmware	**f**	Update the firmware on a Luna Backup HSM. See "token backup update firmware" on page 787.
show	**s**	Show a list of the available Luna Backup HSM updates. See "token backup update show" on page 789.

token backup update capability

Update a Luna Backup HSM Capability, using a capability update package that you have acquired from Thales and transferred via **pscp**/**sftp** to the Luna Network HSM 7 appliance. Before you can use this command, you must:

> Acquire the secure package update file from Thales and send the file to the Luna Network HSM 7 (using **pscp** or **sftp**)

> Open the file on the Luna Network HSM 7 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.

> **NOTE** This command is deprecated as capability upgrades are included in firmware updates. See "token backup update firmware" on page 787.

User Privileges

Users with the following privileges can perform this command:

> Admin

> Operator

Syntax

token backup update capability -serial <serialnum> **-capability** <capabilityname> [**-force**]

Argument(s)	Shortcut	Description
-capability <capabilityname>	**-c**	Specifies the capability name.
-force	**-f**	Force the action without prompting.
-serial <serialnum>	**-s**	Specifies the Backup HSM 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 Luna Backup HSM, using a firmware update package available on the Luna Network HSM 7 appliance. The package must be transferred to the appliance by **pscp**/**sftp** (individually or as a component of a system update), and you must log in to the Backup HSM as HSM SO (using the **token backup login** command) before the token backup update firmware command is run. The command requires no package name.

Before you can use this command, you must acquire the firmware update file from Thales and send the file to the Luna Network HSM 7 (using **pscp** or **sftp**)

> **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.

User Privileges

Users with the following privileges can perform this command:

- Admin
- Operator

Syntax

token backup update firmware -serial <serialnum> [**-force**]

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

Example

```
lunash:>token backup update firmware -serial 496771

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.
```

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

token backup update show

Display information about any capability updates that are available for Luna Backup HSMs. This refers to update files that have been uploaded to the Luna Network HSM 7 appliance and are available to be applied to an attached Backup HSM.

> **NOTE** This command is deprecated as capability upgrades are included in firmware updates. See "token backup update firmware" on page 787.

User Privileges

Users with the following privileges can perform this command:

- Admin
- Operator
- Monitor

Syntax

token backup update show

Example

```
lunash:> token backup update show

Capability Updates:
   HsmStorage15.5Meg
   Partitions20

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).

For Luna Network HSM 7 Appliance Software 7.7.1 and newer, the LunaSH "user" command blocks using the following names as LunaSH users:

> Standard Linux users

> Standard Linux groups

> All the Linux and Luna services, whether active or not.

Attempts to add, change, or delete any such names result in messages returned like (examples):

> 'sshd' is reserved for system use and cannot be added.

> 'sshd' is reserved for system use and cannot be deleted.

> 'sshd' is reserved for system use and cannot be modified.

Syntax

user

add
delete
disable
enable
list
password
radiusadd
role

Argument(s)	Shortcut	Description
add	**a**	Add LunaSH user. See "user add" on page 792.
delete	**de**	Delete a named LunaSH user. See "user delete" on page 794.
disable	**di**	Disable a LunaSH user (but the user still exists with role(s) assigned. See "user disable" on page 795.

Argument(s)	Shortcut	Description
enable	**e**	Enable a locked LunaSH user (with whatever roles are assigned to that user). See "user enable" on page 796.
list	**l**	List the LunaSH user accounts. See "user list" on page 797.
password	**p**	Set User Password. See "user password" on page 798.
radiusadd	**ra**	Add a RADIUS-authenticated user. See "user radiusAdd" on page 800.
role	**ro**	Access the user role commands. See "user role" on page 801.

user add

Add a LunaSH user. Adds a new administrative LunaSH (command line) user. This command is available only to the **admin** account.

LunaSH user names can be 1-32 characters in length, chosen from letters a-z, or A-Z, numbers 0-9, the dash, the dot, or the underscore:

```
abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789-._
```

No spaces are allowed. User names cannot begin with a dot, dash, or number. As with any secure system, no two users (regardless of role) can have the same name.

This command prompts for a password, and summarizes the rules for new passwords. The newly-created administrative user cannot do anything in LunaSH until the **admin** user assigns it a role with the **user role add** command.

> **NOTE** Previously, the **user add** command would create the new named user with default password PASSWORD.
>
> For Luna Network HSM 7 Appliance Software 7.7.0 and newer, you are prompted to assign a real password, following standard password rules. The new user must be told that temporary new password. The user is prompted to change password when logging in for the first time.

User Privileges

Users with the following privileges can perform this command:

> Admin

Syntax

user add -username <username>

Argument(s)	Shortcut	Description
-username <username>	**-u**	Specifies the user name of the user to create.

Example

```
lunash:>user list

               Users       Roles      Status      RADIUS
--------------------    --------    --------    --------
               admin       admin     enabled          no
               audit       audit    disabled          no
             monitor     monitor    disabled          no
            operator    operator    disabled          no

Command Result : 0 (Success)
lunash:>


lunash:>user add -username james
```

```
Changing password for user james.

You can now choose the new password.

The password must be at least 8 characters long.
The password must contain characters from at least 3 of the following 4 categories:
    - Uppercase letters (A through Z)
    - Lowercase letters (a through z)
    - Numbers (0 through 9)
    - Non-alphanumeric characters (such as !, $, #, %)

New password:
Retype new password:
passwd: all authentication tokens updated successfully.

Stopping sshd:                                             [  OK  ]

Starting sshd:                                             [  OK  ]

Command Result : 0 (Success)

lunash:>user list

               Users       Roles      Status      RADIUS
--------------------    --------    --------    --------
               admin       admin     enabled          no
               audit       audit    disabled          no
               james        none     enabled          no
             monitor     monitor    disabled          no
            operator    operator    disabled          no

Command Result : 0 (Success)

lunash:>
```

At this time, you must assign a role to the new user with the **user role** command, and then convey to that person their login username and the temporary password that you have just created for them.

user delete

Delete a role from a user. This command removes a LunaSH 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.

User Privileges

Users with the following privileges can perform this command:

> Admin

Syntax

user delete -username <username>

Argument(s)	Shortcut	Description
-username <username>	**-u**	Specifies the user name of the user being removed.

Example

```
lunash:>user delete -username anna


Command Result : 0 (Success)
```

user disable

Disable a named LunaSH user.

User Privileges

Users with the following privileges can perform this command:

> Admin

Syntax

user disable -username <username>

Argument(s)	Shortcut	Description
-username <username>	**-u**	Specifies the user name of the user to disable.

Example

```
lunash:>user disable -username james

James was disabled successfully.


Command Result : 0 (Success)
```

user enable

Enable a locked LunaSH user.

User Privileges

Users with the following privileges can perform this command:

> Admin

Syntax

user enable -username <username>

Argument(s)	Shortcut	Description
-username	**-u**	Specifies the user name of the user being enabled.

Example

```
lunash:>user enable -username monitor

monitor was enabled successfully.


Command Result : 0 (Success)
```

user list

List all of the LunaSH user accounts.

User Privileges

Users with the following privileges can perform this command:

- Admin
- Operator
- Monitor

Syntax

user list

Example

```
lunash:>user list

                  Users       Roles      Status      RADIUS
   --------------------    --------    --------    --------
                  cindy        none     enabled          no
                  james        none    disabled          no
                  admin       admin     enabled          no
                  audit       audit     enabled          no
                monitor     monitor     enabled          no
               operator    operator    disabled          no

Command Result : 0 (Success)
```

user password

Set or change the appliance password for the specified user. This command allows admin-level users to change their own password or the password for another admin-level, operator-level, or monitor-level user. Operator-level or monitor-level users, as well as the audit user, can use the **my password set** command to change their own password.

Using Luna Appliance Software 7.9.0 or newer, LunaSH passwords must be at least eight characters in length, and include characters from each of the following four categories. Previous versions require characters from three categories:

> lowercase alphabetic: `abcdefghijklmnopqrstuvwxyz`

> uppercase alphabetic: `ABCDEFGHIJKLMNOPQRSTUVWXYZ`

> numeric: `0123456789`

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

Using Luna Network HSM 7 Appliance Software 7.4.0 and older, **user password** <username> changes the password for <username> and expires the password such that the named user must change password after first login.

Using Luna Network HSM 7 Appliance Software 7.7.0 and newer, **user password** (with no argument) changes password for the currently logged-in user and does not expire it.

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

> Regular credential rotation as part of your organization's security policy

> Compromise of a role or secret due to loss or theft of a PED key

> Personnel changes in your organization or changes to individual security clearances

> Changes to your security scheme (implementing/revoking M of N, PINs, or shared secrets)

User Privileges

Users with the following privileges can perform this command:

> Admin for any user

> other users for themselves if logged in

Syntax

user password [<username>]

Argument(s)	Description
<username>	Specifies the user name of the user whose password you want to change. You can change the password for **operator**-level, **monitor**-level, or other **admin**-level users. Omit this parameter to change your own password. *

(*Prior to Luna Network HSM 7 Appliance Software 7.4.0, the username parameter was mandatory for every use of this command. For Luna Network HSM 7 Appliance Software 7.4.0 and newer, omitting the username changes the password for the current logged-in user.)

Example

```
lunash:>user password james

Changing password for user james.

You can now choose the new password.

The password must be at least 8 characters long.
The password must contain characters from at least 3 of the following 4 categories:
    - Uppercase letters (A through Z)
    - Lowercase letters (a through z)
    - Numbers (0 through 9)
    - Non-alphanumeric characters (such as !, $, #, %)

New password:
Retype 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.

LunaSH user names can be 1-32 characters in length, chosen from letters a-z, or A-Z, numbers 0-9, the dash, the dot, or the underscore:

```
abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789-._
```

No spaces are allowed. User names cannot begin with a dot, dash, or number. As with any secure system, no two users (regardless of role) can have the same name.

After the new, named administrative user is created, it can authenticate via RADIUS only. The newly-created administrative user cannot do anything in LunaSH until the **admin** assigns it a role with the **user role add** command.

User Privileges

Users with the following privileges can perform this command:

> Admin

Syntax

user radiusAdd -username <username>

Argument(s)	Shortcut	Description
-username <username>	**-u**	Specifies the user name of the user to add.

Example

```
lunash:>user radiusAdd -username jon

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
import
list

Argument(s)	Shortcut	Description
add	**a**	Add a role to a LunaSH user. See "user role add" on the next page.
clear	**c**	Clears user role assignments. See "user role clear" on page 804.
delete	**d**	Delete a role from a LunaSH user. See "user role delete" on page 805.
import	**i**	Import a role description or definition from a file. See "user role import" on page 806
list	**l**	List the possible role assignments. See "user role list" on page 808.

user role add

Assign an operational role to a user account. A role is a profile defining a level of access and authority with respect to the appliance.

The purpose of this command in combination with the **user add** command is to apply one of the possible roles to a new named user, which defines the scope of access and authority of that named user. This **user role add** command adds a role to a named LunaSH administrative or auditor user that you have already created with the **user add** command. This command is available only to the original **admin** account, and cannot be used to modify the predefined **admin**, **operator**, **monitor** or **audit** accounts (whose names are permanently the same as their roles).

See Appliance Users and Roles for more information.

Users

A user is an identity on the Luna Network HSM 7 appliance. A user has a name. The name of a user can be one of the following:

> a predefined user name (the general administrative users **admin**, **operator** or **monitor**, and the special **audit** user whose only function is managing the auditing of the HSM.

> any name that you wish to use for operational convenience, as created using the command "user add" on page 792.

Predefined Roles

The available predefined roles are **admin**, **operator**, **monitor** or **audit**. These predefined role names are the same as the names of the built-in, permanent user names. A predefined user always has the same role as its name.

In addition to the predefined users, you can create a user account and assign one of the predefined roles to it, which confers upon that user a specific access and authority on the appliance.

Custom Roles

In addition to the predefined roles, you can use the command "user role import" on page 806 to create a custom role. A custom role is able to perform a set of commands that you provide in a file and upload to the appliance. For example, you could create a role called **snmp** that is able to access only the SNMP commands. See Appliance Users and Roles.

Example

For example, we can create a new user called "indigo" and give indigo the authority of "operator". Therefore, if you can log in as the built-in user named "operator", you can perform read-and-write operations with some limits, and if you can log in as user "indigo", you have exactly the same scope of operation and abilities/constraints as would someone logged in as user "operator". Of course, this assumes that the role is also enabled with **user enable** command.

Adding a role to a user displaces or overwrites any previous role held by that user. To see the role currently held by a user, run the **user role list -username** <username> command.

User Privileges

Users with the following privileges can perform this command:

> Admin

Syntax

user role add -username <username> **-role** <rolename>

Argument(s)	Shortcut	Description
-username <username>	**-u**	Specifies the name of the existing named user account to which the role is being added.
-role <rolename>	**-r**	The name of the administrative role being added to that user. The available default roles, in descending order of capability are **admin**, **operator**, and **monitor**, for general administration, and **audit** for managing HSM auditing functions. **Valid values:** admin, operator, monitor, audit, or a custom role

Example

```
lunash:>user role add -username james -role audit


User james 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.

User Privileges

Users with the following privileges can perform this command:

> Admin

Syntax

user role clear -username <username>

Argument(s)	Short	Description
-username <username>	**-u**	Specifies the name of the user account from which the role is being removed.
-force	**-f**	Force the action. Useful for scripting.

Example

```
lunash:>user role clear -username james


WARNING !!  This command will delete all james's role assignments.
If you are sure that you wish to proceed, then enter 'proceed', otherwise this command will
abort.

> proceed
Proceeding...
Role list cleared for user James


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**, **operator**, or **audit** accounts.

User Privileges

Users with the following privileges can perform this command:

> Admin

Syntax

user role delete -role <rolename> **-username** <username>

Argument(s)	Shortcut	Description
-username <username>	**-u**	Specifies the name of the user account from which the role is being removed.
-role <rolename>	**-r**	The role name of the role being removed from the user. The available roles, in descending order of capability are admin, operator and monitor, and the special role audit. **Valid values:** admin,operator,monitor,audit

Example

```
lunash:>user role delete -username cindy -role admin


User cindy was successfully modified.


Command Result : 0 (Success)
```

user role import

Import a role description or definition from a file that defines the list of commands a custom role is able to perform. See Appliance Users and Roles for more information.

> **NOTE** The commands that can be recruited for this operation include all those available to the appliance **admin** user, or roles subordinate to **admin**.(*)
>
> The appliance *audit* user is not a subordinate role under admin, and those commands cannot be included in a custom role definition file.
>
> (* Availability of commands also depends on whether or not a command exists in the particular appliance or the cryptographic module within the appliance. Thus an older software or firmware version might not include commands that were introduced in later versions. Similarly, some commands might be present only if specific optional secure packages are installed. In either case the attempt to import a role definition file with unavailable commands would be rejected. Rejection can also occur if commands in a role definition file are misspelled or do not have exact lettercase. The rejection message will name any rejected commands to help you troubleshoot.)

A role definition file is a UNIX-format file containing a list of LunaSH commands that are allowed for the role, for example:

```
exit
help
scp
hsm init
hsm login
hsm logout
hsm show
my file list
partition create
```

All lines must end with a UNIX-style linefeed (lf) character. If you create your file in Windows, be sure to convert to the UNIX style before transferring it to a Luna Network HSM 7 appliance.

When the definition is applied to a named role using the command "user role add" on page 802, that role will have access only to commands that are named in the file.

> **NOTE** The system does not pre-detect the purpose of the file, so it is up to you to name your role definition files usefully, and to recognize them when you import them.

LunaSH role names can be 1-255 characters in length. The following characters are allowed:

```
abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789_
```

No spaces are allowed. Creating a role name that begins with a number is not recommended. As with any secure system, no two roles can have the same name.

Syntax

user role import -file <filename> **-role** <rolename>

Argument(s)	Shortcut	Description
-file <filename>	**-f**	Name of the file being imported.
-role <rolename>	**-r**	The name of the administrative role for which a description file is being imported.

Example

```
lunash:>user role import -file rolefile1 -role indigo

"rolefile1" was successfully imported.

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.

User Privileges

Users with the following privileges can perform this command:

- Admin
- Operator
- Monitor

Syntax

user role list [**-username** <username>]

Argument(s)	Shortcut	Description
-username <username>	**-u**	See the roles assigned to the named user.
.	**.**	If no user is named, all users and their roles are listed.

Example

```
lunash:>user role list

Available  Roles:
--------------------------------------------------

admin
audit
monitor
operator


Command Result : 0 (Success)
```

webserver

The **webserver** command set configures REST API functions on the Luna Network HSM 7 appliance.

Syntax

webserver

bind
certificate
ciphers
disable
enable
show

Argument(s)	Shortcut	Description
bind	**b**	Set REST API service network port. See "webserver bind" on the next page.
certificate	**ce**	Manage REST API service certificate. See "webserver certificate" on page 812.
ciphers	**ci**	Manage REST API service cipher suite. See "webserver ciphers" on page 817.
disable	**d**	Disable REST API service. See "webserver disable" on page 823.
enable	**e**	Enable REST API service. See "webserver enable" on page 824.
origin	**o**	Manage REST API's allowed origin domains. See "webserver origin" on page 825.
show	**s**	Show REST API service configuration and status. See "webserver show" on page 829.

webserver bind

Bind the REST API service to a network interface and port.

User Privileges

Users with the following privileges can perform this command:

> Admin

Syntax

webserver bind -netdevice <netdevice> [**-port** <port>] [**-force**] [**-restart**]

Argument(s)	Shortcut	Description
-netdevice <netdevice>	**-n**	Network device that REST API Service is to use for communication. **Valid values**: eth0, eth1, eth2, eth3, all, bond0, bond1
-force	**-f**	Force the action without prompting.
-port <port>	**-p**	Network port that REST API service is to use for communication. **Range**: 1024 to 65535 **NOTE** Using Luna Appliance Software 7.8.5 or older, LunaSH allows you to set a port in the range **80-65535**, but setting a port number lower than **1024** prevents sessions from opening. Refer to known issue RAPI-4018. **Default**: 8443
-restart	**-r**	Restart the REST API service if parameter is specified. Otherwise, the administrator must restart the REST API service by running **service start webserver**.

Examples

Attempting to bind the REST API service when the service is not enabled

```
webserver bind -netdevice eth0

Error: The REST API Service is not enabled.
The REST API Service must be enabled in order to execute this command.

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

Binding the REST API service without specifying the -restart option

```
webserver bind -netdevice eth0 -port 8443

WARNING: This operation will modify REST API Server binding information !!!
Type 'proceed' to continue, or 'quit' to quit now.

> proceed
Proceeding...

You chose not to restart REST API Service now.
The changes will be effective when REST API Service is restarted.
To restart it run: service restart webserver

Command Result : 0 (Success)
```

Binding the REST API service with the -restart option

```
lunash:>webserver bind -netdevice eth0 -restart

WARNING: This operation will modify REST API Server binding information !!!

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

> proceed
Proceeding...

Restarting REST API service...

Command Result : 0 (Success)
```

webserver certificate

Manage REST API service certificates.

Syntax

webserver certificate

generate
show

Argument(s)	Shortcut	Description
generate	**g**	Create REST API service certificate. See "webserver certificate generate" on the next page.
show	**s**	Show REST API service configuration and status. See "webserver certificate show" on page 815.

webserver certificate generate

Generates a REST API Server certificate.

User Privileges

Users with the following privileges can perform this command:

> Admin

Syntax

webserver certificate generate -keytype <key_type> [**-keysize** <size>] [**-curve** <curve_name>] [**-restart**] [**-force**]

Argument(s)	Shortcut	Description
-keytype <key_type>	**-keyt**	Key type. **Valid values:** ecc,rsa
-keysize <size>	**-keys**	RSA key size (default: 2048). **Valid values:** 2048,3072,4096
-curve <curve_name>	**-c**	Elliptic Curve name (ECC only, default: secp384r1). **Valid values:** secp256k1,secp384r1,secp521r1,prime256v1
-force	**-f**	Force the action without prompting.
-restart	**-r**	Restart the REST API service if parameter is specified. Otherwise, the administrator must restart the REST API service via other means (i.e., **service start webserver**).

Example

```
lunash:>webserver certificate generate -keytype rsa -restart

WARNING: This operation will generate/regenerate the REST API Server certificate !!!

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

> proceed
Proceeding...

Restarting REST API service...
Redirecting to /bin/systemctl restart  webserver.service

REST API Server Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            d6:93:f0:66:1c:04:9f:34
    Signature Algorithm: sha384WithRSAEncryption
```

```
        Issuer: C=CA, ST=Ontario, L=Ottawa, O=Thales, CN=local_host
        Validity
            Not Before: Mar  1 20:22:56 2017 GMT
            Not After : Feb 27 20:22:56 2027 GMT
        Subject: C=CA, ST=Ontario, L=Ottawa, O=Thales, CN=local_host
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (2048 bit)
                Modulus:
                    00:cf:f2:56:9b:22:24:f2:4e:bb:ab:8b:d3:38:42:
                    24:65:0d:98:13:de:62:92:8f:5b:a5:6b:a5:ea:15:
                    aa:08:f7:ae:c4:62:58:cf:54:3c:0b:16:fe:ba:71:
                    93:ac:a9:71:14:f0:a7:41:94:0f:34:80:cc:fd:6d:
                    d2:ae:2b:8d:a5:ef:f2:25:43:d6:5e:08:59:b7:1b:
                    a1:7a:dc:96:08:c1:ee:c0:35:41:1e:90:7f:16:d1:
                    32:d0:c6:4c:6b:df:3c:b3:48:2d:14:5f:fa:cc:b4:
                    cf:11:27:3a:74:14:80:17:eb:87:c8:f6:41:35:91:
                    c6:c5:60:67:87:d7:58:ba:b0:7b:97:b8:a9:08:de:
                    67:c9:2d:cf:ac:08:3e:a1:c1:31:23:b3:cd:96:7b:
                    af:45:4e:fd:e6:80:61:28:52:4e:27:27:9c:d6:01:
                    19:ef:74:6e:15:7d:51:d4:62:be:38:a8:8f:04:7e:
                    82:18:7c:75:a5:6a:4c:10:3e:d8:ec:86:03:52:fe:
                    f7:15:0a:45:55:f4:ae:be:c7:88:e5:6b:09:be:18:
                    27:96:54:c2:ad:30:8e:43:d9:0e:f4:4a:00:06:28:
                    fb:08:cd:df:af:31:e3:1d:58:95:f8:51:90:ee:5a:
                    48:3a:21:83:f1:53:59:a8:8f:7c:cf:e8:0f:b2:09:
                    1c:49
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            X509v3 Subject Key Identifier:
                C1:20:E0:21:B8:19:7F:11:0B:57:7C:3E:0D:CA:70:63:6D:97:E4:CD
            X509v3 Authority Key Identifier:
                keyid:C1:20:E0:21:B8:19:7F:11:0B:57:7C:3E:0D:CA:70:63:6D:97:E4:CD

            X509v3 Basic Constraints:
                CA:TRUE
    Signature Algorithm: sha384WithRSAEncryption
        6c:b6:04:92:f9:52:6f:ae:1f:ef:b8:fa:f9:40:16:97:28:10:
        f2:13:64:af:cb:67:63:4b:81:42:cb:00:cb:5a:9b:39:2d:88:
        30:c1:75:bc:90:69:33:67:51:1c:05:c0:b1:e2:88:47:8e:ad:
        48:28:eb:d0:24:e0:48:46:b0:5a:97:e8:c8:0d:39:b9:13:e3:
        78:5a:c2:f6:66:cf:25:97:8e:0b:47:70:41:7e:e1:46:f5:4a:
        25:9a:b0:3f:43:2b:4c:ed:64:b0:2d:24:13:17:2f:bd:09:11:
        c0:15:f2:da:aa:7e:9d:27:2e:b5:cd:7d:0d:b5:80:23:14:3a:
        8c:fc:e2:76:92:d1:87:1b:9e:a5:c6:ef:b2:a0:af:f3:15:cc:
        41:84:5c:d1:fc:d3:3f:9a:c1:65:b0:bf:3c:be:e9:07:f4:25:
        45:ff:f0:65:a7:a6:38:d8:f8:13:55:a6:ee:b1:9f:4a:31:c1:
        d5:e2:b7:a2:f1:8d:07:72:cc:39:d1:4f:34:a7:df:1d:bc:4e:
        d0:94:c4:f2:f9:a0:53:c4:fb:fe:03:4a:01:13:8b:bd:c0:ef:
        ed:1b:90:c8:ec:e9:26:ee:90:9f:94:f2:9c:62:8e:09:55:27:
        26:fb:00:02:3b:6b:5b:53:8a:b4:9c:25:7c:33:78:ec:40:30:
        02:09:cf:20

Command Result : 0 (Success)
```

webserver certificate show

Shows the REST API Server certificate.

User Privileges

Users with the following privileges can perform this command:

> Admin

Syntax

webserver certificate show

Example

```
lunash:>webserver certificate show

REST API Server Certificate:
    Data:
        Version: 1 (0x0)
        Serial Number:
            0a:ca:e6:fe:4f:8c:f8:d7:a0:fb:c0:ff:d4:7d:c1:19:93:b5:b1:9e
    Signature Algorithm: sha256WithRSAEncryption
        Issuer: C=CA, ST=Ontario, L=Ottawa, O=Gemalto, CN=webserver
        Validity
            Not Before: Dec 13 13:44:10 2023 GMT
            Not After : Dec 10 13:44:10 2033 GMT
        Subject: C=CA, ST=Ontario, L=Ottawa, O=Gemalto, CN=webserver
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (2048 bit)
                Modulus:
                    00:aa:5b:d6:0a:cc:86:2e:30:dd:36:e7:f9:4e:a0:
                    01:d2:78:b5:32:e3:9c:e4:2c:10:21:be:34:33:b0:
                    1a:19:2b:c2:98:17:9e:0c:ad:2f:9b:98:e3:54:e4:
                    59:2a:61:bd:12:b4:a1:9a:64:34:60:2b:14:13:08:
                    f0:e1:a2:ac:22:87:93:f3:d9:12:ae:3c:cb:b3:5c:
                    86:41:e5:0d:bf:68:7f:27:e7:0d:3a:f6:f1:1e:1b:
                    21:64:49:65:a4:f8:00:59:43:4d:0a:4c:4f:b9:08:
                    0a:a8:41:bb:ad:ff:da:f8:a4:3f:67:6b:90:df:f9:
                    52:35:04:8a:7d:ef:43:81:e6:f7:59:f2:79:22:c3:
                    7a:f6:04:c3:c6:ca:6e:48:da:43:1b:bc:bd:fd:12:
                    ed:cd:ad:1e:4e:7c:7b:5e:c7:87:ad:6e:13:42:7f:
                    3d:32:c6:5c:c4:9e:92:bc:9a:6f:32:2a:6c:4e:06:
                    ef:ce:bd:b5:bb:0b:e8:7f:f8:ff:90:72:50:d1:4e:
                    a4:95:d8:86:29:94:c3:c4:59:49:66:6e:43:77:7e:
                    1e:c8:c9:98:21:36:8d:44:ab:f4:de:91:fb:67:48:
                    6d:65:fb:6e:50:66:e8:75:f1:5c:d0:9e:cb:ed:74:
                    a8:b9:3a:6e:46:ee:92:f1:d1:db:d4:4a:04:f9:34:
                    36:7f
                Exponent: 65537 (0x10001)
    Signature Algorithm: sha256WithRSAEncryption
         79:fb:4e:1f:36:a5:6e:7d:a0:44:8d:b5:b1:9a:ea:f3:b1:8a:
         76:76:ce:92:10:53:2d:b4:92:70:8a:09:ab:34:a5:33:4e:88:
         ca:38:a1:4e:a4:6a:dd:57:6e:99:8a:fa:66:78:d7:26:9f:9d:
```

```
        8f:df:b4:8f:a2:61:6c:eb:f4:db:4a:3a:cb:92:82:47:75:e0:
        b1:f8:c5:d5:dd:9d:6d:f3:f3:18:77:72:48:c7:7b:96:a9:4e:
        aa:18:5d:7c:b4:ef:f3:b0:34:99:22:4a:43:4f:40:7b:a2:63:
        dd:e4:56:8d:60:22:1d:df:cd:da:ab:1d:c1:5e:88:3e:6f:39:
        e2:93:f3:49:32:2c:9d:4d:eb:b4:32:f5:33:62:33:c1:0c:76:
        3b:0f:57:e2:b0:68:12:c8:df:68:68:8f:8d:8a:b3:85:2e:64:
        7c:fa:b1:1e:85:98:47:79:3d:81:e3:cd:14:f4:a5:c9:35:91:
        bd:74:84:c3:84:3e:8e:ac:d1:bb:6a:59:90:32:9b:26:53:11:
        51:fb:f5:9a:01:2a:48:8c:02:14:86:c1:0b:6f:3e:2b:ae:e4:
        e2:5e:67:30:f9:ad:bc:4c:88:03:d8:50:a8:69:ac:bd:f8:ce:
        17:e0:3b:2e:1e:75:d6:cc:10:52:22:1f:5c:33:1f:66:c8:2d:
        ed:06:6b:07


Command Result : 0 (Success)
```

webserver ciphers

Set or show the REST API Server ciphers suite.

Syntax

webserver ciphers

set
show

Argument(s)	Shortcut	Description
reset	**r**	Resets REST API server ciphers suite to its default settings. See "webserver ciphers reset" on the next page.
set	**se**	Set REST API Server ciphers suite. See "webserver ciphers set" on page 819.
show	**sh**	Show REST API Server supported ciphers. See "webserver ciphers show" on page 821.

webserver ciphers reset

Resets REST API server ciphers suite to its default settings.

> **NOTE** This command requires Luna Appliance Software 7.8.4 or newer.

User Privileges

Users with the following privileges can perform this command:

> Admin

Syntax

webserver ciphers reset [**-force**]

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

Examples

```
lunash:>webserver ciphers reset

This operation will reset the webserver cipher(s) to use the following default cipher(s):
TLS_AES_256_GCM_SHA384
TLS_CHACHA20_POLY1305_SHA256
TLS_AES_128_GCM_SHA256
ECDHE-ECDSA-AES256-GCM-SHA384
ECDHE-RSA-AES256-GCM-SHA384
DHE-RSA-AES256-GCM-SHA384
ECDHE-ECDSA-AES128-GCM-SHA256
ECDHE-RSA-AES128-GCM-SHA256
DHE-RSA-AES128-GCM-SHA256
ECDHE-ECDSA-AES256-SHA384
ECDHE-RSA-AES256-SHA384
DHE-RSA-AES256-SHA256
ECDHE-ECDSA-AES128-SHA256
ECDHE-RSA-AES128-SHA256
DHE-RSA-AES128-SHA256
AES256-GCM-SHA384
AES128-GCM-SHA256
AES256-SHA256
AES128-SHA256

This operation will restart the webserver service.
Type 'proceed' to reset webserver cipher(s) to default settings and restart the webserver
service, or 'quit'
    to quit now. > proceed


Command Result : 0 (Success)
```

webserver ciphers set

Sets REST API server ciphers suite.

User Privileges

Users with the following privileges can perform this command:

> Admin

Syntax

webserver ciphers set -list <cipher_list> [**-tls1_2**] [**-tls1_3**] [**-restart**] [**-force**]

Argument(s)	Shortcut	Description
-list <cipher_list>	**-l**	Colon-separated list of ciphers. To allow all ciphers, set **-list all**.
-force	**-f**	Force the action without prompting.
-restart	**-r**	Restart the **webserver** service automatically. Otherwise, the administrator must restart the REST API service by running **service restart webserver**. This option is deprecated and has been removed in Luna Appliance Software 7.8.4 and newer. In newer versions, the service is always restarted automatically.
-tls1_2	**-tls1_2**	Specify this option with **-list all** to set all TLS 1.2 ciphers. Requires Luna Appliance Software 7.8.4 or newer.
-tls1_3	**-tls1_3**	Specify this option with **-list all** to set all TLS 1.3 ciphers. Requires Luna Appliance Software 7.8.4 or newer.

Examples

```
lunash:>webserver ciphers set -list TLS_AES_256_GCM_SHA384:TLS_AES_128_GCM_SHA256


This operation will set the webserver cipher(s) to use the following cipher(s):

Configured Ciphers
--------------------------------------------------
TLS_AES_256_GCM_SHA384
TLS_AES_128_GCM_SHA256

This operation will restart the webserver service.
Type 'proceed' to set webserver cipher(s) and restart the webserver service, or 'quit'
    to quit now. > proceed

Command Result : 0 (Success)
```

```
lunash:>webserver ciphers set -list all -tls1_3

This operation will set the TLS1.3 cipher(s) for webserver.
TLS_AES_256_GCM_SHA384
TLS_CHACHA20_POLY1305_SHA256
TLS_AES_128_GCM_SHA256

This operation will restart the webserver service.

Type 'proceed' to set webserver cipher(s) and restart the webserver service, or 'quit'
    to quit now. > proceed

Command Result : 0 (Success)


lunash:>webserver ciphers set -list all -tls1_2 -force

This operation will set the TLS1.2 cipher(s) for webserver.
ECDHE-ECDSA-AES256-GCM-SHA384
ECDHE-RSA-AES256-GCM-SHA384
DHE-RSA-AES256-GCM-SHA384
ECDHE-ECDSA-AES128-GCM-SHA256
ECDHE-RSA-AES128-GCM-SHA256
DHE-RSA-AES128-GCM-SHA256
ECDHE-ECDSA-AES256-SHA384
ECDHE-RSA-AES256-SHA384
DHE-RSA-AES256-SHA256
ECDHE-ECDSA-AES128-SHA256
ECDHE-RSA-AES128-SHA256
DHE-RSA-AES128-SHA256
AES256-GCM-SHA384
AES128-GCM-SHA256
AES256-SHA256
AES128-SHA256

This operation will restart the webserver service.
Force option used. Proceed prompt bypassed.

Command Result : 0 (Success)
```

webserver ciphers show

Show the REST API Server supported ciphers.

User Privileges

Users with the following privileges can perform this command:

> Admin

Syntax

webserver ciphers show

Example

```
lunash:>webserver ciphers show

The following cipher(s) are available to configure webserver:

Available Ciphers
--------------------------------------------------
TLS_AES_256_GCM_SHA384         TLSv1.3  Kx=any   Au=any    Enc=AESGCM(256)             Mac=AEAD
TLS_CHACHA20_POLY1305_SHA256   TLSv1.3  Kx=any   Au=any    Enc=CHACHA20/POLY1305(256)  Mac=AEAD
TLS_AES_128_GCM_SHA256         TLSv1.3  Kx=any   Au=any    Enc=AESGCM(128)             Mac=AEAD
ECDHE-ECDSA-AES256-GCM-SHA384  TLSv1.2  Kx=ECDH  Au=ECDSA  Enc=AESGCM(256)             Mac=AEAD
ECDHE-RSA-AES256-GCM-SHA384    TLSv1.2  Kx=ECDH  Au=RSA    Enc=AESGCM(256)             Mac=AEAD
DHE-RSA-AES256-GCM-SHA384      TLSv1.2  Kx=DH    Au=RSA    Enc=AESGCM(256)             Mac=AEAD
ECDHE-ECDSA-AES128-GCM-SHA256  TLSv1.2  Kx=ECDH  Au=ECDSA  Enc=AESGCM(128)             Mac=AEAD
ECDHE-RSA-AES128-GCM-SHA256    TLSv1.2  Kx=ECDH  Au=RSA    Enc=AESGCM(128)             Mac=AEAD
DHE-RSA-AES128-GCM-SHA256      TLSv1.2  Kx=DH    Au=RSA    Enc=AESGCM(128)             Mac=AEAD
ECDHE-ECDSA-AES256-SHA384      TLSv1.2  Kx=ECDH  Au=ECDSA  Enc=AES(256)
Mac=SHA384
ECDHE-RSA-AES256-SHA384        TLSv1.2  Kx=ECDH  Au=RSA    Enc=AES(256)
Mac=SHA384
DHE-RSA-AES256-SHA256          TLSv1.2  Kx=DH    Au=RSA    Enc=AES(256)
Mac=SHA256
ECDHE-ECDSA-AES128-SHA256      TLSv1.2  Kx=ECDH  Au=ECDSA  Enc=AES(128)
Mac=SHA256
ECDHE-RSA-AES128-SHA256        TLSv1.2  Kx=ECDH  Au=RSA    Enc=AES(128)
Mac=SHA256
DHE-RSA-AES128-SHA256          TLSv1.2  Kx=DH    Au=RSA    Enc=AES(128)
Mac=SHA256
AES256-GCM-SHA384              TLSv1.2  Kx=RSA   Au=RSA    Enc=AESGCM(256)             Mac=AEAD
AES128-GCM-SHA256              TLSv1.2  Kx=RSA   Au=RSA    Enc=AESGCM(128)             Mac=AEAD
AES256-SHA256                  TLSv1.2  Kx=RSA   Au=RSA    Enc=AES(256)
Mac=SHA256
AES128-SHA256                  TLSv1.2  Kx=RSA   Au=RSA    Enc=AES(128)
Mac=SHA256


The selected Webserver cipher(s) are used by the webserver service
REST API Server is using the following cipher(s):

Configured Ciphers
--------------------------------------------------
```

```
TLS_AES_256_GCM_SHA384
TLS_CHACHA20_POLY1305_SHA256
TLS_AES_128_GCM_SHA256
ECDHE-ECDSA-AES256-GCM-SHA384
ECDHE-RSA-AES256-GCM-SHA384
DHE-RSA-AES256-GCM-SHA384
ECDHE-ECDSA-AES128-GCM-SHA256
ECDHE-RSA-AES128-GCM-SHA256
DHE-RSA-AES128-GCM-SHA256
ECDHE-ECDSA-AES256-SHA384
ECDHE-RSA-AES256-SHA384
DHE-RSA-AES256-SHA256
ECDHE-ECDSA-AES128-SHA256
ECDHE-RSA-AES128-SHA256
DHE-RSA-AES128-SHA256
AES256-GCM-SHA384
AES128-GCM-SHA256
AES256-SHA256
AES128-SHA256

Command Result : 0 (Success)
```

webserver disable

Disable the REST API service.

User Privileges

Users with the following privileges can perform this command:

> Admin

Syntax

webserver disable [**-force**]

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

Example

```
lunash:>webserver disable

WARNING: This operation will stop and disable REST API Service !!!

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

> proceed
Proceeding...

Command Result : 0 (Success)
```

webserver enable

Enable the REST API service. After enabling the service, use **service start webserver** to start the service.

User Privileges

Users with the following privileges can perform this command:

> Admin

NOTE You must call **webserver bind** to access the REST API.

Syntax

webserver enable [**-force**]

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

Example

```
lunash:> webserver enable

WARNING: This operation will enable REST API Service !!!

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

> proceed
Proceeding...

Command Result : 0 (Success)
```

webserver origin

Manage the allowed origin domains for clients using browsers with AJAX calls to execute REST API commands on the appliance. You must add a client's domain or IP to this list before you can use REST API with the appliance.

> **NOTE** This feature requires minimum Luna Network HSM 7 Appliance Software 7.4.0.

Syntax

webserver origin

clear
set
show

Argument(s)	Shortcut	Description
clear	**c**	Clear the list of approved REST API origin domains. See "webserver origin clear" on the next page.
set	**se**	Set approved REST API origin domains. See "webserver origin set" on page 827.
show	**sh**	Display the approved REST API origin domains. See "webserver origin show" on page 828.

webserver origin clear

Clear the list of approved REST API origin domains.

> **NOTE** This feature requires minimum appliance software version 7.4. See Version Dependencies by Feature for more information.

User Privileges

Users with the following privileges can perform this command:

> Admin

Syntax

webserver origin clear

Example

```
lunash:>webserver origin clear

All domains have been removed.

Command Result : 0 (Success)
```

webserver origin set

Set allowed origin domains for the REST API webserver.

> **NOTE** This feature requires minimum Luna Network HSM 7 Appliance Software 7.4.0.

User Privileges

Users with the following privileges can perform this command:

> Admin

Syntax

webserver origin set

Argument(s)	Shortcut	Description
-force	**-f**	Force the action without prompting.
-list <origin_list>	**-l**	Specify the list of allowed origin domains, separated by commas. You can specify domains, IP addresses, or IP/port combinations.
-restart	**-r**	Restart the webserver service after setting the allowed origin domains. If you do not include this option, you must restart the webserver manually before the origin changes take effect (lunash:>"service restart" on page 467 **webserver**).

Example

```
lunash:>webserver origin set -list "luna.com,thales.com,safenet.com,192.168.0.1:8081"

WARNING: This operation will modify REST API Server allowed origin domains.

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

> proceed
Proceeding...

New REST API Service Allowed Origin Domains:
"luna.com","thales.com","safenet.com","192.168.0.1:8081"
You chose not to restart REST API Service now.
The new allowed origin domains will be effective when REST API Service is restarted.
To restart it run: service restart webserver

Command Result : 0 (Success)
```

webserver origin show

Display a list of currently-allowed origin domains.

> **NOTE** This feature requires minimum Luna Network HSM 7 Appliance Software 7.4.0.

User Privileges

Users with the following privileges can perform this command:

- Admin
- Operator
- Monitor

Syntax

webserver origin show

Example

```
lunash:>webserver origin show

Origin Domains Allowed by REST API Server:
"luna.com","thales.com","safenet.com","192.168.0.1:8081"

Command Result : 0 (Success)
```

webserver show

Display the REST API Server configuration.

User Privileges

Users with the following privileges can perform this command:

> Admin

Syntax

webserver show

Example

```
lunash:>webserver show

   REST API Service:
   ==================
   API Version:           8
   Configuration:         enabled
   Status:                running
   IP address:            0.0.0.0
   Port:                  8443
   Certificate Key Type:  rsa
   Key Size:              2048

Command Result : 0 (Success)
```