THALES

Thales Luna Network HSM 7

APPLIANCE ADMINISTRATION GUIDE

Document Information

Last Updated	2025-06-05 09:28:02 GMT-05:00

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.

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 Appliance Administration Guide

The maintenance and administrative tasks in this document are for the Luna Network HSM 7 appliance, outside of the HSM. HSM administrative tasks are described in the *HSM Administration Guide*. Some activities might encompass both portions of the Luna Network HSM 7 server.

As an HSM Server, Luna Network HSM 7 provides increased operational flexibility over traditional HSMs. The Luna Network HSM 7 appliance includes an integrated FIPS 140-2 level 3 HSM, the Luna K7 Cryptographic Engine.

The HSM appliance that you have purchased has been factory configured to authenticate as either:

- Password authentication version (equivalent to FIPS 140-2 level 3, using password strings for authentication and access control.
- Multifactor Quorum (a.k.a. PED or Trusted Path) authentication version that requires the Luna PED and role-/function-authenticating PED keys for authentication and access control.

The HSM appliance adds a secure service layer (NTLS and STC) that allows the Luna Cryptographic Engine (the HSM inside the appliance) to be shared as a service to network applications. Like traditional servers that provide e-mail, web pages, and file download (FTP) services to authenticated clients, the HSM appliance offers HSM services to clients on the network.

As an Ethernet-attached device, the HSM appliance can be shared among many applications on a network. Rather than requiring many HSMs to fulfill the security demands of many applications, one HSM appliance can be shared among many applications simultaneously.

This document contains the following chapters:

The preface includes the following information about this document:

> "Support Contacts" on page 12

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

Customer Release Notes

The Customer Release Notes (CRN) provide important information about 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.
{**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).

CHAPTER 1: Luna Network HSM 7 Hardware Installation

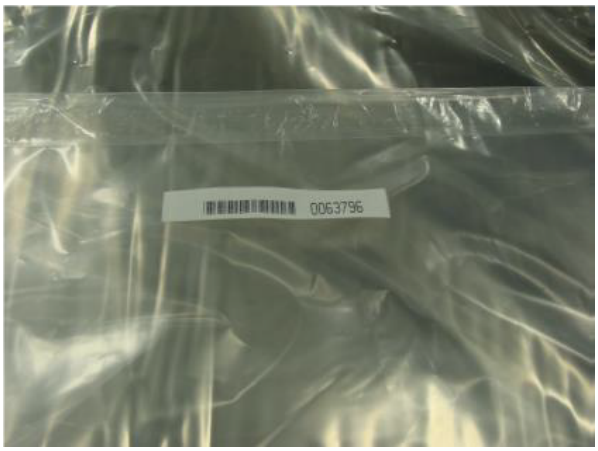
This chapter describes how to install and connect a Luna Network HSM 7. To ensure a successful installation, perform the following tasks in the order indicated:

1. Before unpacking your new hardware, refer to "Verifying the Integrity of Your Shipment" below for safe unpacking instructions.
2. Ensure that you have all of the required components, as listed in "Luna Network HSM 7 Required Items" on page 16.
3. If you plan to mount the hardware in an equipment rack, follow the instructions in "Rack-Mounting the Luna Network HSM 7" on page 22.
4. Install and connect the hardware, as described in "Installing the Luna Network HSM 7 Hardware" on page 29

Verifying the Integrity of Your Shipment

> **CAUTION!** Thales employs a number of security measures to allow you to verify that your new hardware was not intercepted in transit or otherwise tampered with before you received it. To verify the authenticity and handling history of your received items, review the following checklist before you unpack your new hardware, and then follow the checklist as you unpack each item.

Step	Yes	No
1. Do the items received (individual items, part numbers) match those listed in the enclosed packing list? If yes, go to the next step. If no, contact Thales support.		
2. Before you received the product, did you receive an advanced shipping notification providing details regarding the shipment (part numbers and serial numbers for the product, and for tamper-evident bag(s))? If yes, go to the next step. If no, contact Thales support.		

Step	Yes	No
3. Are any tamper-evident bag serial numbers that are listed in the advanced shipping notification present, and do they match the actual bag(s) received? The tamper-evident bag serial numbers appear as shown below.  If yes, go to the next step. If no, contact Thales support. **NOTE** The serial number of the bag is tracked. Serial numbers of additional stickers on the bag are not tracked, and are meant only for inspection against physical alteration.		
4. Did you receive any tamper-evident bags that are *not* listed on the advance shipping notification? If yes, contact Thales support. If no, go to the next step.		

Step	Yes	No
5. Are the correct number of tamper seals affixed to the device? There should be two tamper seals affixed to the device: one affixed to the left side and one affixed to the top-left front of the unit (when unit is facing you).   If no, contact Thales support. If yes, go to the next step. **NOTE** The serial number of the bag is tracked. Serial numbers of additional stickers on the bag are not tracked, and are meant only for inspection against physical alteration.		
6. Are all of the tamper seal serial numbers listed in the advanced shipping notification present, and do they match the actual seals affixed to the device? If yes, go to the next step. If no, contact Thales support.		
7. Are there any tamper seals affixed to the device that are *not* listed on the advance shipping notification? If yes, contact Thales support. If no, go to the next step.		
8. Are there any signs of physical tampering? The tamper seals on the sides indicate tampering if they show the **ALERT** markings as illustrated.  If yes, contact Thales support. If no, go to the next step.		
9. Once you have verified all of the received items, you can proceed with the installation.		

Luna Network HSM 7 Required Items

This section provides a list of the components you should have received with your Luna Network HSM 7 order. The specific items you received depend on whether you ordered a password-authenticated or a multifactor quorum-authenticated Luna Network HSM 7, and whether your order included a backup device or other options as described below.

Basic Luna Network HSM 7 order items

The standard items that you should have received as your basic order for a Luna Network HSM 7 are:

Qty	Item
1	**Luna Network HSM 7 Appliance**  Your order should include one password-authenticated or multifactor quorum-authenticated Luna Network HSM 7. The different HSM models appear physically identical.
1	**Adapter Cable: RJ45 to USB with a standard eight-pin, eight connector (8P8C) modular connector**  Used to open a terminal connection to the HSM during initial configuration.

Qty	Item
1	**Front Ear Bracket Set**  Set includes: > (2) front ear brackets > (4) bracket screws
1	**Friction Rail Mounting Bracket Set**  The standard mounting bracket set is designed for use in standard 483mm (19")-wide racks with depth of 620-902mm (24.5”-35.5”). See "Using the Supplied Mounting Brackets" on page 23 for installation instructions. Set includes: > (2) side rails > (8) side rail screws > (2) sliding rear brackets (fit into the rails for rear support adjustable positioning) **CAUTION!** The included mounting hardware is meant for static positioning of the appliance. The long tab that slides into the bracket, applied to each side of the appliance, is adjustable for fitting the appliance into racks of depth - it must not be used to extend the appliance out of the rack. Optional sliding rails with rolling bearings are available for situations where rolling excursion of the appliance, while attached to the rack, is required for maintenance. See "Optional Items" on page 20.

Qty	Item
1	**Friction Rail Rack Mounting Screws/Cage Nuts**  Set includes: > (8) M5 cage nuts > (8) M5x14 rack screws If you did not receive this set, you can request one from Thales (part number: 216-000035-001) or obtain your own suitable screws/nuts.

Other Required Items

The following required items are not shipped with the standard Luna Network HSM 7 order.

Qty	Item
2	**Power Supply Cord**  You must provide one for each power supply, with connectors appropriate to your region of operation, usually sold separately. Thales no longer includes power cords with HSM appliances. Many customers reship our products to labs and data centers all over the world, and the correct format power cord is readily and economically sourced at the destination.

Multifactor Quorum-Authenticated Luna Network HSM 7 order items

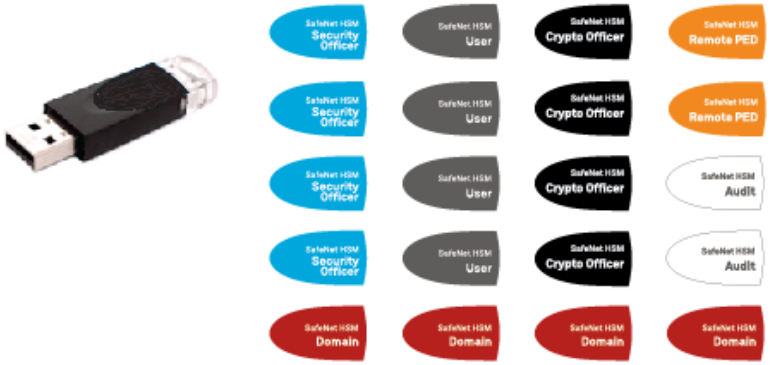
If you ordered a multifactor quorum-authenticated Luna Network HSM 7, you should have received some combination of the following items in addition to the items in the basic order.

Note that you can use PED keys that you already own and use with other HSMs -- PED keys can be used with multiple HSMs if that is appropriate in your context. You should purchase the number of PEDs you need for your own convenient operation, and for backup/standby units as your security policies might require.

Qty	Item
1+	**Standard or Remote-Capable Luna PED**  Your order should include at least one Luna PEDdevice. If you intend to combine remote operation and backup, you might prefer to have a second Luna PED. It is possible to use a single Luna PED for both connections, and to simply change between local and remote mode as needed. Note that you can use PED keys that you already own and use with other HSMs if appropriate. You should purchase the number you need for your own convenient operation, and for backup/standby units as your security policies might require.
1	**Luna PED cable**  The PED device connects to your HSM using a Type A to Mini B USB cable.

Other Required Multifactor Quorum-Authentication Items

The following required items may be shipped with your Luna PED, or ordered separately.

Qty	Item
1	**Set of PED keys and Labels**  Your order may include a set of PED keys and peel-and-stick labels.

Optional Items

You may have also ordered one or more of these optional items:

Qty	Item
1	**Secure Locking Bezel**  For maximum physical security, this faceplate bezel can restrict access to the Luna Network HSM 7's front-facing inputs. Includes set of three (3) keys for each lock (locks are keyed differently). This item is included with the 10 Gbps Optical Ethernet model, and can be ordered separately for other models.

Qty	Item
1	**Sliding Rail Mounting Bracket Set**  The sliding rail system is designed for use in standard 483mm (19")-wide racks with depth of 620-902mm (24.5”-35.5”). The sliding rail mounts allow for easy removal and access to the rear face of the HSM. See "Using the Optional Sliding Rail System" on page 25 for installation instructions. The set includes: > (2) sliding rail mounts with removable side rails > (2) transformer brackets > (6) rail screws
1	**Sliding Rail Rack Mounting Screws**  Set includes: > (8) M5x8 flat-headed screws If you did not receive this set, you can request one from Thales (part number: 216-000034-001) or obtain your own suitable screws. If you do not use the screws included in this kit, ensure that the screw heads are flat enough so as not to interfere with the locking bezel.

Qty	Item
1	**Luna Backup HSM 7**  You can back up your selected Luna Network HSM 7 partition contents (root keys, certificates, other items) to a Luna Backup HSM 7. The Luna Backup HSM 7 is suitable for off-site storage and for backing up multiple HSM partitions. It can back up contents of password-authenticated or of multifactor quorum-authenticated HSMs. Refer to Luna Backup HSM 7.
2	**SFP 10 Gbps Optical Ethernet multimode transceiver modules**   If you ordered the 10 Gbps Optical Ethernet option, two of the RJ45 ports on the base-model appliance are replaced by SFP+ connectors (protected by dust covers during shipping). The SFP 10G Optical multimode transceiver modules are packed separately, within the appliance packaging, and must be inserted in the appliance before use.

Rack-Mounting the Luna Network HSM 7

The Luna Network HSM 7 appliance comes with front ear brackets, side rails, rear slider brackets, and the necessary screws packed separately in the carton. You may also have ordered the optional sliding rail mounting system. See "Luna Network HSM 7 Required Items" on page 16 for details. Instructions for installing both systems are provided below:

> If you intend to use the supplied mounting brackets, see "Using the Supplied Mounting Brackets" on the next page.

> If your order included the optional sliding rail mounting system, see "Using the Optional Sliding Rail System" on page 25. The sliding rails are recommended for ease of installation and maintenance.

> **CAUTION!** Do not attempt to mount the appliance using only the front brackets – damage can occur.

Using the Supplied Mounting Brackets

Install and adjust the rails and brackets to suit your equipment rack. The standard mounting bracket set is designed for use in standard 483mm (19")-wide racks with depth of 620-902mm (24.5”-35.5”).

> **CAUTION!** The included mounting hardware is meant for static positioning of the appliance. The long tab that slides into the bracket, applied to each side of the appliance, is adjustable for fitting the appliance into racks of varying depth - it must not be used to extend the appliance out of the rack.
>
> Optional gliding rails with rolling bearings are available for situations where rolling excursion of the appliance, while attached to the rack, is required for maintenance. See "Using the Optional Sliding Rail System" on page 25 (below).

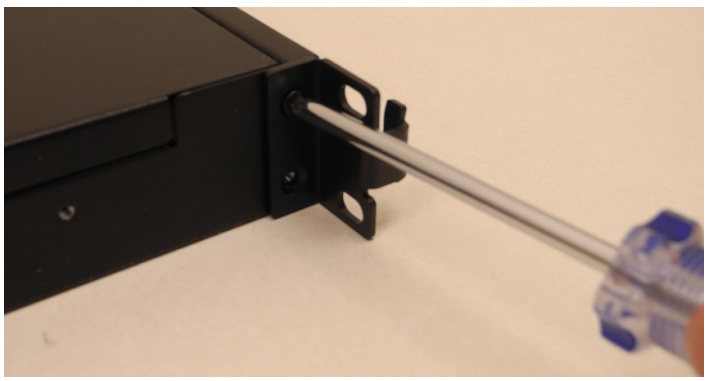
Ensure you have all the necessary components before proceeding. In addition to the supplied components, you will need:

- #2 Philips screwdriver
- hydraulic equipment lift

> **CAUTION!** If you are installing the appliance in a rack without a mounting tray or shelf, ensure that the appliance is supported at all times or damage may occur. Use of a hydraulic equipment lift is strongly recommended. If you do not have access to a lift, you will need at least one assistant to mount the appliance.

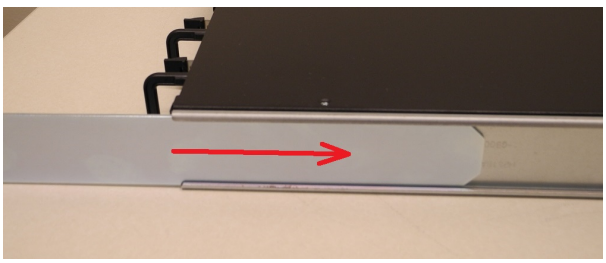
To mount the Luna Network HSM 7 hardware

1. Install the two front ear mounting brackets on the HSM chassis using the included screws and a #2 Phillips screwdriver.



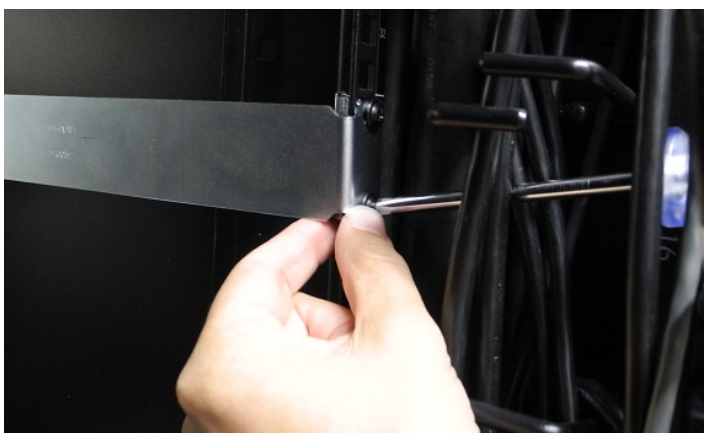
2. Fit eight cage nuts into the rack space where you want to install the appliance. Ensure that they are spaced correctly.

3. Install the two side rails on either side of the HSM chassis, using the included screws and a Phillips screwdriver. Note how the sliding rear brackets fit into the side rails.



4. Install the two sliding rear brackets in your equipment rack using four rack mounting screws.

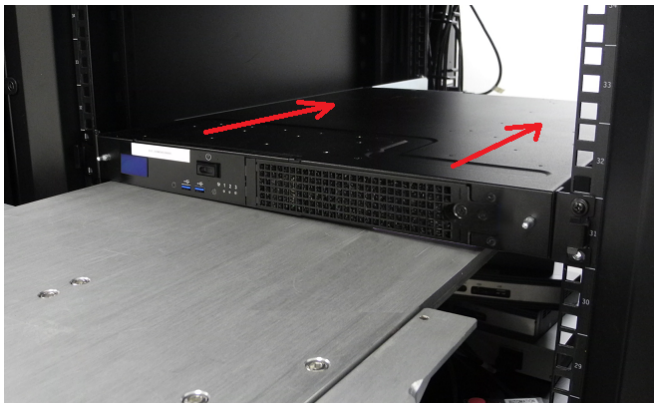
> **NOTE** While any standard equipment rack screws should fit the brackets, certain large-headed screws may interfere with the operation of the secure locking bezel.



5. Using a hydraulic lift, raise the HSM to the level of the brackets and extend the lift into the rack.

> **CAUTION!** Perform the next step from the rear of the server rack. Do not push the HSM off the lift without supporting its rear end.

6. From the rear of the server rack, pull the appliance back towards you until the sliding rear brackets fit into the side rails. Pull the appliance back onto the rear brackets until the front ear brackets meet the equipment rack.

> **CAUTION!** Support the weight of the appliance with the hydraulic lift until all four brackets are secured.

7. Secure the front ear brackets using rack mounting screws.

See "Luna Network HSM 7 Hardware Installation" on page 13 to continue the installation process.

Using the Optional Sliding Rail System

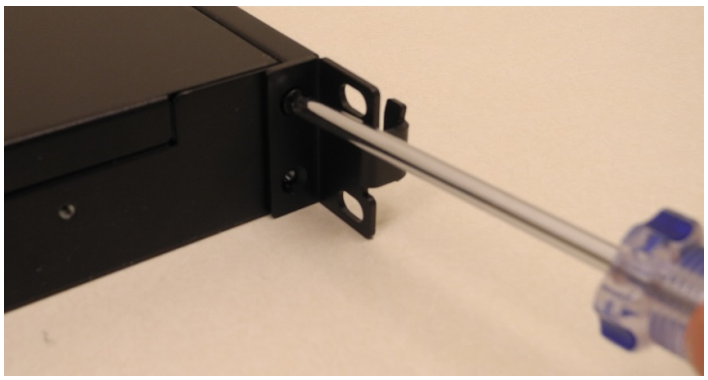
The optional sliding rail system allows for the appliance to be extended out in front of the equipment rack, possibly easing access to other racked appliances. This is rarely necessary. After configuration, the Luna Network HSM 7 should remain secured in the rack with the locking bezel installed. Some security standards require the use of this bezel. Leaving the HSM uncovered for ease of access might compromise physical security.

The sliding rail system is designed for use in standard 483mm (19")-wide racks with depth of 620-902mm (24.5”-35.5”).

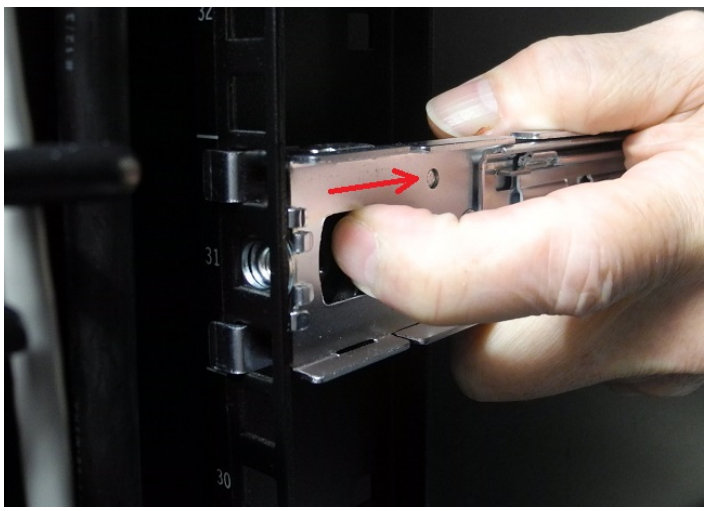
Ensure you have all the necessary components before proceeding. In addition to the supplied components, you will need a #2 Philips screwdriver.

To mount the Luna Network HSM 7 hardware

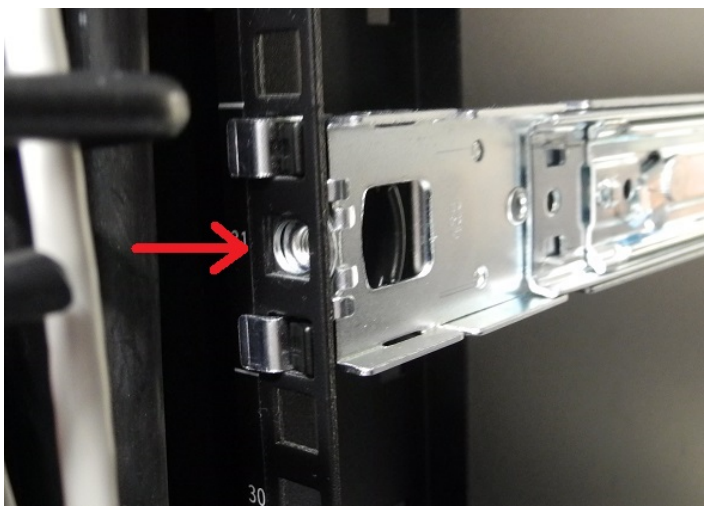
1. Install the two front ear mounting brackets on the HSM chassis using the included screws and a #2 Phillips screwdriver.



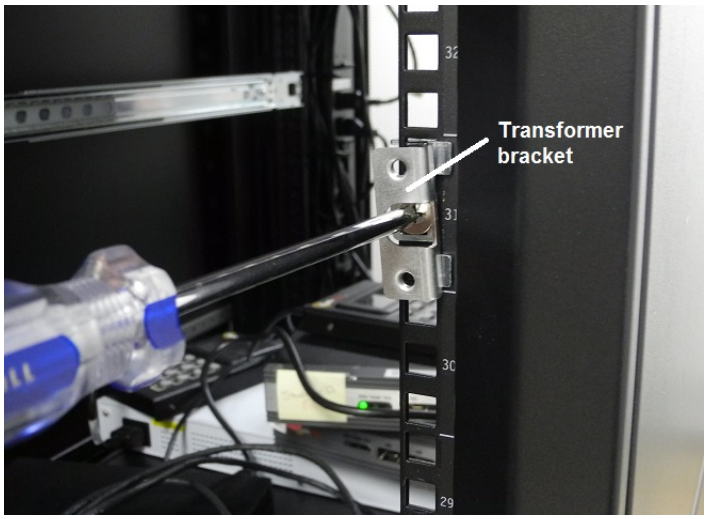
2. Fit the front end of each mount into either side of the rack and pull the spring-loaded latch at the rear to snap it in place.



3. Secure the rear end of each mount to the rack with two wide flat-headed screws.

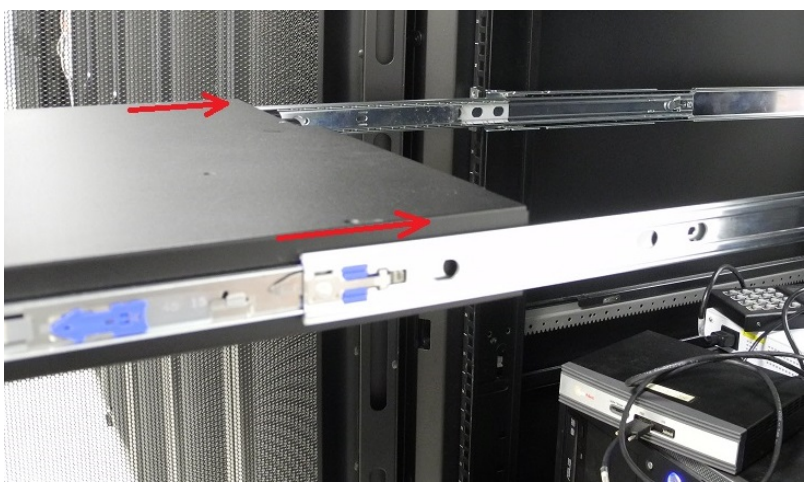


4. Fasten the transformer bracket to each sliding mount with two wide flat-headed screws.



5. Loosely thread two small flat-headed screws into each side of the Luna Network HSM 7. Fit each sliding rail over the screw heads and slide it forward into place before tightening the screws. Fasten each sliding rail with a third screw where it lines up with the hole in the HSM chassis.

6. Fit the sliding rails onto the rack mounts until they lock into place.



7. The HSM now moves smoothly and securely on the rails. Push the HSM all the way back and secure it to the transformer bracket with four rack screws.

> **NOTE** Screws with heads that are too large can prevent the locking bezel from fitting to the faceplate. Use the screws included with the Luna Network HSM 7, or other screws with suitable heads.

See "Installing the Luna Network HSM 7 Hardware" on the next page to continue the installation process.

Installing the Luna Network HSM 7 Hardware

This section provides basic Luna Network HSM 7 hardware installation instructions (connecting cables, booting, etc.). If you intend to mount the appliance in a standard equipment rack, see "Rack-Mounting the Luna Network HSM 7" on page 22 before following these instructions.

Installation Notes

- Any computer that is to act as a client to the Luna Network HSM 7 appliance must have the Luna HSM Client software installed. Windows users should log in to their computer as a user with Administrator privileges.
- A computer that is to be used only for administering the Luna Network HSM 7 does not need the Luna HSM Client software – only an SSH client such as the provided PuTTY program for Windows, or the SSH utilities that come standard with most Linux and UNIX platforms.
- A computer that is to be used for Remote PED workstation operation against a Luna Network HSM 7 must have the PEDServer software and PED USB driver installed. Applies to select Windows platforms only.
- All three tasks (Client, administration, and Remote PED) can be performed on a single computer, but in normal practice they are often separate tasks for separate computers.
- See About Remote PED if you will be using Remote PED.

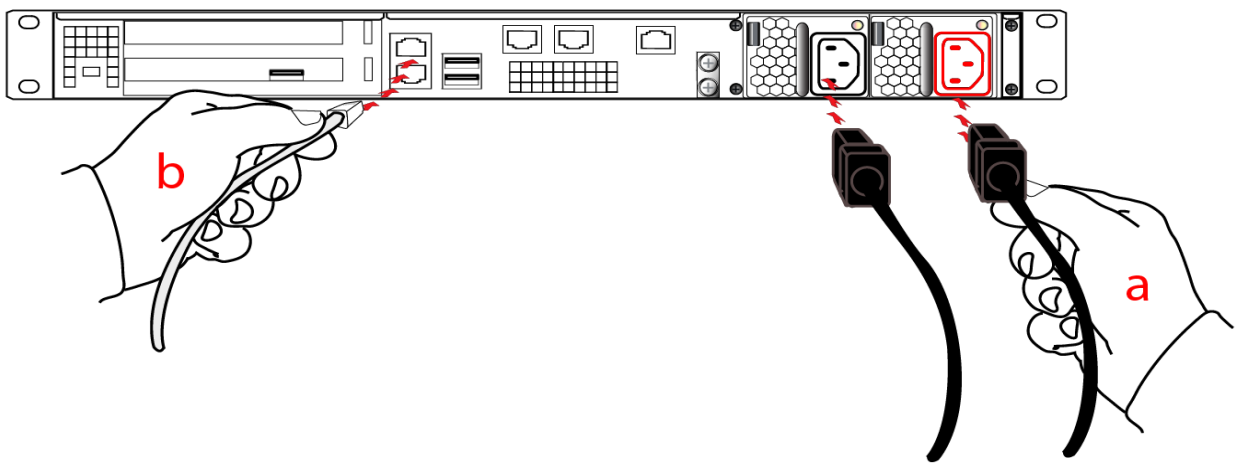
Installing the Luna Network HSM 7 Hardware

Follow these instructions to install and begin configuring the appliance.

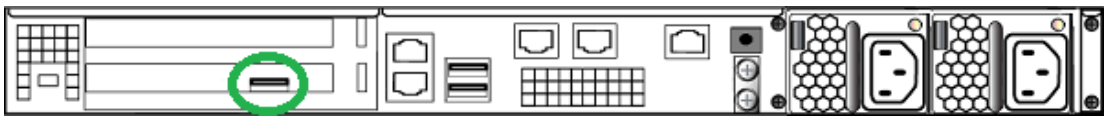
To install the Luna Network HSM 7 hardware

1. Insert the power (a) and network (b) cables at the rear panel.

   For proper redundancy and best reliability, the power cables should connect to two completely independent power sources.



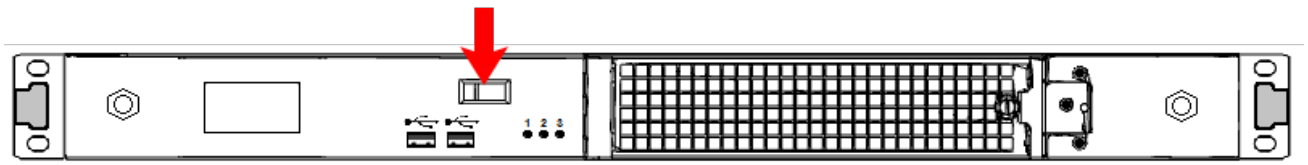
2. If you have a multifactor quorum-authenticated Luna Network HSM 7, connect the Luna PED directly to the HSM card's USB port (on the rear panel's left side), using the included USB-to-MiniUSB PED cable. See also Local PED Setup. If you have a password-authenticated HSM, skip to the next step.



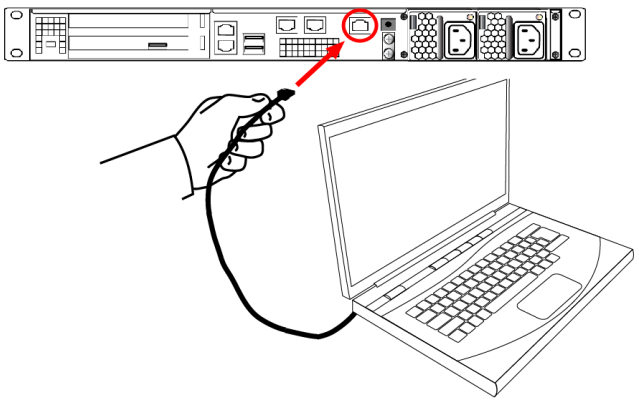
NOTE Refreshed-hardware Luna PEDs - identifiable by the part number on the manufacturer's label: 808-000060-002 or 808-000060-003, or by Luna PED Firmware 2.8.0 or newer - are powered by the USB connection and do not require a separate, external power adapter.

If you have an older Luna PED, it must be connected to a suitable power source. The USB 2.0 connection does not provide enough power to run the PED.

3. Press and release the Start/Stop switch on the front panel.



4. Connect the terminal port on the HSM appliance's rear panel to a dumb terminal, PC, or laptop, using the USB-to-RJ45 adapter cable (supplied). This terminal provides serial access to LunaSH for initial network configuration. See "Opening a Serial Connection" on page 54 for more information.



5. For maximum physical access security, when you are finished configuring the HSM, fit the locking bezel over the HSM's faceplate. Certain security standards require the use of these physical access measures. The locks fit over the posts highlighted below.

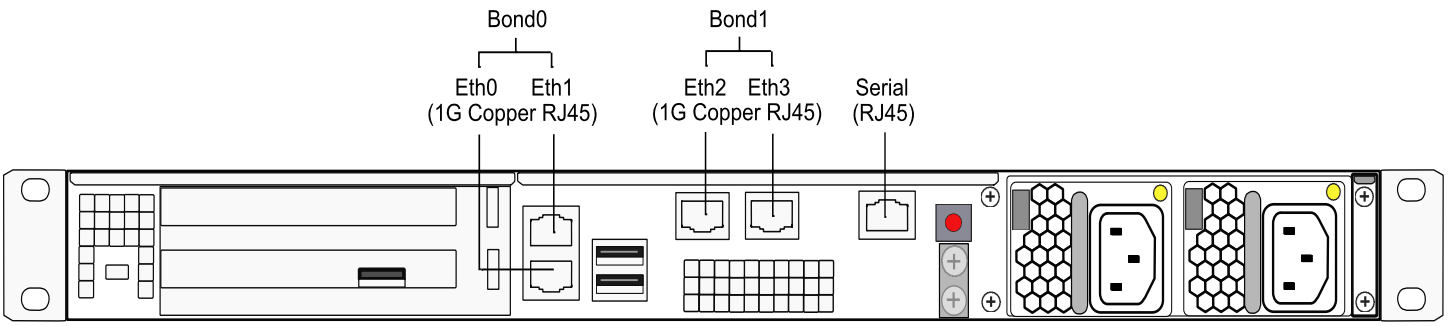
Turn the keys to the vertical position to lock the bezel. The keys cannot be removed if the bezel is unlocked. The two locks are keyed differently, so the keys can be issued to different security personnel and kept in secure, separate locations.

> **NOTE** Leaving the keys in the bezel could interfere with closing the rack door, and compromise security.

Installing optional 10 Gigabit Optical Ethernet

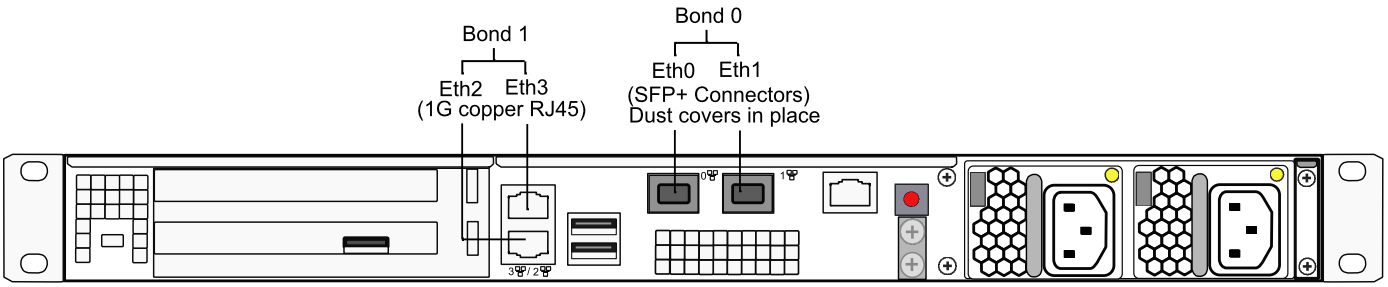
If you ordered the 10G Optical Ethernet option, then the two side-by-side RJ45 ports are replaced by optical-ready SFP+ connectors. The SFP optical Ethernet modules are packed separately, within the Network HSM shipping carton.

The original Luna Network HSM 7, with copper-only 1G Ethernet, looks like this (below) at the back panel.



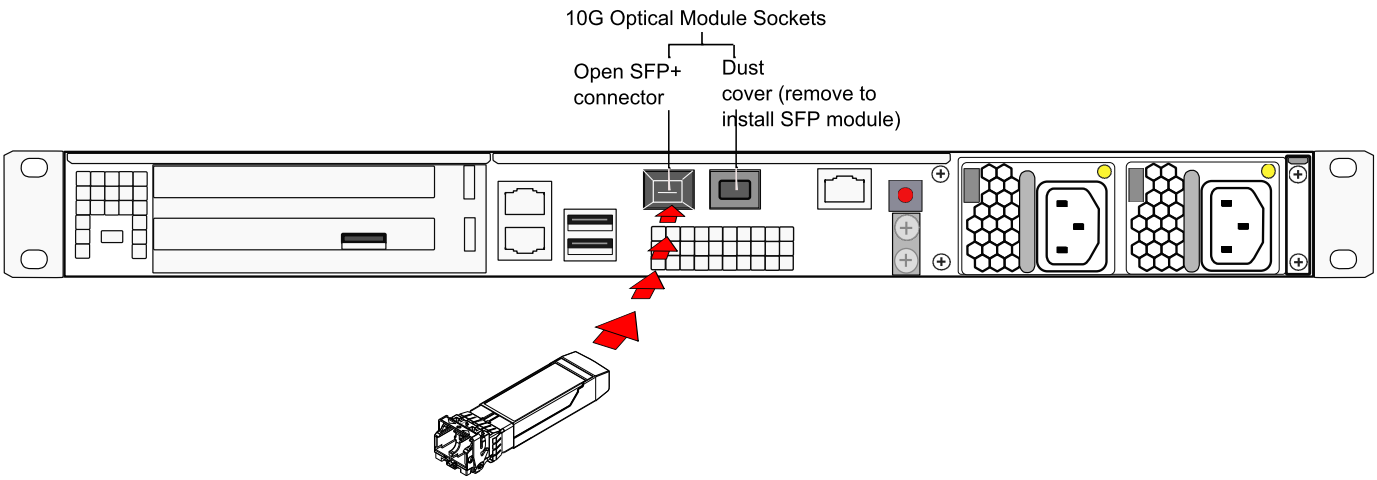
The Luna Network HSM 7 with the 10G Optical Ethernet option looks like this, below. The two optical-ready connectors are protected by dust covers during shipping and handling.

NOTE The physical ports assigned Ethernet port numbers by system software are changed; the new optical ports become Eth0 and Eth1, while the remaining RJ45 1G copper ports are labeled Eth2 and Eth3. This could require change to setup scripting, if you have previously installed and configured Luna Network HSM 7 appliances with copper-only Ethernet ports.



To install the SFP modules

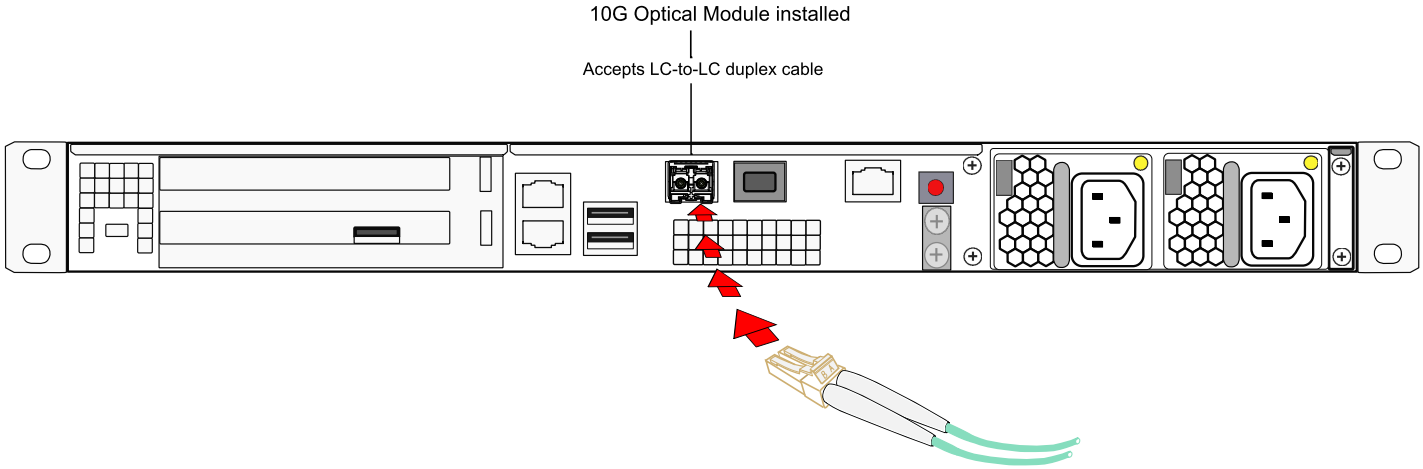
1. Locate the SFP modules in the accessory box, within the Luna Network HSM 7 shipping carton.
2. Remove the dust plug from one of the two SFP+ connectors on the back panel of the Luna Network HSM 7.
3. Remove an SFP module from its packaging and slide it into the selected connector slot, ensuring that the module seats firmly, making a positive connection at the back of the slot.



4. Repeat for the other 10G module if desired.

To connect a Dual L-to-L optical cable to an installed 10G SFP module

1. Remove the dust plug from the installed 10G SFP Ethernet module.
2. Insert the dual cable connector as shown.


10G Optical Module installed
Accepts LC-to-LC duplex cable

CHAPTER 2: Appliance Hardware Functions

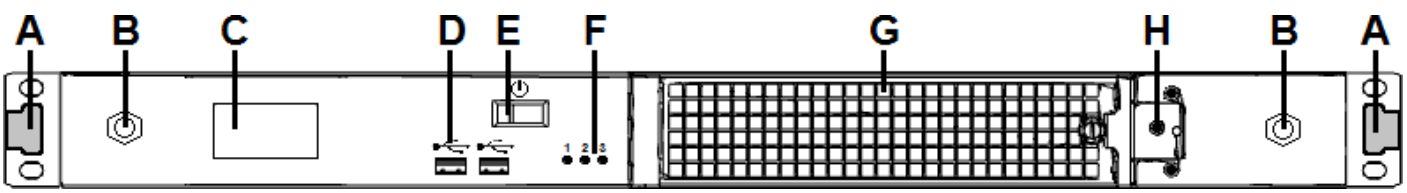
This chapter describes the administrative and maintenance tasks you can perform directly on the Luna Network HSM 7 hardware. It contains the following sections:

Physical Features

The Luna Network HSM 7 is 1U high and fits into standard 483mm (19")-wide equipment racks.

Front Panel

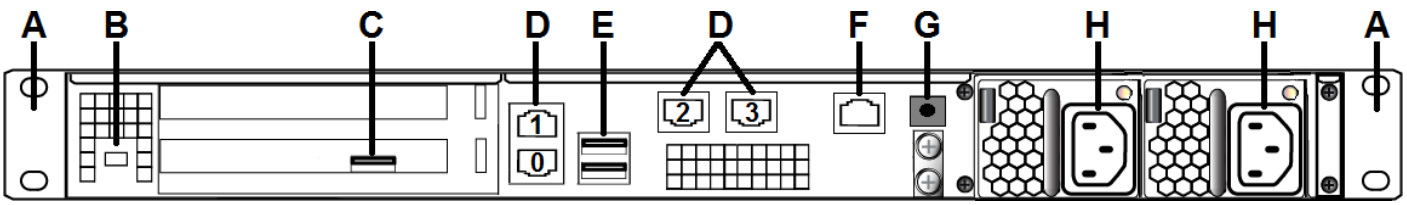
The front panel is illustrated below, with the secure locking bezel removed:



Item	Name	Description
A	Front ear brackets	Connect to the front of the appliance chassis with the provided screws, allowing it to be mounted in a standard 483mm (19")-wide equipment rack. The extending tabs act as posts for the locking bezel.
B	Mounts for locking bezel	The secure locking bezel connects to the appliance faceplate here.
C	Front-panel display	Displays basic configuration and status information for the appliance. See also "Front-panel LCD Display" on page 37
D	USB 2.0 ports	The appliance has a total of four (4) USB 2.0 ports (two on the front panel and two on the back), for connecting to such devices as card readers and backup HSMs.
E	Start/stop switch	Powers the appliance on or off. See also "Power-on, Power-off, or Reboot the Appliance" on page 41.
F	Fan status LEDs	The appliance has three (3) cooling fans. If these lights are illuminated, the fans are working correctly.
G	Ventilation fan filter cover	Removable cover allows cleaning of air filter. See also "Power Supply and Fan Maintenance" on page 43.
H	Fan bay securing screw	Torx screw secures the fan bay. **CAUTION!** Opening to swap fan modules triggers a tamper event on the appliance. See also "Power Supply and Fan Maintenance" on page 43.

Rear Panel

The rear panel is illustrated below:



Item	Name	Description
A	Sliding rail brackets	Connect to the sliding rails mounted on the sides of the appliance chassis, allowing it to be mounted in a standard 483mm (19")-wide appliance rack.
B	Kensington lock connector	Allows the appliance to be secured to a desk or equipment rack using a Kensington lock.

Item	Name	Description
C	HSM card USB port	When authenticating with a local Luna PED, the PED must be connected directly to the HSM card. **NOTE** This rule does not apply for multifactor quorum authentication to a Luna Backup HSM 7 connected to the appliance. In this case you connect a remote PED to one of the appliance USB ports and connect to the **pedserver** service running on the appliance at IP address 127.0.0.1. See Luna Backup HSM 7 Connected to Luna Network HSM 7 Using Remote Multifactor Quorum Authentication for more information.
D	LAN ports	The appliance has a total of four (4) 1Gbit LAN ports that can be bonded in active-backup mode. They are labeled on the illustration above as follows: > Bond0: eth0 and eth1 > Bond1: eth2 and eth3
E	USB 2.0 ports	The appliance has a total of four (4) USB 2.0 ports (two on the front panel and two on the back), for connecting to such devices as card readers and backup HSMs.
F	RJ45 serial port	Connect a terminal to this port using the included RJ45 to USB cable (see "Luna Network HSM 7 Required Items" on page 16). See also "Installing the Luna Network HSM 7 Hardware" on page 29.
G	Decommission button	This button should only be pressed as part of decommissioning and zeroizing the appliance. See also "Decommissioning the Luna Network HSM 7 Appliance" on page 190.
H	Power supplies	Connect the appliance to power. For proper redundancy and best reliability, the power cables should connect to two completely independent power sources. See also "Power Supply and Fan Maintenance" on page 43.

Luna Network HSM 7 Network Interface Configuration Variants

The configuration of the network interfaces on the Luna Network HSM 7 depends on the model, as follows:

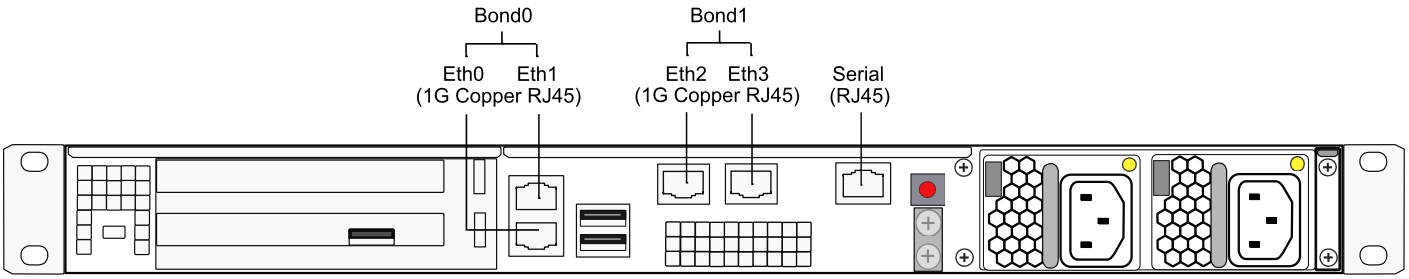
> The 1G model provides four 1G RJ45 copper Ethernet network interfaces.

> The 10G model provides two 10G SFP optical Ethernet network interfaces, and two 1G RJ45 copper Ethernet network interfaces.

The mapping of the network interfaces to their software equivalents (eth0, eth1, eth2, and eth3) is different on each model, as detailed in the following sections. The network interface mappings are not configurable.

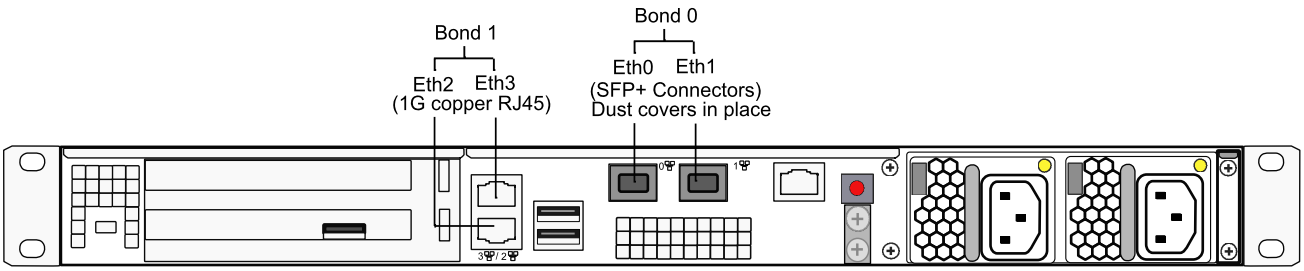
1G Model Network Interface Mapping

The 1G model provides four 1G RJ45 copper Ethernet network interfaces. You can optionally bond eth0 and eth1 to bond0, or eth2 and eth3 to bond1, to provide a redundant active/standby virtual interface.



10G Model Network Interface Mapping

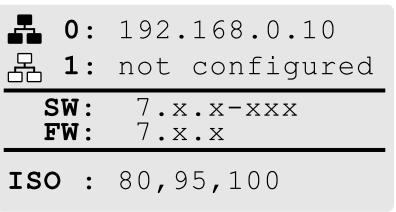
The 10G-equpped Luna Network HSM 7 provides two 10G SFP optical Ethernet network interfaces (mapped to eth0/eth1), and two 1G copper RJ45 network interfaces (mapped to eth2/eth3). You can optionally bond eth0 and eth1 to bond0, or eth2 and eth3 to bond1, to provide a redundant active/standby virtual interface.



Front-panel LCD Display

The LCD on front panel of the Luna Network HSM 7 provides basic configuration and status information for the appliance. The LCD is split horizontally into three sections as follows:

Figure 1: The LCD display



Top	Displays the current IP address configuration of the Ethernet ports on the appliance. If a port is configured, its IP address is displayed. If the port is not configured, the string "not configured" is displayed. This section automatically cycles between ports eth0 and eth1, and ports eth2 and eth3. The icons indicate the connection status of the port, as follows: An Ethernet cable is connected to the port. An Ethernet cable is not connected to the port.

Middle	Automatically cycles between displaying the following information: > Software (SW) and firmware (FW) versions currently installed on the appliance > Appliance host name > HSM label and HSM serial number
Bottom	Displays the current appliance state and status codes, as detailed in "Appliance State and Status Codes" below. The icon shading indicates the appliance state, as follows: **ISO** The appliance state is normal, indicated by dark text on a light background. **IST** **OOS** **OFL** **OFT** The appliance state is not normal, indicated by light text on a dark background.

Appliance State and Status Codes

The bottom section of the LCD displays the current appliance state and related status codes. The state can be one of the following.

ISO	In Service Operational. The appliance is operating normally. All services are running and the appliance is providing encryption/signing services as expected.
IST	In Service Trouble. The appliance is operational, but is experiencing a fault condition. The required services are operational and the appliance is able to provide encryption/signing services, but some services, such as SSH, are not running.
OOS	Out of Service. The appliance is not operational. The appliance is online but one or more required services are not operational. The appliance is not providing service. (* See, in particular, ALM codes that result in LCD Status OOS 30 displayed, at the bottom of this page.)
OFL	Offline. There is no network connectivity to the appliance. In this service state the appliance is not currently connected to the network and cannot provide service. **NOTE** Prior to Luna Network HSM 7 Appliance Software 7.8.3, this code is incorrectly displayed as **OFT** (see resolved issue LUNA-28763).

Status Codes

Each state is associated with one or more status codes, which provide additional information about the status of the appliance. For example, if there are no faults detected, the display indicates that the appliance is in service (ISO), with status code 0, so the display reads "ISO 0."

The codes are listed in the following table. You can also use lunash:> **status sysstat code all** to display a list of the possible status codes.

If one or more faults have been detected, the display shows the most severe status code until that fault has been corrected, then it displays the next most severe status code, until all errors have been corrected.

> **NOTE** Not all faults are serious. Some might merely indicate that an available service is not running because you chose not to run it.

The displayed messages update following a scan of selected system conditions, approximately every 15 seconds. If you have fixed a fault that caused an error, the display should clear the error indication at the next update. If the display continues to show the error message, then the fault may have re-occurred and you should investigate.

The statuses in the table, below, are displayed on the appliance front panel and are recorded in system logs that you can collect and parse remotely.

State	Status	Description
ISO	0	In Service Operational. No trouble.
	60	In Service Operational. The eth0 interface is offline. Use lunash:> **network show** and lunash:> **service status****network** to display more information about the status of the network interfaces.
	61	In Service Operational. The eth1 interface is offline. Use lunash:> **network show** and lunash:> **service status****network** to display more information about the status of the network interfaces.
	62	In Service Operational. The eth2 interface is offline. Use lunash:> **network show** and lunash:> **service status****network** to display more information about the status of the network interfaces.
	63	In Service Operational. The eth3 interface is offline. Use lunash:> **network show** and lunash:> **service status****network** to display more information about the status of the network interfaces.
	80	In Service Operational. The STC service is not running. Use lunash:> **service status****stc** to display more information about the status of the STC service.
	95	In Service Operational. The webserver service is not running. The REST API is not available. Use lunash:> **service status****webserver** to display more information about the status of the webserver service.
	100	In Service Operational. The SNMP service is not running. Use lunash:> **service status****snmp** to display more information about the status of the SNMP subsystem.

State	Status	Description
OOS	20	Out of Service. The NTLS service is not running. Use lunash:> **service statusntls** to display more information about the status of the NTLS service.
	25	Out of Service. The NTLS service is not bound to an Ethernet device. Use lunash:> **service statusntls** to display more information about the status of the NTLS service, and lunash:> **syslog tail** to view the system logs to help troubleshoot the issue.
	30	Out of Service. The HSM service has experienced one or more errors or critical events. Use lunash:> **hsm information show** and lunash:> **syslog tail** to help troubleshoot the issue.
OFL	50	Offline. None of the Ethernet interfaces are connected to the network. Use lunash:> **network show** to display more information about the status of the network, and lunash:> **syslog tail** to view the system logs to help troubleshoot the issue. **NOTE** Prior to Luna Network HSM 7 Appliance Software 7.8.3, this code is incorrectly displayed as **OFT** (see resolved issue LUNA-28763).
IST	70	In Service Trouble. The syslog service is not running. Use lunash:> **service statussyslog** to display more information about the status of the syslog service, and lunash:> **syslog tail** to view the system logs to help troubleshoot the issue.
	90	In Service Trouble. The SSH service is not running. Use lunash:> **service statusssh** to display more information about the status of the syslog service, and lunash:> **syslog tail** to view the system logs to help troubleshoot the issue.
	110	In Service Trouble. Hard disk utilization is too high. Use lunash:> **syslog tarlogs** to create a tar archive of the logs and then use **pscp** to transfer the log archive from the appliance to a remote computer for archiving.

NOTE The LCD initially displays the Thales logo when it (re)starts, and then displays the status information for the appliance. If you find that the LCD is failing to update, you may need to restart it using the service commands for the sysstat service (**service start sysstat**, **service stop sysstat** or **service restart sysstat**). You can also disconnect and reconnect the power from the appliance to restart the LCD.

Appliance reports out-of-service (OOS) code 30

Anything that halts the firmware (such as ALM_2004, ALM_2009, ALM_2026) results in an out-of-service code 30. Other critical events that halt the firmware include:

- failed self-test

- failure in the random number generator
- failure in integrity of the bootloader
- failure in integrity of the firmware
- failure in integrity of the HSM memory

Power-on, Power-off, or Reboot the Appliance

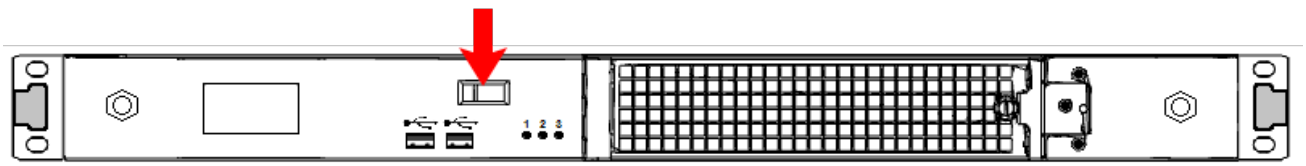
This section describes how to power-on, power-off, or reboot the appliance. It contains the following sections:

- "Power On" below
- "Power Off" below
- "Reboot" on the next page
- "Hard Reboot" on the next page
- "Automatic Restart Following a Power Interruption" on the next page

Power On

On the back panel, ensure that the power supplies are connected and working - the green LED on each power supply glows steadily when in operation.

If the appliance does not immediately begin to start up, press and release the START/STOP switch ⏻ on the front panel.



The HSM appliance begins to power up.

If power was removed while the system was on (either a power failure, or the power cable was disconnected), the system restarts without a button press. This behavior allows unattended resumption of activity after power interruption.

The front-panel LCD begins showing activity, then settles into the ongoing system status display once the appliance has completed its boot-up and self-test activity. See "Front-panel LCD Display" on page 37.

Power Off

To power-off the HSM appliance locally, press and release the START/STOP switch. Do not hold it in. The HSM appliance then performs an orderly shutdown (that is, it closes the file system and shuts down services in proper order for the next startup). This takes approximately 30 seconds to complete. In the unlikely event that the system freezes and does not respond to a momentary “STOP” switch-press, then press and hold the START/STOP switch for five seconds. This is an override that forces immediate shutoff.

> **CAUTION!** Never disconnect the power by pulling the power plug. Always use the START/STOP switch.

To switch off the HSM appliance from the LunaSH command line, use lunash:> **sysconf appliance poweroff**.

Reboot

To perform a system restart, you can switch the power off and then on again using the momentary-contact START/STOP switch on the front panel of the system, or use lunash:> **sysconf appliance reboot**.

To switch off the system, use lunash:> **sysconf appliance poweroff**, or use the START/STOP switch on the Luna Network HSM 7 front panel:

- If you issue the poweroff command, the system requests that you confirm by typing "proceed". After you type "proceed", the system returns a success message. From that point the orderly shutdown takes 15 to 20 seconds.
- After you momentarily press and release the START/STOP switch, the system performs a graceful shutdown, which takes 15 to 20 seconds.

If the system does not appear to be properly shutting down, then press and hold the front-panel START/STOP switch, which forces an immediate shutdown. This is not normally required, and should never be done unless it is required, since it bypasses the normal, graceful file-system closing and shutdown procedure.

Hard Reboot

The commands lunash:> **sysconf appliance reboot** and lunash:> **sysconf appliance poweroff** are preferred when you have easy physical access to the appliance, because they perform orderly shutdown, but you can access the START/STOP button if the commands fail.

For situations where you do not have convenient local access to the START/STOP button on the appliance, the preferred command choice is lunash:> **sysconf appliance hardreboot**.

- The disadvantage is that the shutdown is abrupt and not orderly - in a constrained and hardened system like Luna Network HSM 7, any risk is minimal, but not zero.
- The advantage of using the hard reboot is that, with many services and file closures being bypassed, there are far fewer opportunities for a shutdown or reboot sequence to hang in an unrecoverable state. You avoid the risk incurred by remotely using one of the other "softer" commands when there is no convenient access to the physical button override in the event that the command fails.

Automatic Restart Following a Power Interruption

If the appliance was deliberately powered down, using the START/STOP switch or lunash:> **sysconf appliance poweroff**, it remains off until you press the START/STOP switch. However, if power was removed while the system was on (either a power failure, or the power cables were disconnected - not good practice), then the system restarts without a button press.

This behavior allows unattended resumption of activity after power interruption. In most cases, it is assumed that this would never be needed, as you would install the appliance with its two power supplies connected to two completely separate, independent power sources, at least one of which would be battery-backed (uninterruptible power supply) and/or generator-backed.

Power Supply and Fan Maintenance

The two power supplies in the Luna Network HSM 7 appliance are hot-swap capable, meaning that one is sufficient to power the appliance while the other is removed and replaced, with no service interruption. The indicator light (LED) on each power supply shows different behavior, depending upon conditions.

Power Supply Condition	Power Supply LED
DC present/only standby output on	Flashing green (1Hz)
Power supply DC output ON and OK	Steady green
Power supply failure	Steady RED
Power supply warning	Flashing Blue/Red (1Hz) alternating
Input power failure (only in n+1 configuration)	Flashing Red (1Hz)

A power supply controller in the appliance monitors the state of the power supplies. It ensures that a failed power supply still gets sufficient direct current from the remaining power supply to light the indicator LED. The controller also sounds an audible alarm when there is a problem, such as one power supply not being connected to AC main power.

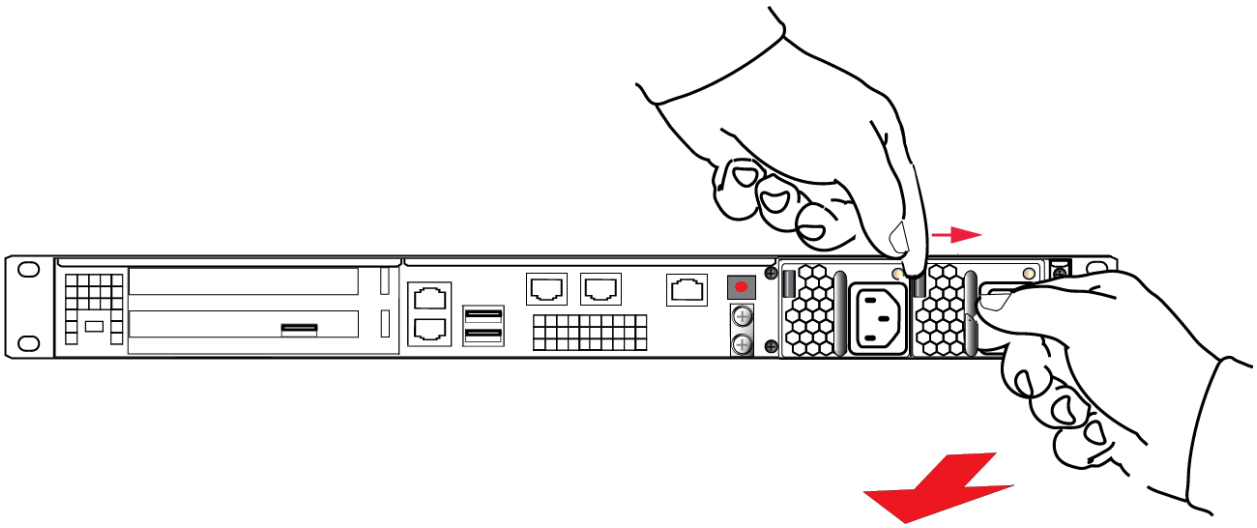
If only one power supply is present, the audible alarm is silent. If you wish to operate your Luna Network HSM 7 appliance with only one power supply, we recommend that you remove the second supply to silence the audible alarm.

Replacing a Power Supply

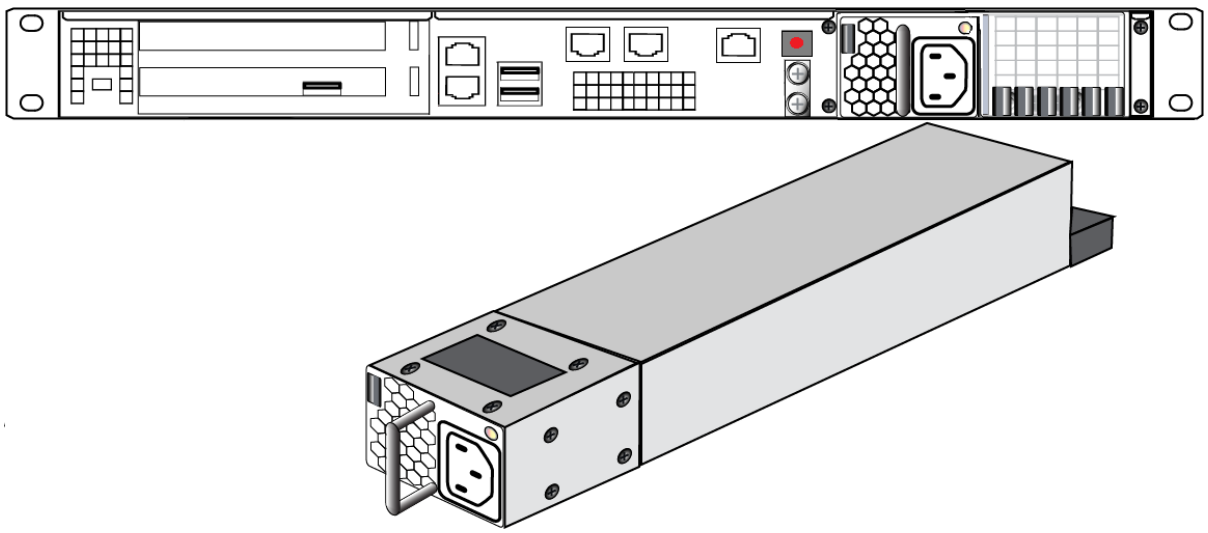
You may need to replace a power supply in the event of a failure.

To remove a power supply

1. To remove a power supply, face the back of the appliance.
2. Disconnect/unplug the selected power supply.
3. Press the lever sideways to release the power supply retaining catch, and simultaneously pull the handle out toward you.



Withdraw the power supply completely, using your other hand to support the body of the power supply as it emerges.



To re-install a power supply

1. To replace a power supply, reverse the steps above. Press firmly to seat the connector. The power supply can be fully inserted only in its proper orientation.
2. Connect an AC power cord.

The Fans

In normal operation, the fans should require no maintenance.

You might need to perform the following tasks:

> Clean the filter (occasionally)

> Replace a defective fan (rarely)

> **CAUTION! Opening the fan bay causes a system tamper event**
>
> We recommend that you use scheduled system maintenance downtime for this activity, as it will temporarily disrupt your client's access to your HSM partitions. If the system detects a tamper event, the HSM stops responding until you reboot (lunash:> **sysconf appliance reboot**), or until you use the Stop/Start switch on the appliance rear panel.

Cleaning the Filter

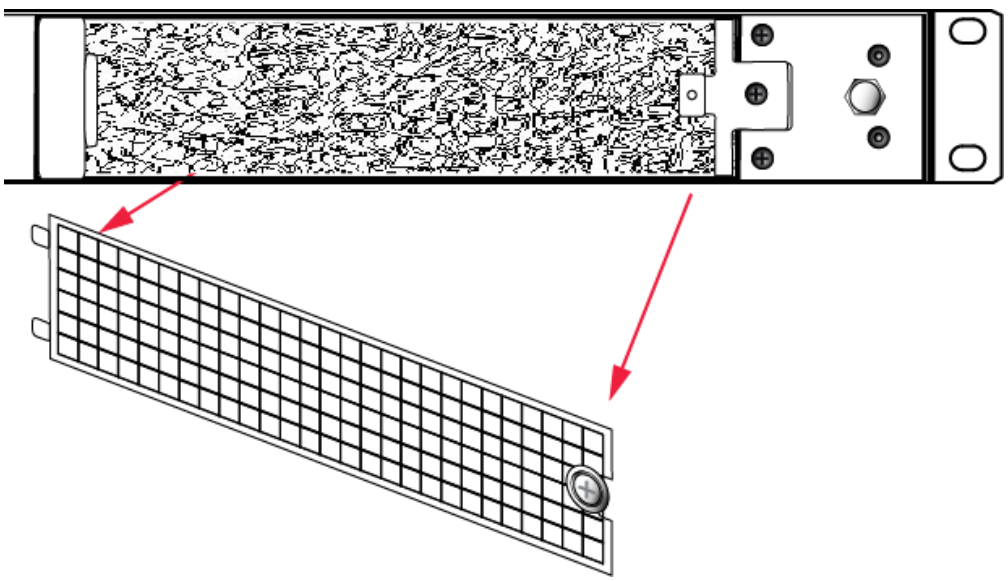
The ventilation grille, located to the right, on the appliance front panel, is secured in two parts, by two screws - a knurled, captive thumb-screw, and a Torx T8 screw. The knurled screw can be fastened or released without tools. It secures the lattice screen that in turn retains the mesh air filter.

While we recommend controlled-atmosphere environments for greatest longevity and reliability of the equipment, we recognize that some environments might include some dust in the air. The mesh filter traps larger particulate matter before it can be drawn into the interior of the appliance. In less-than-perfect non-clean-room conditions, the mesh might accumulate a buildup of dust, and should be cleaned occasionally for best cooling airflow into the equipment.

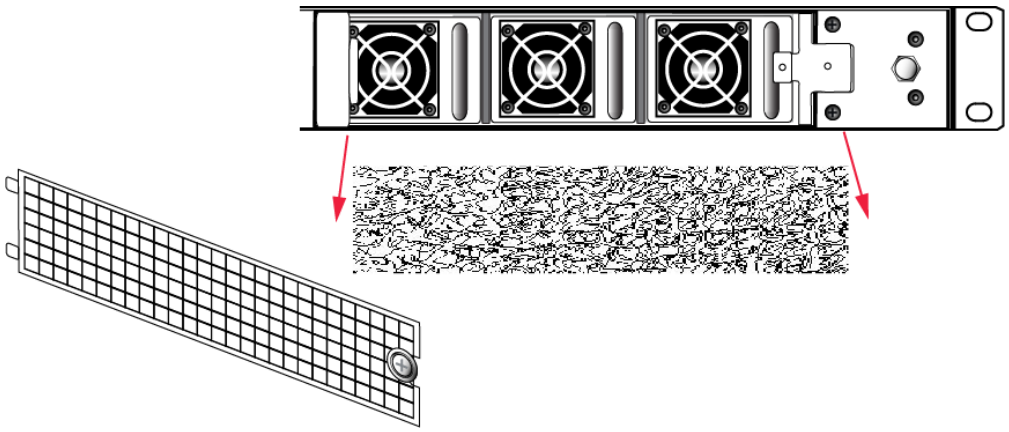
> **NOTE** Accessing the air filter mesh in front of the fans (using the thumbscrew to open the retaining grille) does not cause a tamper.

To clean the filter

1. Twist the knurled knob counter-clockwise until it no longer secures the airflow lattice. The lattice is anchored at its left end by two tabs, and can be easily pulled off the appliance, once the knurled retaining screw is loosened.



2. With the air filter exposed, it is easy to grasp the mesh with fingers and tug it free. The mesh is flexible and is held in its cavity only by friction. If it is dusty, handle carefully so as not to dislodge any dirt that could then be sucked in by the fans.



3. To clean the filter, either blow it out with compressed air (away from the vicinity of the appliance), or rinse with water. If using water, ensure that the mesh is dry before reinstalling.
4. To reinstall the mesh, place it in its cavity in front of the fans, and use fingers or a blunt tool to tuck-in the corners.
5. Then, replace the lattice in front of the mesh by inserting the tabs first, then swinging the lattice closed like a door, and securing with the knurled screw.

Replacing a Fan

The three fan modules (each containing two in-line fans) provide cooling redundancy. If one fan or module fails, it is detected by sensors. View a summary of appliance sensor conditions by running lunash:> **status sensors**. In the FAN section of the command output, the fans are listed in the order that they appear, left-to-right, as viewed from the front of the appliance. The example shows a fault with the first fan module:

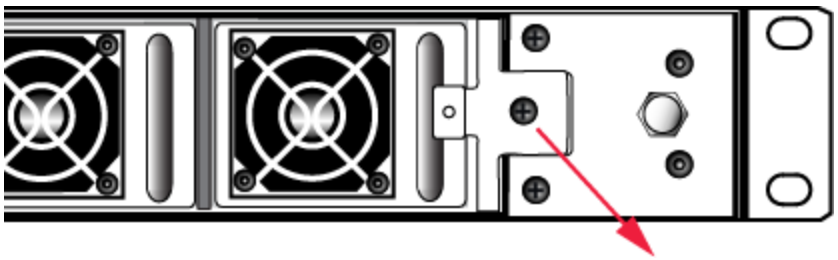
```
----------- Front Cooling Fans Status --------------
FAN1A  lnr     0 RPM   Unplugged or Failed
FAN1B  lnr     0 RPM   Unplugged or Failed
FAN2A  OK      3000 RPM
FAN2B  OK      2900 RPM
FAN3A  OK      2900 RPM
FAN3B  OK      3000 RPM
```

When the system returns from restarting, the HSM returns to find both splits of the MTK available and it immediately reconstitutes the MTK, allowing you to resume operations.

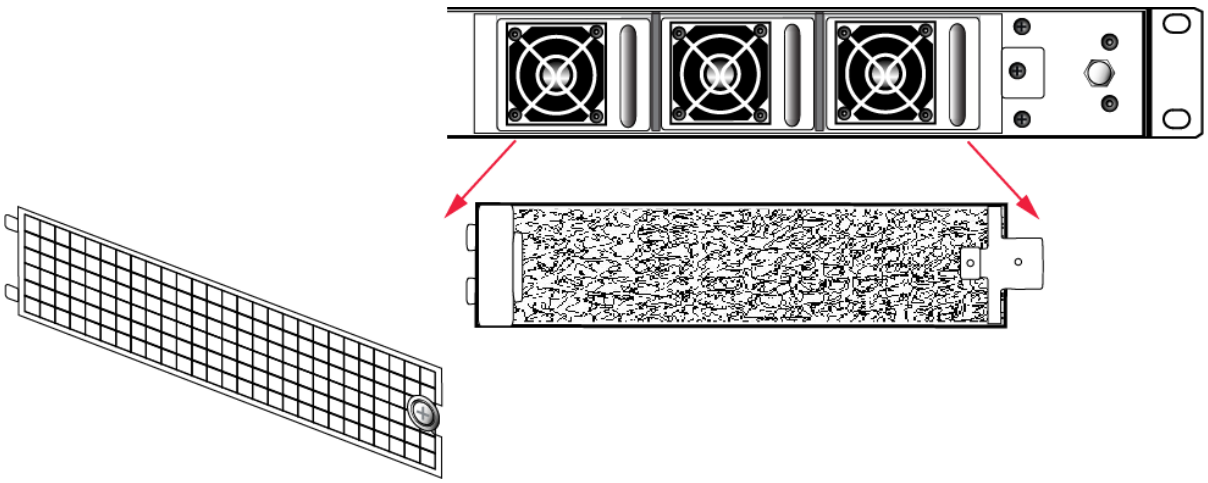
> **NOTE** Partition authentication data is de-cached by the tamper - you must re-activate each of your application partitions by logging in with the PED key and challenge secret before your clients can resume accessing them (see Activation on Multifactor Quorum-Authenticated Partitions). Partition activation does not survive a tamper event. In either case, you can examine the log for tamper events: lunash:> **syslog tail -search tamper -entries 200**

To replace a fan

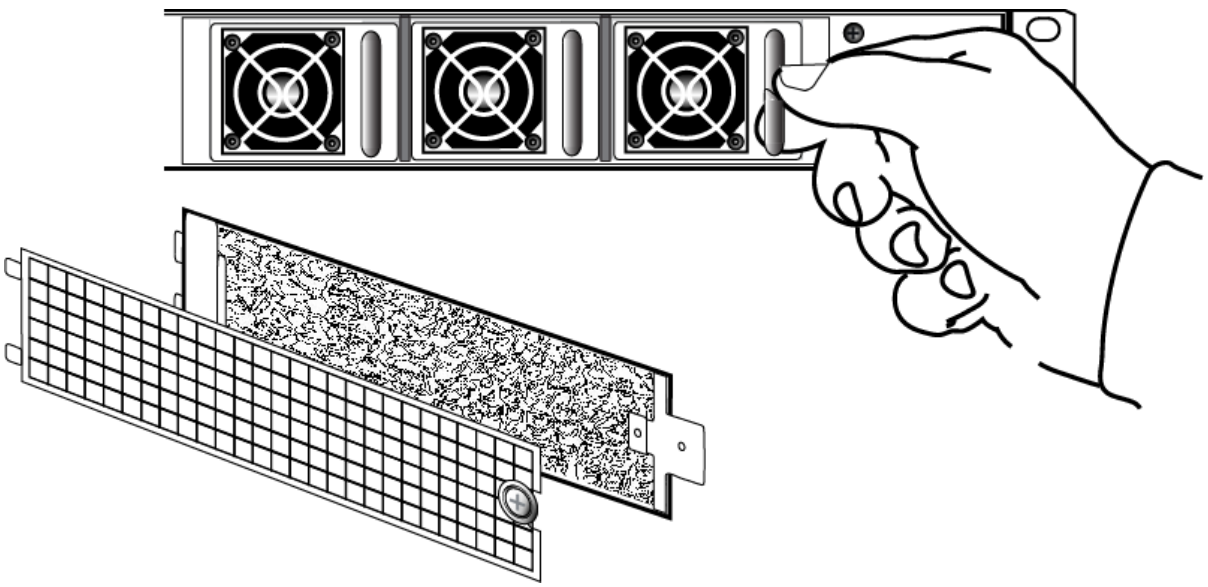
1. To open the fan bay, use a Torx number 8 screwdriver to remove the screw that secures the right-side tab of the fan retainer.



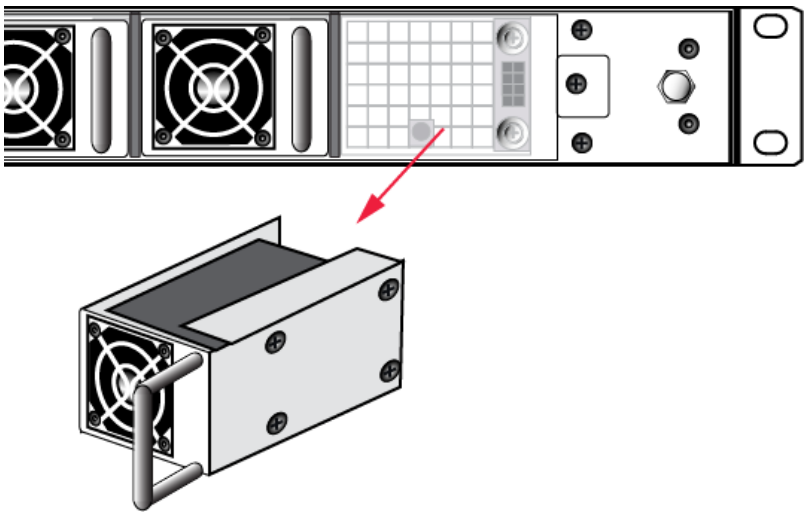
2. The fan retainer is anchored at its left by two tabs - swing the retainer out like a door, and remove it. There is no need to separate the filter mesh and its retainer from the larger fan retainer; the assembly can come out as one piece. The illustration below happens to show them separated.



3. The fan modules are now exposed and are held in place only by the friction of their electrical connectors.
4. Grasp the handle of the selected fan module and pull straight out toward you.



5. After slight initial resistance, the fan module should easily slide free of the appliance.



6. To replace the fan module or install a new one, reverse the above sequence.
   The index peg on the back of the module, and the matching index hole at the back of the fan bay, ensure that the module can be inserted only in its proper orientation.
7. Close up, replace the bezel, reconnect any cables, and return the appliance to service. If the power was left on during the operation, you will nevertheless need to restart (lunash:> **sysconf appliance reboot**) in order to clear the tamper event caused by opening the fan bay.
8. You will also need to re-Activate your application partitions by logging in with the PED key and challenge secret before your clients can resume accessing them (see Activation on Multifactor Quorum-Authenticated Partitions).

Summary

Removing, cleaning, and replacing the fan filter (the black mesh behind the grille) does not cause a tamper, and can be done at any time without disrupting your Clients.

Opening the fan bay (behind the filter), by unscrewing that Torx screw, does cause a tamper and therefore some down-time for your Clients. If only one fan module is showing a defect, you can probably leave replacing it until scheduled down-time, during which there would be no unexpected disruption to your Clients.

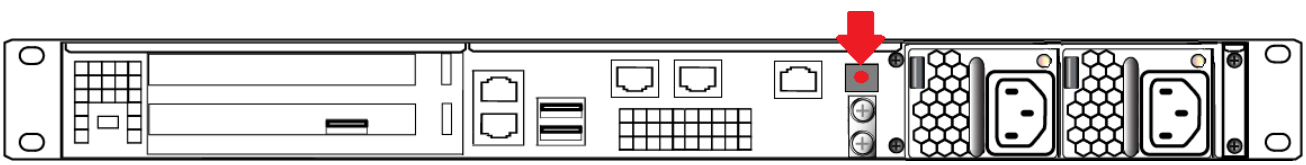
HSM Emergency Decommission Button

The Luna Network HSM 7 appliance includes a way to decommission the HSM, or permanently deny access to all objects on it, without need for either a serial console or a remote (SSH) connection.

To directly decommission the HSM (cryptographic module) inside the Luna Network HSM 7 appliance, press and release the small red button on the rear panel.

> The appliance does not need to be powered on.

> The appliance does not need to have power cables connected.



You will need a small screwdriver or other tool to reach the Emergency Decommission button. This is intentional, to prevent accidental pressing of that button.

What the Emergency Decommission Button Does

When you press the Decommission button, all partitions and their contents are deleted, as well as the **audit** role, and the audit configuration. The HSM policy settings are retained.

To bring the HSM back into service, you need to:

1. Reinitialize the HSM
2. Reinitialize the audit role and reconfigure auditing
3. Recreate the partitions
4. Reinitialize the partition roles

Event Summary

After the button is depressed:

- Communication to the internal HSM card is blocked, as is the software process that polls the HSM for status.
- At this point, you must power cycle the Luna Network HSM 7 appliance by depressing the momentary-contact START/STOP switch on the back panel of the system.
- After restarting, writes a tamper log message to the messages syslog.
- lunash:> **hsm show** displays the text `Manually Zeroized: Yes`, to signify that the system executed the decommission process.
- The HSM must be re-initialized (lunash:> **hsm init**) before you can begin using it again.

Comparison Summary

View a table that compares and contrasts the "Emergency Decommission" event with other deny access events or actions that are sometimes confused: Comparison of Destruction/Denial Actions.

Disabling Decommissioning

You can disable the decommissioning feature if you have the factory-installed **HSM Capability 46: Allow Disable Decommission** (see HSM Capabilities and Policies). The primary reason for disabling decommissioning is to prevent the HSM from being automatically decommissioned due to loss of battery (see Tamper Events). If decommissioning is disabled, you can continue to use the Luna Network HSM 7 after the battery has been depleted, but this is not recommended by Thales.

To disable decommissioning

Set **HSM Policy 46: Disable Decommission** to **1**(ON).

lunash:> **hsm changepolicy -policy 46 -value 1**

When to Use the Emergency Decommission Button

The primary purpose of the decommission button is for a situation where the appliance is not responding, you wish to send it back to Thales, but you need a way to permanently prevent access to material contained within the HSM. You might find other uses, in your organization.

What to do after decommission if the Luna Network HSM 7 is being returned to Thales

1. Obtain a Return Material Authorization and shipping instructions from Thales, if you have not already done so.
2. Pack the appliance and ship it to Thales.

Front Locking Bezel

The locking bezel (pictured below) fits over the front of the Luna Network HSM 7 appliance for maximum physical access security. The purpose of the bezel is to:

> cover the appliance's ports, and the power button

> lock the appliance to the rack to prevent removal

The locking bezel comes with three (3) keys for each lock. The locks are keyed differently so that keys can be issued to different security personnel and kept in secure, separate locations.

To lock the bezel

1. The locks fit over the posts highlighted below. Fit the bezel over the posts with both keys in the horizontal position.

2. Turn the keys to the vertical position to lock the bezel.

Remove the keys and store them in a secure location.

Replacement Keys

To obtain replacement keys, contact Technical Support (see "Support Contacts" on page 12). Please have the lock serial numbers ready. You can find these numbers on the sides of the bezel by each lock.

Power Consumption

When installed and connected to appropriate electrical power sources, the Luna Network HSM 7 draws power as follows:

Activity	Draw
Standby (connected to AC electrical mains but not powered on)	26W (typical)
Power-on inrush surge	15A (typical) 40A at 90-132VAC (max) 60A at 180-265VAC (max)
Active (under load from clients)	100W (idle) 105W (max)

The Luna Network HSM 7 appliance has two power supplies, each rated at 300W, either of which is capable of running the system alone.

CHAPTER 3: Configuring the Luna Network HSM 7 for Your Network

This chapter describes how to configure your Luna Network HSM 7 appliance so that you can access it over the network. This involves performing the following tasks, in the order specified:

1. "Powering Up the Appliance" below
2. "Opening a Serial Connection" on the next page
3. "Logging In to LunaSH" on page 101
4. "Recommended Network Characteristics" on page 57
5. "IPv6 Support and Limitations" on page 61
6. "Configuring IP and Network Parameters" on page 64
7. "Making Your Network Connection" on page 72
8. [Optional] "Setting TLS Ciphers" on page 73
9. "Setting the System Date and Time" on page 76
   a. "Setting the Time Zone" on page 79
   b. "Correcting Clock Drift Manually" on page 80
   c. "Network Time Protocol on Luna Network HSM 7" on page 81
10. "Generating the Luna Network HSM 7 Server Certificate" on page 84
11. "Binding Your NTLS or SSH Traffic to a Device" on page 90
12. [Optional] "Configuring RADIUS Authentication" on page 93

Powering Up the Appliance

Instructions on this page assume that the Luna Network HSM 7appliance has been installed, including the following:

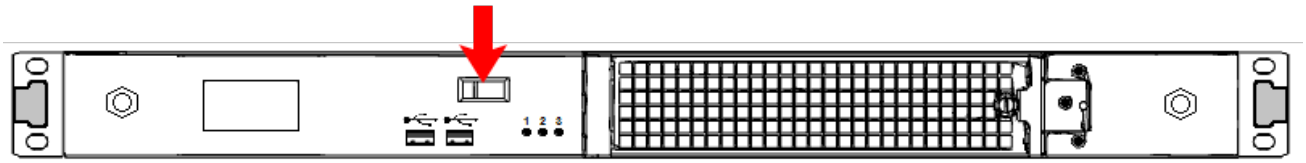
- Power connections: We suggest that each of the two power supplies be connected to an independent electrical source, and that at least one of those sources should be protected by UPS (uninterruptible power supply) and generator backup.
- A connection between the HSM appliance's serial terminal port and your administration computer or a terminal. This is a recommended option, so your administrative connection remains active when you assign new IP addresses; later, you would need a local serial link if you ever need to log in to the Recover account. See "Making Your Network Connection" on page 72.

The following instructions require the HSM appliance to be connected and running.

Power On Instructions for the Luna Network HSM 7 Appliance

On the back panel, ensure that the power supplies are connected and working - the green LED on each power supply should glow steadily.

If the appliance does not immediately begin to start up, press and release the START/STOP switch on the front panel.



The HSM appliance begins to power up.

If power was removed while the system was on (either a power failure, or the power cable was disconnected), then the system should restart without a button press. This behavior allows unattended resumption of activity after power interruption.

The front-panel LCD begins showing activity, then settles into the ongoing system status display once the appliance has completed its boot-up and self-test activity. See "Front-panel LCD Display" on page 37.

Power Off

To power-off the HSM appliance locally, press and release the START/STOP switch. Do not hold it in. The HSM appliance then performs an orderly shutdown (that is, it closes the file system and shuts down services in proper order for the next startup). This takes approximately 30 seconds to complete. In the unlikely event that the system freezes and does not respond to a momentary “STOP” switch-press, then press and hold the START/STOP switch for five seconds. This is an override that forces immediate shutoff.

> **CAUTION!** Never disconnect the power by pulling the power plug. Always use the START/STOP switch.

To switch off the HSM appliance from the LunaSH command line, use lunash:> **sysconf appliance poweroff**.

Next, see "Opening a Serial Connection" below.

Opening a Serial Connection

It is best to perform your initial configuration via direct serial connection to the Luna Network HSM 7 appliance. Once network parameters are established, you can switch to an SSH session over your network. However, if you are setting up your appliance on a network using DHCP, you can connect via SSH using the IP automatically assigned to the appliance's network interface.

Direct administration connection via serial terminal is the best method for initial configuration for the following reasons:

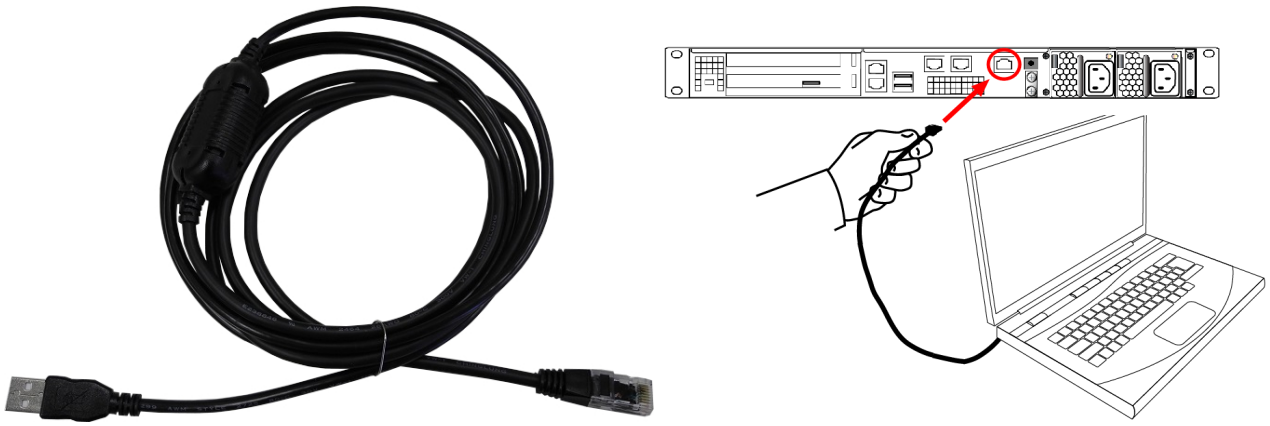
- When configuring network settings via SSH, in addition to requiring the original IP address, you may lose the connection when a new IP is set.

> A direct serial connection is the only route to log into the **recover** account, in case you ever lose the appliance's **admin** password and need to reset. Therefore, you should verify that the connection works before you need it - performing the appliance's network configuration is an ideal test.

> If you ever need to issue the lunash:> **hsm factoryreset** command, you must be connected through a local serial console for that command to be accepted.

To open a serial connection

1. Connect the serial port on the HSM appliance's rear panel to a terminal server, dumb terminal, PC, or laptop, using the supplied Prolific Technology Inc. USB to RJ45 (with 8P8C connector) adapter.



NOTE Do not connect the serial cable to one of the Ethernet ports.

2. If the driver for the Prolific Technology Inc. USB to RJ45 (with 8P8C connector) adapter did not download and install automatically, you can download the PL2303 USB-to-Serial Windows driver from https://prolificusa.com.

3. Open **Device Manager** (**Control Panel** > **Hardware** > **Device Manager**) and expand the **Ports (COM and LPT)** folder. If the driver installed successfully, an entry is displayed for the **Prolific USB-to-Serial Comm Port**, followed by the port associated with the adapter. For example:

   ```
   Prolific USB-to-Serial Comm Port (COM4)
   ```

   Record the COM port (COM4 in this example) associated with the adapter. You will need this port number when you open a serial connection.

4. Use a terminal emulation package, such as PuTTY, to open a serial connection to the COM port associated with your Prolific USB-to-Serial adapter. Set the serial connection parameters as follows:

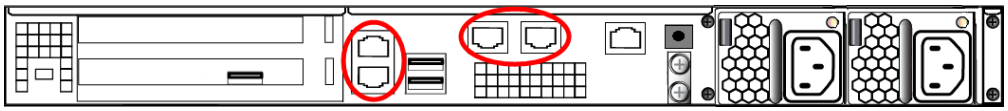
Baud rate	115200
Data bits	8
Parity	None
Stop bits	1

5. When the connection is made, the HSM appliance login prompt appears: **[local_host] login:**, where [local_host] is the currently configured host name. The displayed host name is updated when you assign a new host name to your HSM appliance and open a new session.

> **NOTE** You might need to press **ENTER** several times to initiate the session. You must log in within two minutes of opening an administration session, or the connection will time out.

To open an SSH connection

1. Connect one or more network devices in the rear panel of the appliance to a network with a running DHCP server.

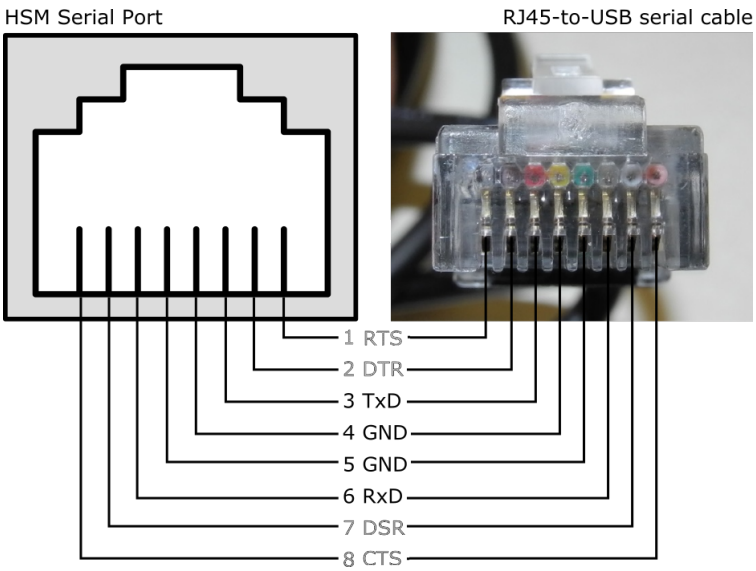


2. Wait for the appliance to acquire a new IP address from the DHCP server. The new IP will be displayed on the front-panel LCD screen.
3. Use SSH, or an SSH application such as PuTTY, to connect to the appliance using the displayed IP address.

Next, see "Logging In to LunaSH" on page 101.

Serial Pinout

The Luna Network HSM 7 appliance serial port uses a configuration equivalent to the Cisco Terminal Console. The Prolific Technologies Inc. RJ45-to-USB serial adapter cable uses a standard RJ45 pinout configuration:



> **NOTE** The Luna Network HSM 7 appliance does not implement serial handshaking, so RTS/CTS (pins 1 and 8) and DSR/DTR (pins 7 and 2) are not used for a successful connection.
>
> The important signals are TxD and RxD (pins 3 and 6).

Troubleshooting

This section contains recommendations for troubleshooting serial connections on the Luna Network HSM 7.

Windows 10 occasionally crashes when trying to detect a serial port
This is a known issue with the Windows 10 PL2303 drivers. If you experience trouble opening a serial connection using Windows 10, use another supported operating system.

Recommended Network Characteristics

Determine whether your network is configured optimally for use of Luna Network HSM 7 appliances.

> **NOTE** Always employ network security best practices. Place the Luna Network HSM 7 behind a firewall.

Bandwidth and Latency Recommendation

Bandwidth

> Minimum supported: 10 MB half duplex

> Recommended: at least 100 MB full duplex

- full Gigabit Ethernet is supported by default on all Luna Network HSM 7 7 appliances
- 10 Gigabit Optical Ethernet is a Luna Network HSM 7 appliance factory-purchase option (i.e., not field upgradeable).

> **NOTE** Ensure that your network switch is set to AUTO negotiation, as the Luna Network HSM 7 appliance negotiates at AUTO. If it is not, there is a risk that the switch and the appliance will settle on a much slower speed than is actually possible in your network conditions.

Network Latency

> Maximum supported: 500ms

> Recommended: 0.5ms

Latency and Testing Troubleshooting

Luna appliance client-server communication uses timeouts less than 30 seconds to determine failure scenarios. Thus the appliance does not tolerate network configurations or conditions that introduce a greater delay - problems can result, especially with High Availability configurations.

When you disconnect the network cable between any Luna appliance and a switch, and then reconnect, traffic should resume immediately, but with certain network switch configurations it might take 30 seconds for traffic to resume. The problem here is at the switch (not the Luna appliance).

If the switch is configured to run the Spanning Tree Protocol on the port, then there is a delay of about 30 seconds while it runs through a series of discovery commands and waits for responses. The switches can be configured to run in “PortFast” mode in which the Spanning Tree Protocol still runs on the port, but the port is placed directly into 'forwarding mode' and starts the traffic flowing immediately.

With the switch introducing a connection detection delay of 30 seconds or greater, transient network failures lasting only seconds are no longer tolerated. A simple test is to set up a ping stream and then disconnect and reconnect the network cable. The ping traffic should resume after a 1 or 2 second delay. A greater delay indicates that a switch in the network is not detecting the reconnection as quickly as is optimal. See the recommendations for network Bandwidth and Latency.

KeepAlive Setting

The Network Trust Link Service uses a keepalive function on the TCP layer, to maintain awareness of the link in low-traffic situations. The intent is to allow the Network HSM appliance to detect a dead peer (client) and respond appropriately. Response is invoked in situations where the client TCP stack has no opportunity to send a TCP reset to the NTL service on the Network HSM, like:

- client is powered down, or
- a network outage occurs

In such a situation, *if* **ntls tcp_keepalive** *is set*, then the NTL service (on the Network HSM appliance) recognizes a dropped connection after
(idlevalue + (intervalvalue x probesvalue)) / 60 = minuteswaiting

In the same situation *without* **ntls tcp_keepalive** enabled, a disconnected client would not be detected by NTLS (on the appliance) and the connection would be held in a Close_Wait state until NTL service was restarted.

How to decide
Many customer use-cases involve opening a session for a brief cryptographic operation or series of operations, and then closing the session. In such cases, the default values for the keepalive function are appropriate.

In the event that your application opens sessions that remain idle for long periods, with occasional bursts of activity, consider using the **ntls tcp_keepalive set** command with recommended values like these:

lunash:> **ntls tcp_keepalive set -idle 200 -interval 150 -probes 15**

Otherwise, set whatever values work best for your application's behavior/requirements and your anticipated network conditions.

Setting SSH Ciphers

Select from a list of available ciphers, to configure a desired subset, among which your appliance and clients can negotiate SSH session encryption. This ability is added with Luna Appliance Software 7.8.3.

The command sysconf ssh ciphers show displays the list of available ciphers (see below).

Modify the configured list

- with sysconf ssh ciphers set, which allows you to present a list for setting or removing from the configured list, or
- with sysconf ssh ciphers reset, which sets the configured list back to just the default ciphers (see below).

Available Ciphers

Using Luna Appliance Software 7.8.3 or newer, the following SSH ciphers are available:

- 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

This is an example, and is likely to change over time, as some ciphers age out of acceptability, due to their relative security being overtaken by newer technology and discovered threats. You can pick from that *available*-ciphers list to populate the *configured* ciphers list that is negotiable with a connecting system.

Default *configured* ciphers, from that list, are:

- aes192-ctr
- aes256-ctr

Cipher names are case sensitive.

Available MAC Algorithms

Using Luna Appliance Software 7.8.3 or newer, the following MAC algorithms can also be specified to encrypt SSH traffic:

> **NOTE** The MAC algorithms do not appear in the output for sysconf ssh ciphers show.

- hmac-sha2-256-etm
- hmac-sha2-512-etm
- hmac-sha2-256
- hmac-sha2-512

Configuring SSH Ciphers

At least one cipher must be configured. You may not remove all configured ciphers, leaving an empty configured list. You can remove the default configured ciphers by using the sysconf ssh ciphers set command.

- The sysconf ssh ciphers set command *always* takes a **-list**, containing at least one member. If you issue the command with a list that contains just one member, without also employing the **-add** or the **-remove** option, then you are *replacing* the entire current configured ciphers list with a list containing only one member.
- Attempting to use sysconf ssh ciphers set command with the **-remove** option, while specifying a **-list** that includes *all* currently configured ciphers yields "`Error: Cannot remove all currently configured SSH ciphers.`"
- Cipher configuration using the **-add** option *appends* the cipher names that you supply with the **-list** option, to the bottom of the current configured ciphers list.
- Cipher configuration using the **-remove** option *removes* the cipher names that you supply with the **-list** option, from the current configured ciphers list.
- Cipher configuration without the **-add** or **-remove** options simply replaces the current configured list with the ciphers included in the command after **-list**, in the order that you specify them.

A reimage operation on the appliance wipes all cipher configuration and sets the configured list back to the default ciphers, only. If reimage returns the appliance to a software version that did not include the **sysconf ssh ciphers** commands, then you cannot see or modify the available ciphers. The assumption is that, if you are reimaging away from a version that has the **sysconf ssh ciphers** commands, to one that does not, then either

- you are implicitly accepting the ciphers that were available/in-use at the time the reimage target appliance software was released, or
- you reimaged as a brief but necessary step on the way to updating your appliance to a desired version.

SSH cipher configuration survives appliance software update, and is unaffected by firmware changes (update, rollback).

The cipher names in the "available" list are the only valid ones to include in the **-list** for appending-to, replacing, or removing-from the configured list; no option is provided for inserting additional ciphers into the "available" list.

The colon ":" is the only character permitted as a separator in a **-list** of ciphers.

If you specify to **-add** a cipher that is already present in the configured cipher list, the command just silently skips that cipher and continues to the next cipher in the **-list**.

Adding a cipher to the configured ciphers list

1. Check the current list of SSH ciphers (available and configured).

   sysconf ssh ciphers show

2. Add a cipher from the available list to the configured list.

   sysconf ssh ciphers set **-list** <name of a cipher from the available list> **-add**

3. Verify that the list of SSH ciphers now includes the desired cipher.

   sysconf ssh ciphers show

Removing a cipher from the configured ciphers list

1. Check the current list of SSH ciphers (available and configured).

   sysconf ssh ciphers show

2. Remove a cipher from the configured list.

   sysconf ssh ciphers set **-list** <name of a cipher from the configured list> **-remove**

3. Verify that the list of configured SSH ciphers no longer includes the removed cipher.

   sysconf ssh ciphers show

Resetting the configured ciphers list

1. Check the current list of SSH ciphers (available and configured).

   sysconf ssh ciphers show

2. Reset the configured cipher list.

   sysconf ssh ciphers reset

3. Verify that the list of configured SSH ciphers now includes only the default ciphers.

   sysconf ssh ciphers show

IPv6 Support and Limitations

Internet Protocol version 6 (IPv6) is the most recent version of the Internet Protocol (IP). It is the result of a study effort from IETF to address limitations in IPv4 that date back to the 1970s. The "World IPv6 Launch" day occurred on June 6, 2012.

IPv6 upgrades to IPv4 are in the internet layer. The link layer remains unchanged. Transport layer and above are unchanged.

application layer	SSH, TLS/SSL, HTTPS
transport layer	TCP/UPD
internet layer	IP ← *All IPv4 to IPv6 upgrades are in this layer.*
link layer	Ethernet

In supporting IPv6, not everything in IPv4 was affected; some subsystems in the internet layer like routing protocols remain the same. The major internet layer upgrades to support IPv6 include:

- 128-bit IP address
- Fixed length, 40-byte header with support for new, optional Extension Headers
- Native security
- Auto-configuration

The most talked about feature in IPv6 is the vastly increased availability of IP addresses due to the IP address size increase from 4 bytes (billions) to 16 bytes (undecillions).

Unlike IPv4, IPv6 doesn't have broadcast addresses; it only has unicast and multicast addresses. A broadcast address is the logical address used for transmission to all network-connected hosts. A multicast address is similar to a broadcast address but its scope is limited to a defined group of network-connected hosts. A unicast address is used for point-to-point transmission.

Global Unicast Address format

For more information on IPv6 addressing, refer to the IP Version 6 Working Group (IPv6) at https://datatracker.ietf.org/wg/ipv6/documents/. Also, try: https://en.wikipedia.org/wiki/IPv6.

IPv6 in the Context of the Luna Network HSM 7

Most software components in the Luna Network HSM 7 operate in the application layer. They use TLS/SSL on top of TCP, but nothing uses the internet layer directly.

Likewise, changes in the internet layer shouldn't directly affect the application layer, but there are some utilities in Luna Network HSM 7 that use information from the internet layer, particularly the IP address, for authentication purposes; they will be affected by upgrading IPv4 to IPv6.

IPv6 Address Configuration Options

You can configure IPv6 addresses using static, SLAAC, or DHCPv6 addressing.

Static	Use lunash:> **network interface static**
SLAAC	Use lunash:> **network interface slaac** **Note:** You must have a SLAAC-enabled router in your network that is reachable by the Luna Network HSM 7 appliance to configure a network interface and obtain an IPv6 address using SLAAC protocol.
DHCPv6	Use lunash:> **network interface dhcp**

IPv6 Network Gateway

IPv6 devices must use an IPv6 gateway.

IPv6 Subnet Mask (Network Mask)

IPv6 devices must use CIDR notation for the subnet mask in IPv6 global unicast format.

For example, in IPv6 global unicast format, a subnet mask of /48 means that the 64-bit Network/Routing prefix will consists of a 48-bit site prefix, leaving 16 bits for the Subnet Identifier.

Typically, within a site, /64 is used to identify a whole subnet; global routing prefix + subnet ID.

Limitations When Using IPv6 on the Luna Network HSM 7

You should be aware of the following limitations before attempting to use IPv6 on your Luna Network HSM 7.

Client and Luna Network HSM 7 must use the same IP version

Clients connecting to the Luna Network HSM 7 appliance must use the same IP version that is configured on the appliance port they are connecting to, so certificates can resolve. Therefore, all clients connecting to an IPv4 port must have an IPv4 address, and all clients connecting to an IPv6 port must have an IPv6 address.

Secure Trusted Channel (STC) links not available via IPv6

STC links are not supported over an IPv6 network. You must use NTLS to make partition-client connections via IPv6.

Single global IPv6 address per network interface

You must use a single global IPv6 address for each active network interface: eth0, eth1, eth2, and/or eth3. You must use a single global IPv6 address for each active Luna HSM Client.

IPv6 address assignment methods (Static, DHCPv6, or SLAAC) are all allowed, however only one is allowed at a time. For example, avoid configuring your network infrastructure such that the following unsupported condition (scheme # 5 in the following table) occurs.

Scheme #	Address assignment scheme	RA M flag (on/off)	RA O flag (on/off)	Has RA prefix info (yes/no)	RA prefix info A flag (on/off)	Supported
1	Static	either	either	either	either	yes
2	DHCPv6 (stateful)	on	either	either	off	yes
3	DHCPv6 (stateless)	off	on	yes	on	yes
4	SLAAC	off	off	yes	on	yes
5	SLAAC + DHCPv6	**on**	either	yes	**on**	**no**

Notes:

1. “RA” stands for Router Advertisement, the critical NDP message used in IPv6 auto-configuration.
2. The above table assumes that a functioning DHCPv6 server is on the network.
3. Scheme #3 (“Stateless” DHCPv6) is configured on Luna Network HSM 7 7.x using SLAAC for address assignment, but DHCPv6 is still used to configure network services like DNS.

Example:

The following example for the eth2 interface is not supported since it has both DHCP, `2018:1:2:3::dcd5/128`, and SLAAC, `2018:1:2:3:215:b2ff:fea8:fd44/64`, global addresses (i.e. entries with “scope global”).

```
4: eth2: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq state UP qlen 1000
   link/ether 00:15:b2:a8:fd:44 brd ff:ff:ff:ff:ff:ff
    inet6 2018:1:2:3::dcd5/128 scope global dynamic
       valid_lft 1036733sec preferred_lft 691133sec
    inet6 2018:1:2:3:215:b2ff:fea8:fd44/64 scope global noprefixroute dynamic
```

```
      valid_lft 2591923sec preferred_lft 604723sec
   inet6 fe80::215:b2ff:fea8:fd44/64 scope link
      valid_lft forever preferred_lft forever
```

Configure the IP Address and Network Parameters

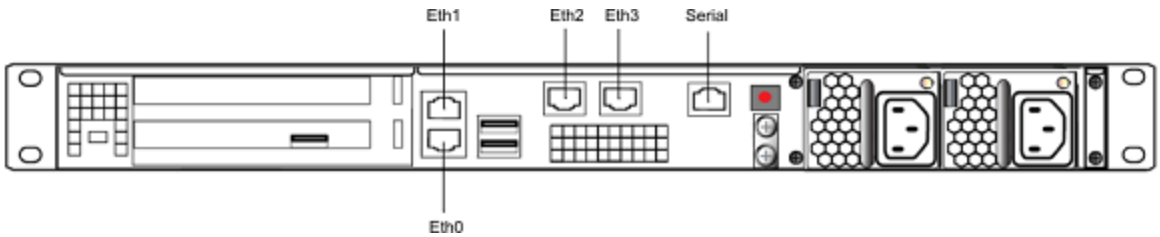
To proceed with configuring the IP address and other network parameters for the Luna Network HSM 7, go to "Configuring IP and Network Parameters" below.

Configuring IP and Network Parameters

The Luna Network HSM 7 is a network device that is intended to be installed in a data center and accessed remotely over a network. Network access to the Luna Network HSM 7 is provided by four 1 Gb/s Ethernet LAN ports. The Luna Network HSM 7 is also equipped with an RJ-45 serial port, used to provide serial access to the appliance for initial network configuration.

> **NOTE** Always employ network security best practices. Place the Luna Network HSM 7 behind a firewall.

The network device interfaces (eth0, eth1, eth2, and eth3) and serial port are located on the rear of the appliance, as illustrated below:



Serial port

Thales recommends using a device connected to the Luna Network HSM 7 appliance serial port to make any changes to the network configuration and routes. If you use an SSH connection to make such changes, the connection can be disrupted by the changes, and associated commands may be interrupted. Partially-configured network settings can make the Luna Network HSM 7 inaccessible via remote SSH connection.

Ethernet LAN device configuration

Depending on the model you chose at time of purchase, the Luna Network HSM 7 is equipped with:

- 4 individually-configurable 1 GB/s auto-sensing Ethernet LAN network devices
- 2 10G SFP optical Ethernet network interfaces (mapped to eth0/eth1), and two 1G copper RJ45 network interfaces (mapped to eth2/eth3)

You can configure the following network settings for each device:

- IPv4 or IPv6 address. You can configure the addresses using static or DHCP addressing. If you are using IPv6 addressing, you can also use Stateless Autoconfiguration (SLAAC) to have a SLAAC-enabled router in your network automatically configure an IPv6 address on a device.
- Network gateway. IPv4 devices must use an IPv4 gateway. IPv6 devices must use an IPv6 gateway.

> Network mask. IPv4 devices must use dotted-quad format (for example, 255.255.255.0). IPv6 devices can use full or shorthand syntax.

> Static network route.

> DNS configuration. Although you configure DNS at the device level, the settings you configure for a device are available to all devices on the appliance if the configured device is connected to the network. To ensure DNS access, it is recommended that you configure each device. You can configure the following settings:

  - DNS nameservers. You can add up to three DNS nameservers.
  - DNS search domains.

  These settings apply to static network configurations only. If you are using DHCP, the DNS search domains and DNS nameservers configured on the DHCP server are used.

Network Routing Table

The Luna Network HSM 7 appliance software allows you to configure the routing table to suit your network. With appliance software versions older than 7.7.0, you can configure a default route for each network interface or bonded virtual interface (eth0/eth1/eth2/eth3/bond0/bond1). The default route for the device is defined automatically when using DHCP, or by specifying the **-gateway** option when configuring a static address.

Using Luna Network HSM 7 Appliance Software 7.7.0 or newer, the network routing table can have one default route only, bound to one network device or bonded virtual interface. The default route is defined automatically when using DHCP, or by specifying the **-gateway** option when configuring a static address. The first interface configured is automatically assigned the default route. Once a default route is defined, no additional default routes can be defined without deleting the first default route. You can use **network show** at any time to see which device has the default route set -- **Default Route (eth#) : Yes/No**.

The default route is tied to the gateway, so interfaces that do not have the default route have their gateway value automatically dropped -- the Gateway field in the output from **network show** will be empty.

Use the **network route** commands to make changes to the routing table.

CAUTION! A change to network routing when updating to Luna Network HSM 7 Appliance Software 7.7.0 or newer, from any prior 7.x version, can cause your appliance to become unreachable via network connection. Older appliance versions permitted the existence of multiple default routes. Beginning with Luna Network HSM 7 Appliance Software 7.7.0, only one instance of the default route can exist.

Options for a successful update with minimal disruption are:

> Remove all but one instance of the 'default route', using the **network route delete** command, *before* upgrading from any appliance software version older than Luna Network HSM 7 Appliance Software 7.7.0.

> Connect locally via serial cable to perform the update, so your access to the network appliance is not lost when network connection becomes temporarily unavailable (pending proper network configuration).

Note also that if you re-image, going back to a version older than Luna Network HSM 7 Appliance Software 7.7.0, the routing table goes back to the old format and you must apply one of the above precautions again, to update.

If the above precautions are not taken and the appliance becomes unreachable, complete the following steps to restore connection to the appliance:

1. Connect locally via serial cable.
2. Delete all network interfaces. See network interface delete.
3. Configure a network interface to use a default route by doing one of the following:
   - Configure the network interface to use a static IP configuration while specifying the **-gateway** option. See network interface static.
   - Configure the network interface to use DHCP. See network interface dhcp.

After you complete the above steps, network connectivity to the appliance is restored and any remaining interfaces that are configured do not have a default route set.

Port Bonding

The Luna Network HSM 7 supports port bonding. Port bonding allows you to create a bond between two interfaces (eth0 and eth1, or eth2 and eth3) into a single bonded interface (bond0 or bond1). In a bonded interface, both ports are bound to a virtual interface with a single IP address, with one port active and one port standby. See "Luna Network HSM 7 Appliance Port Bonding" on page 152 for more information.

NTLS Binding

You can bind the NTLS traffic (used to securely transport cryptographic messages exchanged between a client and the HSM across the network) to a specific Ethernet device (eth0, eth1, eth2, eth3, bond0, bond1, all) on the appliance. This allows you to divide the traffic going to the appliance into cryptographic (destined for the HSM) and administrative (LunaSH) streams, for enhanced security and performance. See "Binding Your NTLS or SSH Traffic to a Device" on page 90 for more information.

SSH Binding

You can optionally bind/restrict the SSH traffic (used to securely transport administrative messages across the network) to a specific Ethernet device (eth0, eth1, eth2, eth3, bond0, bond1, all) on the appliance, to the appliance hostname, or to a specific IP address. This allows you to divide the traffic going to the appliance into cryptographic (destined for the HSM) and administrative (LunaSH) streams, for enhanced security and performance. By default, SSH traffic is unrestricted. See "Binding Your NTLS or SSH Traffic to a Device" on page 90 for more information.

Gathering Appliance Network Information

Before you begin, obtain the following information (see your network administrator for most of these items):

HSM Appliance Network Parameters

- IP address and subnet mask for each LAN port you want to use (if you are using static IP addressing)
- Hostname for the HSM appliance (registered with network DNS)
- Domain name (per port)
- Default gateway IP address (per port)
- DNS Name Server IP address(es) (per port)
- Search Domain name(s) (per port)
- Device subnet mask (per port)

DNS Entries

- Ensure that you have configured your DNS Server(s) with the correct entries for the appliance and the client. The HSM appliance expects fully qualified hostnames.
- If you are using DHCP, then all references to the Client and the HSM appliance (as in Certificates) should use hostnames.

Other Considerations

Clients need to be able to route directly to each HSM appliance they need to talk to, with no load balancing in place. The Luna Network HSM 7 does not work with off-the-shelf load balancers and service discovery techniques. You can NAT or forward the traffic so long as it always goes to the same place so the TLS tunnel isn't terminated by outside forces.

Default Route and Gateway

When setting up, or adjusting, network configuration, keep in mind that the first interface to be configured gets the default route.

From Luna Network HSM 7 appliance software version 7.8.1 onward, a network interface gateway is tied to the default route. If there is no default route then the gateway field is automatically dropped. A default route cannot be applied to an interface that was not configured with a gateway (referring to static configuration since DHCP automatically obtains the gateway).

If an issue occurs in that respect, recover by re-configuring (dhcp or static) the interface that is intended to have the default route, by specifying the gateway, and it automatically has the default route applied.

The default route could, for example, be removed from an interface using network route delete by specifying 0.0.0.0 as the gateway field. If, later on, you want that interface to have the default route, you must re-configure it (specifying the gateway) *while no other interface has the default route*. In that case, the interface automatically gets the default route.

Some Network Configuration Best Practices

Consider how you would proceed for (say) a Linux server with very sensitive data and that contains 4 NICs. Whatever you would do for the most sensitive servers you have, that's what you should do for the HSMs.

Do you separate flows between admin networks and application network? Then do that with the HSM.

Do you divide into 3 layers like DMZ/L1/L2 and put sensitive equipment in the L2 network? Then do that with the HSM.

Do you put the sensitive servers behind a firewall or particular router? Then do that with the HSM.

Do you set specific routes in your Linux servers? Then do that with the HSM.

Do you use specific DNS servers with internal split views? Then do that with the HSM, for the same reasons.

After every network configuration command you issue, follow that with network show to confirm:

- that what you expected to happen did happen
- that nothing else unexpected was triggered by your change. (See previous section above about interdependency of gateway and default route, for example.)

Configuring the Network Parameters

You can use the serial connection to configure all of your network parameters now, or you can perform a minimal configuration now, where you only configure a single port, and then use the configured port to access the appliance over the network and complete the configuration.

> **NOTE** Use a locally connected serial terminal when changing the appliance IP address, to avoid SSH admin console disconnection due to the change.

To configure the appliance and port network parameters

You can configure all of the ports now, using the serial connection, or you can configure only one port now, and then use a network connection to that port to configure the remaining ports. It is recommended that you configure and test each device. You need to know the IP address of at least one network interface to establish a SSH connection to the appliance.

Once configured, you can find the interface IP addresses on the appliance's front-panel LCD screen. If there is no IP address shown on the LCD, you must use a serial port connection to connect to the appliance.

1. Configure the IP address, network mask, and gateway (optional) on at least one of the Ethernet LAN ports, using the **network interface** commands. You can configure the ports to use an IPv4 or IPv6 address. A mix of IPv4 and IPv6 ports is supported. If you are configuring the device using DHCP, the first device configured will receive the default route for the appliance. If you are configuring a static address, the **-gateway** option is used to define the default route. The first device configured with a gateway receives the default route.

> **CAUTION!** Clients connecting to the appliance must use the same IP version that is configured on the port they are connecting to, so that certificates resolve. That is, all clients connecting to an IPv4 port must have an IPv4 address, and all clients connecting to an IPv6 port must have an IPv6 address.

- If you are configuring an IPv4 address, you can configure a static address, or use DHCP.

Static	lunash:> **network interface static -device** <netdevice> **-ip** <IP_address> **-netmask** <netmask> [**-gateway** <IP_address>]
DHCP	lunash:> **network interface dhcp -device** <netdevice>

- If you are configuring an IPv6 address, you can configure a static address, configure the port to obtain an IPv6 address using the Stateless Address Autoconfiguration (SLAAC) protocol, or use DHCP. To use SLAAC, you must have a SLAAC-enabled router in your network.

Static	lunash:> **network interface static -device** <netdevice> **-ip** <IP_address> **-netmask** <netmask> [**-gateway** <IP_address>] **-ipv6**
SLAAC	lunash:> **network interface slaac -device** <netdevice>
DHCP	lunash:> **network interface static -device** <netdevice> **-ipv6**

You are prompted to confirm the action. If no network cable is attached to the port you configured, the following message is displayed:

```
Warning. Unable to activate interface <netdevice> Ensure that the network cable is connected.
```

This message is informational. The interface will automatically activate when you connect a network cable to the port.

2. [Optional] If you wish to use the Port Bonding feature described above to configure **bond0** and/or **bond1** interface, you can configure it now. If one of the secondary interfaces within the bond has the default route, the bonded interface receives the default route.

> **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" on page 154.

lunash:> **network interface bonding config**

lunash:> **network interface bonding enable**

See "Luna Network HSM 7 Appliance Port Bonding" on page 152 for more information.

3. [Optional] Make any desired changes to the appliance network routing table.

Using older versions of the Luna Appliance Software, each network device can be configured with its own default route. Using Luna Network HSM 7 Appliance Software 7.3.3, **Luna Appliance Software 7.4.2**, or Luna Network HSM 7 Appliance Software 7.7.0 and newer, only one default route may be configured on the appliance. The first network route configured (either automatically using DHCP, or by specifying a valid **-gateway** option when configuring a static IP on a network device) becomes the default route. If you wish to change this default route, you must first delete the original default route. This applies if the default route has been applied on a network interface and you want to enable it on a different interface. The default route remains constant if you switch the device between static and DHCP address selection. See "Network Routing Table" on page 65 for more information, and refer to the following example procedures:

To move the default route from eth0 to eth1

a. [Optional] Display the current network settings.

lunash:> **network route show**

b. Remove the default route from **eth0**. When the default route is removed from a network device or bonding interface, the gateway is automatically dropped.

lunash:> **network route delete network** <IP_address> **-device eth0 -gateway 0.0.0.0**

c. Add the default route to **eth1**. This step is different depending on your appliance software version:

- Using one of the appliance software versions mentioned above (7.3.3, 7.4.2, 7.7.x), add the network route to an already-configured **eth1**.

  lunash:> network route add **network** <IP_address> **-device eth1 -gateway 0.0.0.0**

- Using Luna Network HSM 7 Appliance Software 7.8.0 or newer, reconfigure **eth1**.

  lunash:> network interface static **-device eth1 -ip** <ip address> **-netmask** <netmask> **-gateway** <gateway>

Now you can add manual network or host routes as required for your desired network flow.

4. [Optional] Set the appliance hostname and domain name. You can specify a simple hostname or a Fully Qualified Domain Name (FQDN) using the format <hostname.domainname>. If you supply a hostname that includes a space, all text after the space is ignored. For example, if you typed **network hostname my hsm** the system would assign a hostname of “my”. Therefore, if you want "my hsm", use "my.hsm", "my-hsm", or similar.

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.

lunash:> **network hostname** <hostname>

> **NOTE** This command replaces the **network domain** command from Luna 5/6.

You must configure your DNS server to resolve the hostname to the IP address configured on the Ethernet port of the appliance. Do this for each Ethernet port you are configuring. See your network administrator for assistance.

5. [Optional] If you wish to use the NTLS or SSH binding features described above to restrict NTLS or SSH messages to an interface (eth0, eth1, eth2, eth3, bond0, bond1, all), use the **ntls bind** or **sysconf ssh** commands. See "Binding Your NTLS or SSH Traffic to a Device" on page 90 for more information.
6. [Optional] 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 name servers to the appliance DNS table. There is one DNS table that applies to all network devices (ports) on the appliance.

   > **NOTE** The domain name settings apply to static network configurations only. If you are using DHCP, the DNS name servers configured on the DHCP server are used.

   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.

   lunash:> **network dns add nameserver** <ip_address> **-device** <net_device>

   > **NOTE** You must restart the **ntls** service (lunash:> service restart **ntls**) for DNS changes to take effect.

7. [Optional] 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 hostname.

   The search domain is added to the appliance DNS table. You can add a maximum of six search domains *totaling* no more than 256 characters.

   > **NOTE** The search domain settings apply to static network configurations only. If you are using DHCP, the DNS search domains configured on the DHCP server are used.

   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.

   lunash:> **network dns add searchdomain** <domain> **-device** <net_device>

> **NOTE** You must restart the **ntls** service (lunash:> service restart **ntls**) for DNS changes to take effect.

If you have chosen to perform setup via SSH, rather than via the direct (serial) administrative connection, then you will likely lose your network connection at this point, as you confirm the change of IP address from the default setting.

8. Display the current network settings, so you can verify that they are now correct for your environment before attempting to use them.

   lunash:> **network show**

Making Your Network Connection

After you have configured at least one of the Ethernet LAN ports on the appliance using a serial terminal connection, you can connect the configured ports to your network and begin connecting to the appliance over the network.

To make a network connection to the appliance:

1. Connect an Ethernet cable to each Ethernet port you configured on the appliance.
2. Use SSH, or an SSH application such a s PuTTY, to connect to the appliance via one of the configured ports. For example, if you set the IP address on eth0 to 123.45.67.89, you could connect from a Linux computer using the following command:

   ```
   ssh admin@123.45.67.89
   ```

3. You will be alerted that the server's host key is not cached in the registry. Examine the fingerprint and add the key to your SSH cache to allow the connection to proceed.
4. Login as **admin**, using the password you configured in "Logging In to LunaSH" on page 101.
5. Verify correctness of your network setup by pinging another server (lunash:> **network ping** <IP_address>) and having the other server ping this HSM appliance. Try pinging by IP address, if pinging by host name is not successful. If you are using DNS name servers, but you are unable to ping by host name, use lunash:> **network show** to verify the DNS name server configuration.

   > **NOTE** Some networks might be configured to reject ICMP ping requests, to prevent certain types of network attacks. In such a case, the ping command will fail, even if the HSM appliance is correctly configured. Consult with your network administrator.

6. Verify your client's network configuration by attempting to ping the HSM appliance by host name and by IP address, from the client. Repeat for each client where the client software was installed.

Network LEDs

The network LEDs glow or blink to indicate the exchange of traffic, as follows.

State Indicated	Indication
Activity status	**Green** (Blinking): Activity detected
	Off: Not active, or LAN cable has no connection
Speed range	**Orange**: 1G
	Green: 100M
	Off: 10M/No connection

When your connection is working, go to "Setting the System Date and Time" on page 76.

Setting TLS Ciphers

The Luna Network HSM 7 uses a default set of cipher suites for Transport Layer Security (TLS) communications, such as client connections, remote PED connections, etc.

If the default list is not suitable, you can modify it. The cipher suite configuration allows you to choose which of the supported cipher suite(s) the appliance can use for TLS communications, and also the preferred order for their usage.

Luna Appliance Software 7.8.3 and newer and Luna HSM Client 10.6.0 and newer (Windows and Linux)

Luna Appliance Software 7.8.3 adds support for TLS version 1.3, and expands the ability to configure cipher suites for use with NTLS, STC, and CBS (callback service for PED Client and Remote PED server).

AIX clients require Luna HSM Client 10.7.0 or newer to use TLS 1.3 ciphers.

Characteristics and behavior

TLS cipher settings are reset when the appliance is reimaged with sysconf reimage.

TLS cipher settings are preserved when the appliance is updated with package update.

TLS cipher settings are backed up and restored by sysconf config backup and sysconf config restore **-service ntls**.

TLS cipher settings are reset to default settings when sysconf config factoryreset **-service ntls** is performed.

The commands sysconf tls ciphers set and sysconf tls ciphers reset can be run by the appliance **admin** user (or a custom role that has admin access) only.

The command sysconf tls ciphers show can be run by any of appliance **admin**, **operator**, or **monitor** users.

TLS Ciphers Available to Configure

Using Luna Appliance Software 7.8.3 or newer, TLS 1.3 ciphers are added to the list of available TLS ciphers.

TLS_AES_256_GCM_SHA384	TLSv1.3
TLS_CHACHA20_POLY1305_SHA256	TLSv1.3
TLS_AES_128_GCM_SHA256	TLSv1.3
ECDHE-RSA-AES256-GCM-SHA384	TLSv1.2
DHE-RSA-AES256-GCM-SHA384	TLSv1.2

ECDHE-RSA-AES128-GCM-SHA256	TLSv1.2
DHE-RSA-AES128-GCM-SHA256	TLSv1.2
ECDHE-RSA-AES256-SHA384	TLSv1.2
DHE-RSA-AES256-SHA256	TLSv1.2
ECDHE-RSA-AES128-SHA256	TLSv1.2
DHE-RSA-AES128-SHA256	TLSv1.2
AES256-GCM-SHA384	TLSv1.2
AES128-GCM-SHA256	TLSv1.2
AES256-SHA256	TLSv1.2
AES128-SHA256	TLSv1.2

Luna Appliance Software 7.2.0 to 7.8.1 and Luna HSM Client 7.2.0 to 10.5.0

> **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.

> **NOTE** Setting some of the stronger ciphers introduces additional overhead, which might affect performance.

To configure TLS ciphers for the appliance

1. [Optional] View the list of supported ciphers in the default priority order.

   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.
```

2. Set your desired list of ciphers, with either a list or template. If you are using a template, you must first transfer the file to the **admin** files using **pscp** or **sftp**.

   lunash:> **sysconf tls ciphers set** {**-list** <cipher_list> | **-applytemplate** <file name>}

```
lunash:>sysconf tls ciphers set -list ECDHE-RSA-AES128-GCM-SHA256:kDHE:ALL

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-AES128-GCM-SHA256  TLSv1.2  Kx=ECDH  Au=RSA  Enc=AESGCM(128)  Mac=AEAD
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
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
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
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-SHA256      TLSv1.2  Kx=ECDH  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 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)
```

3. [Optional] You can restore the default cipher list at any time.

   lunash:>**sysconf tls ciphers reset**

```
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
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 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)
```

Setting the System Date and Time

You can set the date and time manually using the appliance's internal clock, or by synchronizing the appliance with a network time protocol (NTP) server. NTP provides a reliable, consistent, and accurate timing mechanism using Coordinated Universal Time (UTC), and is the recommended option for providing an accurate date and time. Accurate time is important for security auditing and troubleshooting using the logs.

New HSM

When setting up a new HSM, ensure that you set the HSM server's system date, time and time zone as appropriate for your network before generating the server certificate. The certificate becomes valid at the time of its creation, which is recorded as part of the certificate, as a GMT value. If your local time is set with an inappropriate local time zone, then the GMT time on the certificate could be incorrect by several hours. When other systems (Clients) attempt to reference your certificate, they might find that it has not yet become valid.

Setting the Time Zone

You must set the time zone before setting the date and time, regardless of whether you are manually configuring the date and time, or using NTP.

To set the time zone

Use the following command:

lunash:> **sysconf timezone set** <time_zone_code>

Time Zone codes

You can view a list of all available time zone codes using lunash:> **sysconf timezone list**. See "Setting the Time Zone" on page 79.

If a code is depicted in the list as a major name (such as a country) followed by a list of minor names (such as city names), then write the major name followed by a forward slash ("/"), followed by the minor name, for example America/Boston.

The code that you enter may not look exactly like the code displayed by lunash:> **status date** or **status zone**. For example, **status date** shows EDT (i.e. Eastern Daylight Time), but to set that you must type "EST5EDT," or "Canada/Eastern" or "America/Montreal" - a number of values produce the same setting.

HSM SO login might be required

While attempting to set the time or zone, you might encounter a message saying that you must log into the HSM first.

```
lunash:>sysconf timezone set Europe/London
This HSM has been initialized to require that the SO is logged in
prior to running this command.
Verifying that the SO is logged in...
The SO is not currently logged in.  Please login as SO and try again.
```

That message appears only if the HSM has been previously initialized with the **-authtimeconfig** option set. The work-around at this stage is to run the command **hsm init -label <yourlabeltext>** without the **-authtimeconfig** option. This way, you can perform your intended initialization out of order, and set the appliance time and zone later. We chose an order for these configuration instructions that is usually convenient and easy to understand, but having the system time set before initializing is not required. However, it is important to have the time set before you create certificates later on.

Manually Configuring the Appliance Date and Time

If the Luna Network HSM 7 has been used before, then it might have been initialized with the option **-authtimeconfig**, which requires that the HSM SO be logged in before you are allowed to set time/time zone. If that is the case, then you will need to log in with the old HSM SO credentials, or initialize the HSM first, before you can set time and time zone.

> **NOTE** Manual adjustment of the time may cause events to appear out of order. It is highly recommended that you use NTP to synchronize the appliance time.

To set the date and time

1. Verify the currently configured date, time, and time zone on the appliance, using the status date command. The command returns the current settings for date, time, and time zone. If desired, you can also use **status time** and **status zone**.

   lunash:> **status date**

   lunash:> **status time**

   lunash:> **status zone**

2. If the date, time, or time zone are incorrect for your location, change them using the following command:

   lunash:> **sysconf timezone set** <time_zone>


```
lunash:>sysconf timezone set Canada/Eastern
Timezone set to Canada/Eastern
```

lunash:> **sysconf time** <time> [<date>]

```
lunash:>sysconf time 15:54 20170427
Thu Apr 27 15:54:00 EDT 2017
```

> **NOTE** You must set the time zone before setting the time and date, otherwise the time zone change adjusts the time that you just set.

Drift correction for the system clock

If you require that your appliance's system clock be as correct as is practical, but are unable to use NTP for the most accurate timekeeping possible, use the system's clock-drift correction protocol. See "Correcting Clock Drift Manually" on page 80.

Synchronizing the Appliance With a Network Time Protocol (NTP) Server

You can optionally configure the appliance to synchronize its date and time with a network time protocol (NTP) server. NTP provides a reliable, consistent, and accurate timing mechanism for the appliance using Coordinated Universal Time (UTC), and is the recommended option for providing an accurate date and time for the appliance. The appliance automatically selects the highest stratum NTP server with which it can reliably communicate. If the appliance loses communications with an NTP server, it automatically selects the next best available server.

> **NOTE** If you wish to use Network Time Protocol (NTP), you must set the system time to within 15 minutes of the time given by the servers that you select. If the difference between NTP server time and the HSM appliance time is greater than 15 minutes, the NTP daemon ignores the servers and quits. To ensure that you are within the 15-minute window, we recommend setting the date and time by fetching it from an NTP server, using the **sysconf ntp ntpdate** command.

To configure the appliance to use NTP

To use NTP, you must add one or more NTP servers to the appliance's NTP server list, and then enable the appliance to synchronize its time to the servers.

1. If you have not already done so, configure the appliance's DNS server settings. See "Configuring IP and Network Parameters" on page 64.
2. Ensure that the correct time zone is set on the appliance:

   lunash:> **sysconf timezone show**

   If the appliance does not have the correct time zone configured, set it before continuing. See "Setting the Time Zone" on page 76.
3. You must now set the correct date and time. You can do this:
   - manually; see "Manually Configuring the Appliance Date and Time" on the previous page
   - by fetching it from an NTP server, using the command:

     lunash:> **sysconf ntp ntpdate** <NTP_server_IP_or_hostname>
4. Add one or more NTP servers to the appliance's NTP server list, using the command:

lunash:> **sysconf ntp addserver** <NTP_server_IP_or_hostname>

This command automatically starts the NTP service and enables time synchronization with the NTP server.

5. Verify the NTP status, using the command:

   lunash:> **sysconf ntp status**

```
[myLuna] 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    8    64     1     0.000    0.000   0.000
time-c.timefreq  .ACTS.      1  u    7    64     1    78.306  -55560.   0.000
=============================================================================
Associations:
=============================================================================
ind assid  status  conf reach auth  condition  last_event cnt
=============================================================
1   21859   963a   yes   yes  none  sys.peer    sys_peer   3
2   21860   9024   yes   yes  none    reject   reachable   2
=============================================================================
NTP Time:
=============================================================================
ntp_gettime() returns code 0 (OK)
time d1504c28.95777000  Wed, Apr 14 2014 12:22:00.583, (.583854),
maximum error 7951596 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 7951596 us, estimated error 0 us,
status 0x1 (PLL),
time constant 2, precision 1.000 us, tolerance 512 ppm,
=============================================================================

Command Result : 0 (Success)
```

> **NOTE** The return code "5 (ERROR)" indicates a gap between your system time and the NTP server's time. If the initial time-gap between your appliance and the server is greater than 15 minutes, the appliance gives up and never synchronizes with that server. If the initial time-gap is less than 15 minutes, the appliance synchronizes with the server, slowly, over several minutes; this ensures that there is no sudden jump in system time which would be unwelcome in your system logging.

Setting the Time Zone

In LunaSH, the **sysconf timezone** command allows you to change the current system time zone setting. The **sysconf timezone** command accepts any time zone defined in the Time Zone Database maintained by IANA

(also often referred to as zoneinfo, tzdata, or tz). You may prefer to use an offset of Greenwich Mean Time (GMT), or to set your local 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.

Note that the time zone code reported by **sysconf timezone show** is a localized abbreviation. For example, the following three commands set the time zone code to “EST” or "EDT", depending on whether Daylight Saving Time (DST) is currently in effect:

> **sysconf timezone set America/Kentucky/Louisville**

> **sysconf timezone set America/Toronto**

> **sysconf timezone set EST5EDT**

If you choose a named time zone, the system automatically adjusts for DST on the appropriate dates.

If you choose a simple time zone abbreviation (like **EST**) or GMT plus-or-minus a numeric offset (like **Etc/GMT+5**), that value is fixed, and the system does not adjust for DST. You must therefore make any appropriate time changes manually.

> **NOTE** If you choose to enter GMT plus-or-minus a numeric offset, please note that zone names beginning with "**Etc/GMT**" have their signs reversed. Zones west of GMT have a (+) sign and zones east of GMT have a (-) sign.

Examples

To set the time zone to...	Command
Eastern Standard Time	**sysconf timezone set EST**
Greenwich Mean Time -5 hours (same as EST)	**sysconf timezone set Etc/GMT+5**
Eastern Time (with automatic DST adjustments)	**sysconf timezone set EST5EDT**
Abidjan	**sysconf timezone set Africa/Abidjan**
Hong Kong	**sysconf timezone set Hongkong**
Knox, Indiana, USA	**sysconf timezone set America/Indiana/Knox**

Correcting Clock Drift Manually

All computer systems show clock drift over time - the system time gradually deviates from accurate or "true" time. For many applications, it is important that servers and clients be working to the same time standard, and that drift be prevented or corrected.

Various methods have been devised to correct drift. The simplest and most reliable way is to implement Network Time Protocol (NTP) and receive accurate time signals from a server that is dedicated to that task and maintained to a very high standard of accuracy. This is discussed in "Network Time Protocol on Luna Network HSM 7" on the next page.

Some situations might not permit maintaining a constant connection to an NTP server. Here we show an example of drift (over several days) and describe how to correct it using the appliance's **sysconf drift** local drift-correction commands.

To establish time drift and set drift correction

1. Begin drift measurement. This also sets the time. In order to establish the drift and its correction, accurate time must be used when beginning and ending drift measurement. One method is to use NTP on a different computer that has no connection to the Luna Network HSM 7.

   lunash:> sysconf drift startmeasure **-currentprecisetime** <hh:mm:ss>

   > **NOTE** The Luna Network HSM 7 appliance must run uninterrupted for several days to allow a clock drift to occur. Other testing can be done, but nothing that would potentially change the system time (no power-cycles, for example) or the exercise would need to be restarted.

   You can check the status of the drift measurement at any time to ensure it has not been interrupted:

   lunash:> sysconf drift status

2. Allow the drift measurement system to run for a minimum of 3 days before issuing the stop command. Issue the **stopmeasure** command with the current accurate time:

   lunash:> sysconf drift stopmeasure **-currentprecisetime** <hh:mm:ss>

   The drift measurement is automatically stored.

3. Initialize drift correction. It is best to do this immediately after stopping the measurement cycle, or it might be necessary to redo the measurement. This also resets the current time:

   lunash:> sysconf drift init **-currentprecisetime** <hh:mm:ss>

4. You can check the status of drift correction at any time:

   lunash:> sysconf drift status

To set the drift correction rate manually:

1. Set the drift rate (in seconds per day):

   lunash:> sysconf drift set

2. Set the current precise time and begin drift correction:

   lunash:> sysconf drift init **-currentprecisetime** <hh:mm:ss>

3. Let drift correction run for at least 3 days, and then check the time against an accurate source to ensure that the drift correction is effective:

   lunash:> status time

Network Time Protocol on Luna Network HSM 7

Network Time Protocol (NTP) corrects clock drift by synchronizing the appliance's internal clock with a reliable, consistent, and accurate time data server. This is the recommended method of keeping an accurate date and time on the appliance. Luna Network HSM 7 uses NTPv4.

NTP is available from a variety of public servers. We recommend using a more secure NTP server that supports symmetric or public-key authentication, as described in "Securing Your NTP Connection" below. Alternatively, your organization might have established its own NTP server(s). Contact your IT manager or security officer for details. For more information about NTP authentication, see "References" on page 84.

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. To make manual drift corrections, see "Correcting Clock Drift Manually" on page 80.

For command syntax, see sysconf ntp.

Connecting to a Public NTP Server

Connections to public NTP servers are unauthenticated and therefore less secure. See "Securing Your NTP Connection" below for authenticated NTP procedures.

To connect to a public NTP server

1. Ensure that NTP is enabled on the appliance.

   lunash:> sysconf ntp enable

2. Add an NTP server.

   lunash:> sysconf ntp addserver <NTPserver>

3. Check the NTP connection.

   lunash:> sysconf ntp status

> **NOTE** It can take a few minutes to synchronize the NTP server. Checking immediately might return an error.

Securing Your NTP Connection

NTPv4 supports two types of trusted authentication: symmetric or public-key (AutoKey). Both methods require access to NTP servers configured to support authentication.

> **NOTE** Security-sensitive elements of the internet have been moving to Network Time Security, due to the drawbacks of the Symmetric Key and AutoKey authentication add-ons to standard ntp. Due to the very high security demands of organizations that need and use HSMs, Luna Network HSM 7 appliances from softwere version 7.8.5 onward have adopted **nts** and discontinued autokey. If you need the older system, keep your Luna appliances at a version before 7.8.5.

Using Symmetric-Key Authentication

This method uses a shared secret held by both the NTP server and its client to establish a trusted connection.

To connect to a trusted NTP server using symmetric-key authentication

1. Obtain the necessary key material from your NTP server administrator. For security purposes, this may be obtainable through non-electronic means only.

2. Add the symmetric key information using LunaSH:

   lunash:> sysconf ntp symmetricauth key add **-id** <keyID> **-type** <keytype> **-value** <NTPkey>

3. Add the key ID from step 2 to the list of trusted keys:

   lunash:> sysconf ntp symmetricauth trustedkeys add <keyID>

4. Add the trusted NTP server, using the **-key** option to enter the key ID for that server:

   lunash:> sysconf ntp addserver <NTPserver> **-key** <keyID>

5. Check the NTP connection:

   lunash:> sysconf ntp status

Using Public-Key (AutoKey) Authentication

This method uses asymmetric keys held by the NTP server and client. An identity scheme is used to prove the identity of the NTP server.

To connect to a trusted NTP server using public-key (Autokey) authentication

1. Obtain an identity scheme from the secure NTP server (IFF, GQ, or MV key). It must be **sftp**'d to the Luna Network HSM 7 and installed:

   lunash:> sysconf ntp autokeyauth install **-idscheme** <IDscheme> **-keyfile** <filename>

2. Restart NTP:

   lunash:> service restart **ntp**

3. Generate an AutoKey and set a password:

   lunash:> sysconf ntp autokeyauth generate **-password** <password>

4. Restart NTP again:

   lunash:> service restart **ntp**

5. Add the trusted NTP server using the **-autokey** option:

   lunash:> sysconf ntp addserver <NTPserver> **-autokey**

6. Check the NTP connection:

   lunash:> sysconf ntp status

Network Time Security

Network Time Security (NTS [RFC 8915]) enhances Network Time Protocol (NTP) and uses a separate TLS connection for initial parameter and key exchange.

Using Luna Appliance Software 7.9.0 or newer, NTS is supported with the sysconf ntp ntsAuth cert commands. The functionality of NTP remains as before.

NTS functions in NTP's "Unicast Client-Server Mode". If you prefer other NTP communication methods, then consider Symmetric Key Authentication or Autokey (see the sections immediately preceding this one).

To connect to a trusted NTP server using NTS authentication

1. Generate your key pair on your NTS server, and send over

- either the root CA that signed the TLS certificates
- or the public key if using self signed certificates.

2. Add this certificate to the appliance's list of trusted certificates

   sysconf ntp ntsAuth cert add <certificate_sent_to_the_LNH>

3. Add a server with the nts authentication flag selected.

   sysconf ntp addserver <hostnameoripaddress> **-nts**

4. Verify the status of the connection with sysconf ntp status", to see connection information and authentication information.

5. [Optional] Repeat the above steps at least 1 more time to have at least 2 NTP servers with NTS authentication.

> **TIP** Generally recommended best practice is to have 3 NTP servers configured and connected, just as you would have multiple network paths for your Luna Network HSM 7 to avoid single points of failure in a production environment.

References

[1] NTP Documentation Page: http://www.ntp.org/documentation.html

[2] NTP FAQ: Authentication http://www.ntp.org/ntpfaq/NTP-s-config-adv.htm#S-CONFIG-ADV-AUTH

[3] NTP Public-Key Authentication: http://www.ntp.org/ntpfaq/NTP-s-config-adv.htm#Q-CONFIG-ADV-AUTH-AUTOKEY

[4] Autokey Identity Schemes: http://www.eecis.udel.edu/~mills/ident.html

[5] ntp-keygen tool: http://doc.ntp.org/4.2.6/keygen.html

[6] NTP Server configuration options http://doc.ntp.org/4.2.6/confopt.html

Generating the Luna Network HSM 7 Server Certificate

You must generate a new Luna Network HSM 7 server certificate before placing the HSM in service. Do not use the default certificate generated at the factory.

You can also regenerate the server certificate anytime, once the HSM is in service. If you generate a new certificate, you must update your client NTLS links to use the new certificate.

To generate a new server certificate for the Luna Network HSM 7

Use the following command in LunaSH.

lunash:> **sysconf regencert** [**-startdate** <YYYYMMDD>] [**-days** <number_of_days>]

If your security policy requires you to change your HSM server certificates periodically, include the **-days** option to place a time limit on the certificate's validity. By default, Luna Network HSM 7 server certificates are valid for 3653 days (10 years).

If you want the certificate to become valid on a specific date, include the **-startdate** option. By default, the date is set to 24 hours earlier, to ensure the certificate is valid in every time zone at the time of creation.

For example:

```
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)
```

> **NOTE** Using Luna Appliance Software 7.8.4 and newer, the options to specify **-keytype**, **-keysize**, and **-curve**, in order to direct or constrain the type and size of keys (as applicable) that are generated for the server certificate. Luna HSM Client 10.7.0 and newer includes the complementing ability to the **vtl** utility for client-side certificate generation. See "Configure NTLS and SSH Key Size and Type" below.

Configure NTLS and SSH Key Size and Type

Key size

Create NTLS keys from the Luna Network HSM 7 appliance with varying sizes using the sysconf regencert command.

Configure SSH keys (key size and curve size) using the sysconf ssh regenkeypair command.

The above key size options are available in Luna Appliance Software 7.8.4 and newer.

On the client side, configure NTLS key size with the vtl createCert andvtl createCSR commands using Luna HSM Client 10.7.0 and newer.

Key type

Configure SSH Ed25519 keys and ECC curves NIST P-256, P-384, and P-521 on the Luna Network HSM 7 appliance using the sysconf regencert command.

The sysconf sysconf ssh regenkeypair command already had the ability to generate keypairs for each type.

On the client side, configure the Ed25519 keys and ECC curves NIST P-256, P-384, and P-521 for NTLS with the vtl createCert andvtl createCSR commands with Luna HSM Client 10.7.0 and newer.

Other affected commands

Using Luna Appliance Software 7.8.4 and newer, the outputs of the commands sysconf tls ciphers show, sysconf fingerprint ssh, and ntls certificate show can show the additional sizes and types mentioned above.

Using Luna HSM Client 10.7.0 and newer, the vtl examineCert command output accommodates the above additions.

Limitations

The following limitations apply:

- Valid RSA key sizes are 2048 (default), 3072, and 4096.
- The keysize argument applies only to RSA key types.
- The length of ECC and Ed25519 keys is inherent and is not adjustable, attempting to set a size yields an error.
- ECC curve type options are NIST P-256, P-384, and P-521, as well as the secp256k1 OpenSSL curve (no NIST alias).
- The default curve is secp384r1 when using sysconf regencert
- The default curve size is 256 when using sysconf ssh regenkeypair (behaviour when restarting sshd)
- The ECC curve secp256k1 is supported only for TLS 1.2, and is not available for TLS 1.3. Additionally, ECDSA ciphers must be configured (using sysconf tls ciphers set) in order to connect to NTLS with this curve type.
- Ed25519 is not supported on AIX clients through the vtl createCert andvtl createCSR commands due to it supporting an older version of OpenSSL that does not support this keytype. OpenSSL 1.1.1+ is required for clients to use this key type through the vtl createCert/createCSR commands.
- RSA keypairs are not permitted for SSH connections, so the sysconf ssh regenkeypair command does not get the **-keysize** option.

Ciphers

With Luna Network HSM 7 appliance version 7.8.4, onward, the ECDSA ciphers supported include:

- ECDHE-ECDSA-AES256-GCM-SHA384,
- ECDHE-ECDSA-AES128-GCM-SHA256,
- ECDHE-ECDSA-AES256-SHA384,
- ECDHE-ECDSA-AES128-SHA256.

See also "Generating the Luna Network HSM 7 Server Certificate" on page 84

Examples

Creating a new server cert on Luna Network HSM 7 with ECC default curve

To create a new server cert with the default ECC curve

1. On the LNH generate/regenerate the server certificate, specifying the ECC keytype, but not specifying a particular curve.

```
[lnh93] lunash:>sysconf regenCert -keytype ecc
...


[lnh93] lunash:>service restart ntls

...


[lnh93] lunash:>service restart stc
...

Command Result : 0 (Success)
[lnh93] lunash:>ntls certificate show

NTLS Server Certificate:
    Data:
        Version: 1 (0x0)
        Serial Number: 1 (0x1)
        Signature Algorithm: ecdsa-with-SHA256
        Issuer: C = CA, ST = Ontario, O = Chrysalis-ITS, CN = " lnh93"
        Validity
            Not Before: Sep  5 18:13:40 2023 GMT
            Not After : Sep  5 18:13:40 2033 GMT
        Subject: C = CA, ST = Ontario, O = Chrysalis-ITS, CN = " lnh93"
        Subject Public Key Info:
            Public Key Algorithm: id-ecPublicKey
                Public-Key: (384 bit)
                pub:
                    04:a7:38:4e:2a:a8:b9:32:41:f9:e2:77:6e:aa:f7:
                    2c:d3:27:52:0d:26:81:d5:fe:58:17:82:06:54:de:
                    c2:1f:94:78:95:59:f8:a4:64:7d:ab:cc:16:f5:09:
                    de:b4:c5:4e:32:50:19:aa:7f:b3:23:fe:9c:f3:31:
                    97:bc:ff:cb:a3:5a:cf:52:6f:00:95:23:b9:bd:b3:
                    04:8f:57:c4:74:0c:80:24:4c:18:42:74:7e:eb:82:
                    bd:96:cd:8c:75:10:ca
                ASN1 OID: secp384r1
                NIST CURVE: P-384
    Signature Algorithm: ecdsa-with-SHA256
         30:64:02:30:07:b7:39:39:ab:53:93:fa:e8:0a:71:58:9a:ba:
         f9:dd:d4:5f:4f:f0:37:6e:4d:5f:0e:61:87:1e:8e:02:7c:98:
         94:85:f6:d8:88:bd:21:1c:df:32:83:91:f0:96:9a:e1:02:30:
         3a:ac:4f:6b:8b:25:5f:dc:f3:e7:d6:e6:39:1b:d8:14:03:cd:
         cb:c5:0a:29:0f:dc:aa:66:dc:d8:4a:15:cd:3b:08:7a:1c:29:
         ad:6f:eb:89:75:97:7c:e8:ba:7b:2c:14


Command Result : 0 (Success)
```



```
[lnh93] lunash:>
```

2. On the client, configure NTLS

```
[root@aa1239 bin]# ./lunacm
lunacm (64-bit) v10.7.0. Copyright (c) 2023 Thales Group. All rights reserved.

        Available HSMs:

        Current Slot Id: None

lunacm:>clientconfig deploy -server 192.168.141.93 -client 192.168.140.45 -partition Par1 -
password 1q@W3e$R -f -v

...


lunacm:>ccfg ls

 Server ID  Server                          Channel  HTL Required
_____________________________________________________________________

 0          192.168.141.93                   NTLS     no


Command Result : No Error
```

3. For the partition on the Luna Network HSM 7, run any command to confirm the connection with the new certificate.

Creating an Ed25519 client certificate with vtl utility

To create an Ed25519 client certificate

Assume that you wish to connect to a Luna Network HSM 7 192.168.141.93, that already has a server certificate of type Ed25519.

1. Acquire the server.pem from the Luna Network HSM 7, and add it to your client's server list.

```
[myclient]# sftp -O admin@192.168.141.93:server.pem 93.pem
admin@192.168.141.93's password:

server.pem                                                                    100% 1387
139.7KB/s   00:00

[myclient]# ./vtl a -n 192.168.141.93 -c 93.pem
vtl (64-bit) v10.7.0-235. Copyright (c) 2023 Thales Group. All rights reserved.


New server 192.168.141.93 successfully added to server list.

[myclient]# ./vtl l
vtl (64-bit) v10.7.0-235. Copyright (c) 2023 Thales Group. All rights reserved.

Server: 192.168.141.93
```

2. Create the Ed25519 client certificate, and optionally verify it

```
[myclient]# ./vtl createcert -n 192.168.140.45 -keytype ed25519
vtl (64-bit) v10.7.0-235. Copyright (c) 2023 Thales Group. All rights reserved.

Private Key created and written to:
/usr/safenet/lunaclient/cert/client/192.168.140.45Key.pem
Certificate created and written to: /usr/safenet/lunaclient/cert/client/192.168.140.45.pem
[myclient]# cd ../cert/client/
[myclient]# openssl x509 -in 192.168.140.45.pem -text -noout
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number: 0 (0x0)
        Signature Algorithm: ED25519
        Issuer: C = CA, ST = Ontario, L = Ottawa, O = My company, CN = 192.168.140.45
        Validity
            Not Before: Nov 13 22:07:00 2023 GMT
            Not After : Nov 11 22:07:00 2033 GMT
        Subject: C = CA, ST = Ontario, L = Ottawa, O = My company, CN = 192.168.140.45
        Subject Public Key Info:
            Public Key Algorithm: ED25519
                ED25519 Public-Key:
                pub:
                    4a:e0:5e:ac:48:12:b7:46:8e:82:e2:ae:f5:a4:b4:
                    89:09:ce:dd:3c:28:61:f7:43:67:36:ad:b0:6f:c4:
                    f7:3a
    Signature Algorithm: ED25519
    Signature Value:
        69:71:66:db:56:40:a9:d3:5c:99:50:d1:25:b7:de:0f:f4:63:
        70:63:4a:3e:12:f6:89:99:e4:a6:b9:5d:32:2a:5c:f1:0d:85:
        4d:3e:00:13:4f:e7:c9:db:16:37:84:04:c5:f0:06:17:82:54:
        b9:31:e2:d0:5d:79:e3:7c:33:0a
[myclient]#
```

3. Send the new client cert to the Luna Network HSM 7.

```
[myclient]# sftp -O ../cert/client/192.168.140.45.pem admin@192.168.141.93:
admin@192.168.141.93's password:

192.168.140.45.pem                                                    100%  546
625.4KB/s   00:00

[myclient]#
```

4. At the Luna Network HSM 7, register the new client and assign it to the partition.

```
[lnh93] lunash:>client register -c 192.168.140.45 -h 192.168.140.45

'client register' successful.


Command Result : 0 (Success)
[lnh93] lunash:>client assignPartition -c 192.168.140.45 -par Pri

'client assignPartition' successful.


Command Result : 0 (Success)
[lnh93] lunash:>
```

5. At the client, confirm that the Luna Network HSM 7 partition appears in the slot list.

```
[myclient]# ./lunacm
lunacm (64-bit) v10.7.0-235. Copyright (c) 2023 Thales Group. All rights reserved.

        Available HSMs:

        Slot Id ->              0
        Label ->
        Serial Number ->        1382217483709
        Model ->                LunaSA 7.8.4
        Firmware Version ->     7.8.4
        Bootloader Version ->   1.1.5
        Configuration ->        Luna User Partition With SO (PW) Key Export With Cloning
Mode
        Slot Description ->     Net Token Slot
        FM HW Status ->         FM Ready

        Current Slot Id: 0


lunacm:>ccfg ls

 Server ID  Server                          Channel  HTL Required
_____________________________________________________________________

 0          192.168.141.93                  NTLS     no


Command Result : No Error
```

Binding Your NTLS or SSH Traffic to a Device

You can configure your appliance to restrict NTLS or SSH traffic to a specific network device (or IP address for SSH traffic):

- NTLS is used to securely transport the cryptographic messages exchanged between a client and the HSM across the network. You must bind your NTLS traffic to a specific network device, a bonded network device, or all network devices.
- SSH is used to securely transport the administrative messages exchanged between LunaSH and the Luna Network HSM 7 appliance or HSM across the network. By default, SSH traffic is unrestricted. SSH binding is optional.

Binding Your NTLS Traffic

By default, the network trust link service (NTLS) is bound to all devices (0.0.0.0). To use the Luna Network HSM 7 on your network, you must bind NTLS to one of the following:

- A specific device (eth0, eth1, eth2 or eth3)
- All devices (eth0, eth1, eth2 and eth3)

> A bonded device (bond0 or bond1). See "Luna Network HSM 7 Appliance Port Bonding" on page 152 for more information.

Use lunash:> **ntls bind** to bind the service. The device you configure is not used until the following conditions are 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.

> **NOTE** When two or more of the appliance's network interfaces are configured to operate on the same subnetwork, a known Linux networking issue can result in a lost connection due to ARP flux. To avoid this, configure the network interfaces to operate on different subnetworks.

To bind your NTLS traffic to a device

Use lunash:> **ntls bind** to bind the NTLS traffic to a network device (eth0, eth1, eth2, eth3, bond0, bond1, all). You can use lunash:> **ntls show** to see the current binding.

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)
```

> **NOTE** The “Stopping ntls” operation might fail in the above example, because NTLS is not yet running on a new HSM appliance. This message can be safely ignored.

```
lunash:>ntls show

NTLS is currently bound to IP Address: "192.20.11.78" (eth0)

Command Result : 0 (Success)


lunash:>ntls bind eth1

NTLS binding set to network device eth1.
```

```
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)


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)
```

Binding Your SSH Traffic

You can optionally bind your SSH traffic a specific device (eth0, eth1, eth2, eth3, all) on the appliance or to a specific IP address. By default, SSH traffic is unrestricted.

To bind your SSH traffic to a device or IP address

Use lunash:> **sysconf ssh** to bind the SSH traffic to a device or IP address, as follows:

> To bind to a specific device, use lunash:> **sysconf ssh device** <netdevice>. For example:

```
lunash:>sysconf ssh device eth1

Success:  SSH now restricted to ethernet device eth1 (ip address 192.168.255.2).
Restarting ssh service.
Stopping sshd:                                             [  OK  ]
Starting sshd:                                             [  OK  ]

Command Result : 0 (Success)


[myluna] lunash:>sysconf ssh show

SSHD configuration:
SSHD Listen Port: 22 (Default)
SSH is restricted to ethernet device eth1 (ip address 192.168.255.2).
Password   authentication is enabled
Public key authentication is enabled


Command Result : 0 (Success)
```

> To bind to an IP address or host name, use lunash:> **sysconf ssh ip** <IP_address>. For example:

```
lunash:>sysconf ssh ip 192.20.10.200

Success:  SSH now restricted to ethernet device eth0 (ip address 192.20.10.200).
Restarting ssh service.
Stopping sshd:                                 [  OK  ]
Starting sshd:                                 [  OK  ]

Command Result : 0 (Success)
```

Configuring RADIUS Authentication

RADIUS (Remote Authentication Dial-In User Service) is a client/server protocol providing authentication, authorization, and accounting service to configured clients. The client passes user information to configured, designated RADIUS servers, and acts on the returned response. A RADIUS server receives user connection requests, authenticates the user if that user's profile exists on the server, and then returns the configuration information according to which the client can deliver service to the user.

While a proposal is being considered (by the custodians of the RADIUS standard) to switch to TLS communication protocol, RADIUS interaction currently takes place over UDP (User Datagram Protocol).

RADIUS Configuration Summary

Configuration and identification must take place at both ends of the RADIUS transaction. These actions include:

On the RADIUS Server Side

> Identify the client systems from which this server will accept requests and return service (this is recorded in the RADIUS server's configuration file).

> Identify the users who will be covered by the service.

On the RADIUS Client Side (your Luna Network HSM 7)

> Enable RADIUS.

> Add a RADIUS server, specifying its IP address, and providing the access secret for that server.

> Check the status of Luna Network HSM 7 appliance users.

> Add desired Luna Network HSM 7 appliance users to the RADIUS list, enabling RADIUS authentication for those users.

> Verify that RADIUS is enabled for any user on your Luna Network HSM 7 that needs to use RADIUS.

Configuring RADIUS with Your Luna Network HSM 7 Appliance

Follow these steps on the RADIUS Server:
You can use any standards-compliant RADIUS server, either a commercial server or one of the free/open-source servers, like freeRADIUS or openRADIUS.

1. Add the client to the RADIUS server's configuration file, specifying:
   - The address of the Luna Network HSM 7 appliance.
   - The secret or password that the client will use when connecting.
   - A short, user-friendly or business-relevant name for the client.

You can edit the file directly, for some RADIUS implementations, or use the provided interface.

```
/etc/raddb/clients.conf:

client 192.20.17.174 {
        ipaddr          = 192.20.17.174
        secret          = testing123
        nas             = other
        shortname       = sa174
}
client 192.20.22.106 {
        ipaddr          = 192.20.22.106
        secret          = testing321
        nas             = other
        shortname       = sa22106
}
```

2. For each client, add the user name and the password for that user to the "users" file of the RADIUS server.

```
/etc/raddb/users:

sauser162       Cleartext-Password := "userpw654"
sauser171       Cleartext-Password := "userpw987"
sauser172       Cleartext-Password := "userpw789"
sauser173       Cleartext-Password := "userpw456"
sauser174       Cleartext-Password := "userpw321"
nagios          Cleartext-Password := "nagiospw"
audit           Cleartext-Password := "myuserpin"
someguy         Cleartext-Password := "userpw"
sauser106       Cleartext-Password := "userpw123"
```

A user can use RADIUS for a Luna Network HSM 7, only if that appliance is registered as a client, and if that user is registered as a user in the appropriate files on the RADIUS server.

Follow these steps on the Luna Network HSM 7 appliance:

> **NOTE** Without RADIUS, use lunash:> **user add -username** <name> to add an appliance administrative user on Luna Network HSM 7. With RADIUS, use the command lunash:> **user radiusadd -username** <name> to both create the user on the appliance and add that user to the RADIUS list. You cannot use lunash:> **user radiusadd** to convert an existing user from non-RADIUS to RADIUS.

1. On the Luna Network HSM 7 appliance, enable RADIUS with lunash:> **sysconf radius addserver**.
2. Add the server (by hostname or IP address), specifying the port to use, and the timeout value in seconds.

```
[1722022106] lunash:>sysconf radius add -s 192.20.15.182 -p 1812 -t 60

Enter the server secret:
Re-enter the server secret:
Command Result : 0 (Success)
```

3. Verify that the desired server has been added.

```
[1722022106] 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)
```

4. Check the user list to see which users exist, are enabled on the appliance, and are RADIUS enabled.

```
[1722022106] lunash:>user list

                  Users       Roles      Status      RADIUS
    --------------------    --------    --------    --------
                  admin       admin     enabled          no
                  audit       audit     enabled          no
                monitor     monitor    disabled          no
               operator    operator    disabled          no

Command Result : 0 (Success)
```

5. Add a user, by name, as a RADIUS user.

```
[1722022106] lunash:>user radiusAdd -u someguy

Creating mailbox file: File exists
Stopping sshd:                                             [  OK  ]
Starting sshd:                                             [  OK  ]

Command Result : 0 (Success)
```

6. Add the user's appliance role (in this example, we are giving him **admin**-level access).

```
[1722022106] lunash:>user role add -u someguy -r admin

User someguy was successfully modified.

Command Result : 0 (Success)
```

7. Verify that the user exists, has the correct role on the appliance, and is a RADIUS user for this appliance.

```
[1722022106] lunash:>user list

                  Users       Roles      Status      RADIUS
    --------------------    --------    --------    --------
                  admin       admin     enabled          no
                  audit       audit     enabled          no
                someguy       admin     enabled         yes
                monitor     monitor    disabled          no
               operator    operator    disabled          no

Command Result : 0 (Success)
```

CHAPTER 4: Appliance Users and Roles

TIP This page concerns authentication and management of roles that govern *network administrative access **to the appliance***.

That is, access, management, and use of the cryptographic module and its application partitions, are distinct from access to the physical platform (and operating system) in which the HSM resides. This is true:

- for Luna PCIe HSM 7 installed in a workstation that you provide, and
- for the same cryptographic module inside a Luna Network HSM 7 appliance with hardened operating system and administrative access restricted to the limited Luna shell command set.

On the appliance, the cryptographic module has its own separate and distinct authentication roles and requirements; see hsm init , hsm login, and partition init, partition init co, partition init cu, partition createchallenge, partition changepw, partition activate, and audit changepwd, audit login among the various other administrative operations on the SSH-accessible appliance command path, or via the equivalent REST APIs, as well as the client-side equivalent commands (in LunaCM) partition init, partition login, partition logout, and all the partition role commands.

The security of an HSM and its cryptographic contents depends on well-controlled access to that HSM. A controlled access policy is defined by:

- the set of users with valid login credentials for the appliance, the HSM and the application partition
- the actions each user is allowed to perform when logged in (the user's role)

For example, an access policy that adheres to the PKCS#11 standard requires two roles: the security officer (SO), who administers the user account(s), and the standard user, who performs cryptographic operations. When a user logs in to the HSM, they can perform only those functions that are permitted for their role.

Configuration and maintenance tasks on the Luna Network HSM 7 appliance (including network setup, file management, and system monitoring) are completed by executing commands in the LunaSH command line interface.

When you log in to LunaSH via SSH or a serial connection, the set of available commands depends on the role assigned to your user account. Appliance roles are defined by their associated command privileges. Clear separation of duties is beneficial to a secure production environment and allows you to easily delegate responsibilities according to your organization's needs. For optimal security, assign each user the lowest-level role necessary to fulfill their responsibilities.

Managing Appliance Users and Roles

Refer to the following procedures to manage appliance roles:

Default Appliance Users and Roles

The default Luna Network HSM 7 appliance user accounts are named after their respective default roles. You cannot delete the default user accounts. For a comprehensive list of the LunaSH commands available to the default roles, see LunaSH Command Summary.

By default, only the **admin** and **recover** user accounts are active. The default password for all accounts is "PASSWORD" (see "Logging In to LunaSH" on page 101).

admin

The **admin** user is the highest-level default user account. This user (or a custom user assigned an **admin** role) has access to the full set of LunaSH commands (except some specialized **audit** commands) and can perform all configuration and maintenance tasks on the Luna Network HSM 7 appliance. Users with an **admin** role can also activate or deactivate the other default user accounts, reset their passwords to default, and create custom user accounts and roles.

The **admin** role is required to access LunaSH commands for configuring and maintaining the HSM within the appliance, so the HSM Security Officer must be assigned an **admin** role to fulfill all HSM SO responsibilities (see HSM Security Officer (SO)).

operator

The **operator** user is a limited-access default user account that can perform most configuration and maintenance tasks on the Luna Network HSM 7 appliance. For example, the **operator** cannot perform the following procedures:

- activating or deactivating other roles on the appliance or resetting passwords
- backup/restore of the LunaSH user configuration
- regenerating the NTLS certificate on the appliance
- setting TLS ciphers

This user (or a custom user assigned an **operator** role) cannot access HSM configuration commands. While it is possible for a user with an **operator** role to log in to the HSM using the HSM SO credential, many of the commands required by the HSM SO are inaccessible. It is therefore not recommended to assign an **operator** role to the HSM SO.

The **operator** user account must be activated by an **admin** user before it can log in to LunaSH (see "Enabling/Disabling Appliance User Accounts" on page 103).

monitor

The **monitor** user is an information-only default user account that can observe the appliance and HSM status. This user (or a custom user assigned a **monitor** role) has access to only those LunaSH commands that present information about the Luna Network HSM 7, including current HSM policies, created partitions, registered clients, and appliance settings. The **monitor** role cannot affect the appliance or HSM in any way.

The **monitor** user account must be activated by an **admin** user before it can log in to LunaSH (see "Enabling/Disabling Appliance User Accounts" on page 103).

audit

The **audit** user is the account used by the HSM Auditor to log in to the appliance and access the HSM audit logging functions. This user (or a custom user assigned an **audit** role) has access to a unique subset of commands that configure audit logging, as well as some informational commands, and commands to manage the **audit** user's account and files. The Auditor credential is required for some commands, and therefore the Auditor must be assigned an **audit** role on the appliance to fulfill all Auditor responsibilities (see Auditor (AU)).

The **audit** user account must be activated by an **admin** user before it can log in to LunaSH (see "Enabling/Disabling Appliance User Accounts" on page 103).

recover

The **recover** user account's only function is to reset the password for the **admin** user. This account cannot access any LunaSH commands, and there is no **recover** role that can be assigned to a custom user. The **recover** account cannot be locked out, and its default password does not expire.

As a security measure, **recover** can log in via the local serial connection only. The **admin** user's account password can be changed remotely by anyone who already knows it, but the **admin** user's password cannot be arbitrarily reset unless the person doing so has physical access to the appliance, to make the serial connection. See "Recovering the Admin Account Password" on page 124.

Custom Appliance Users and Roles

If the default set of users and roles do not conform to your organization's specific security profile, you can customize the user configuration on your Luna Network HSM 7 appliance to fit your needs. This system of users and roles gives you complete control over how your Luna Network HSM 7 is accessed.

Custom User Accounts

LunaSH allows you to create custom, named user accounts. These users are assigned one of the default appliance roles, or a custom role that you create. For example, the following user configuration options are available:

- Multiple **admin**-level users, each with a different name
- Multiple **operator**-level users (or none), each with a different name
- Multiple **monitor**-level users (or none), each with a different name
- Multiple **audit**-level users (or none), each with a different name
- Multiple custom users, each with a different name, with custom roles defined by the users' responsibilities

Named user accounts can be useful in distinguishing the actions of different people in the logs. For example, a user named **john** executing the command **syslog tail** in LunaSH would appear in the April 13 log as:

```
Apr 13 14:17:15 172 -lunash: Command: syslog tail  : john : 192.20.10.133/3107
```

If you have personnel performing similar functions at physically separate locations, or assigned to teams or shifts for 24-hour coverage, it could be useful (or required by your security auditors) be able to show which specific person performed which actions on the system.

See "Creating Custom Appliance User Accounts" on page 116.

Custom Roles

You can also create custom roles with access to a specified subset of LunaSH commands. This allows you to delegate specific tasks to personnel according to your organization's security structure. Like the default roles, a custom role is defined by the commands it can access in LunaSH. When a custom role is assigned to any existing user, that user can see and use only those commands associated with the role. This ensures that a given user does not obtain access beyond their security clearance. The **admin** user can create custom roles, assign them to users, or revoke them as required.

See "Creating Custom Appliance Roles" on page 117.

> **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.)

Security of LunaSH User Accounts

In most cases anticipated by the design and target markets for Luna Network HSM 7, both the Luna Network HSM 7 appliance and any computers that make network connections for administrative purposes would reside inside your organization's secure premises, behind well-maintained firewalls. Site-to-site connections would be undertaken via VPN. Therefore, attacks on the shell account(s) would normally not be an issue.

However, if your application requires placing the Luna Network HSM 7 appliance in an exposed position (e.g., in a cloud implementation), your shell account(s) may be vulnerable to attackers. It is your responsibility to protect your sensitive data.

Some recommendations for enhancing your security include using strong passwords, changing the SSH port number from its default, or using certificate-based authentication.

Logging In to LunaSH

TIP This page concerns authentication and management of roles that govern *network administrative access **to the appliance***.

That is, access, management, and use of the cryptographic module and its application partitions, are distinct from access to the physical platform (and operating system) in which the HSM resides. This is true:

- for Luna PCIe HSM 7 installed in a workstation that you provide, and
- for the same cryptographic module inside a Luna Network HSM 7 appliance with hardened operating system and administrative access restricted to the limited Luna shell command set.

On the appliance, the cryptographic module has its own separate and distinct authentication roles and requirements; see hsm init , hsm login, and partition init, partition init co, partition init cu, partition createchallenge, partition changepw, partition activate, and audit changepwd, audit login among the various other administrative operations on the SSH-accessible appliance command path, or via the equivalent REST APIs, as well as the client-side equivalent commands (in LunaCM) partition init, partition login, partition logout, and all the partition role commands.

When you open a connection to the Luna Network HSM 7 appliance (serial or SSH) you are presented with the **login as:** prompt. By default, only the **admin** user is enabled; the other roles must be enabled by an **admin** user before they can log in (see "Enabling/Disabling Appliance User Accounts" on page 103). After entering the user name and password, you are presented with the **lunash:>** prompt.

To log in to LunaSH on the Luna Network HSM 7 appliance

1. At the **login as:** prompt, enter the name of the account you want to use (**admin**, **operator**, **monitor**, **audit**, or a custom user account) and press **ENTER**.

   You are prompted for the password.

2. Enter the account password and press **ENTER**. If you are logging in to this account for the first time, the initial password is “PASSWORD” (uppercase).

   NOTE You must log in within two minutes of opening an administration session, or the connection will time out. The username and passwords are case-sensitive.

3. For security, you are immediately prompted to change the factory-default 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): `!@#$%^&*()-_=+[]{}\|/;:'",.<>?`~`

> **NOTE** If you forget the password to any account, an **admin**-level user can set a new password for you (see "Changing Appliance User Passwords" on page 104).
>
> If you forget the **admin** password, and no other **admin**-level accounts are available, you can use a local serial connection to log in to the **recover** account (see "Recovering the Admin Account Password" on page 124).

After successful login, the HSM appliance presents a **lunash:>** prompt. Type **?** or **help** and press **Enter** for a summary of the main commands. Type **?** followed by any of the commands, with or without parameters, and press **Enter** to see a summary of sub-commands and parameters for that command.

> **NOTE** If you are using Luna Network HSM 7 Appliance Software 7.7.1 or newer, SSH sessions timeout after 30 minutes of inactivity.

Failed Appliance Login Attempts

The response to failed login attempts is the same for **admin**, **operator**, **monitor**, **audit**, and any named users you have created, and is limited by default SSH settings:

- If you initiate an SSH session against the appliance, and fail to respond to the prompts, the session expires after 120 seconds. You must restart or launch a new session in your SSH terminal tool.
- If you initiate an SSH session against the appliance, provide a user name, and then provide an incorrect password, the session prompts you to re-attempt the correct password for that user account. If you fail to provide the correct authentication six (6) times*, the session is dropped. You must restart or launch a new session in your SSH terminal tool.

The maximum number of simultaneous sessions per channel is the SSH default of 10. These factors help to limit the pace of brute-force attacks, while still allowing timely recovery from mistyping or forgetfulness by an administrative user.

You can configure Luna Network HSM 7 to accept administrative connections (SSH) on only one Ethernet LAN port, and client (NTLS) connections on another.

*** Luna Network HSM 7 Appliance Might Allow Fewer Than Six Bad Logins**

Your appliance uses the default SSH setting for MaxAuthTries of six attempts; it will not allow more bad attempts. Two conditions can affect the number of tries that are permitted:

- The client with which you are connecting, can have a different number. If the client's MaxAuthTries number is greater, the appliance prevails and stops at six attempts. If the client's MaxAuthTries is lower, the client prevails.
- The client might have a preference set for public key authentication. If the appliance and client are unable to establish a public-key authenticated connection, then that attempt *silently* fails, and further attempts to authenticate with a bad password are halted after MaxAuthTries-1 (according to whichever party has the lower setting for bad login attempts).

Failed Logins Reported on New Luna Network HSM 7 Appliance

Upon first login to the Luna Network HSM 7 appliance, you might see a system message like the following:

```
Last failed login: Wed Jan 02 14:25:11 EDT 2019 from 192.168.10.105 on ssh:notty
There were 2 failed login attempts since the last successful login.
Last login: Wed Jan 02 14:15:09 from 192.168.10.105
```

This is expected. The manufacturing process uses a temporary password, then resets the default password and verifies that the temporary password is no longer valid. This accounts for the "failed login attempts".

Enabling/Disabling Appliance User Accounts

> **TIP** This page concerns authentication and management of roles that govern *network administrative access **to the appliance***.
>
> That is, access, management, and use of the cryptographic module and its application partitions, are distinct from access to the physical platform (and operating system) in which the HSM resides. This is true:
>
> - for Luna PCIe HSM 7 installed in a workstation that you provide, and
> - for the same cryptographic module inside a Luna Network HSM 7 appliance with hardened operating system and administrative access restricted to the limited Luna shell command set.
>
> On the appliance, the cryptographic module has its own separate and distinct authentication roles and requirements; see hsm init , hsm login, and partition init, partition init co, partition init cu, partition createchallenge, partition changepw, partition activate, and audit changepwd, audit login among the various other administrative operations on the SSH-accessible appliance command path, or via the equivalent REST APIs, as well as the client-side equivalent commands (in LunaCM) partition init, partition login, partition logout, and all the partition role commands.

By default, **admin** is the only active user account on the Luna Network HSM 7 appliance. The other default accounts (**operator**, **monitor**, **audit**) exist and cannot be deleted. The **admin** account (or a custom user account with an **admin** role) must first enable them using the procedure below.

To enable a default appliance user account

1. Connect to the appliance via SSH or a serial connection, and log in to LunaSH as **admin** or a custom user with an **admin** role (see "Logging In to LunaSH" on page 101).
2. Enable the desired account.

   lunash:> **user enable -username** <account_name>

   The user of this account can now log in to LunaSH with the account name and default password "PASSWORD". See "Logging In to LunaSH" on page 101.

To disable any appliance user account

1. Connect to the appliance via SSH or a serial connection, and log in to LunaSH as **admin** or a custom user with an **admin** role (see "Logging In to LunaSH" on page 101).
2. Disable the desired account.

   lunash:> **user disable -username** <username>

Changing Appliance User Passwords

> **TIP** This page concerns authentication and management of roles that govern *network administrative access **to the appliance***.
>
> That is, access, management, and use of the cryptographic module and its application partitions, are distinct from access to the physical platform (and operating system) in which the HSM resides. This is true:
>
> - for Luna PCIe HSM 7 installed in a workstation that you provide, and
> - for the same cryptographic module inside a Luna Network HSM 7 appliance with hardened operating system and administrative access restricted to the limited Luna shell command set.
>
> On the appliance, the cryptographic module has its own separate and distinct authentication roles and requirements; see hsm init , hsm login, and partition init, partition init co, partition init cu, partition createchallenge, partition changepw, partition activate, and audit changepwd, audit login among the various other administrative operations on the SSH-accessible appliance command path, or via the equivalent REST APIs, as well as the client-side equivalent commands (in LunaCM) partition init, partition login, partition logout, and all the partition role commands.

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)

Individual users can change the password for their own account at any time. The **admin** or users with **admin** privileges may change the password for other accounts, including other **admin**-level accounts.

Password Guidelines

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

For more information, see "Name, Label, and Password Requirements" on page 125.

In addition, see "Manage Appliance User Passwords" on the next page for configuration of password length password history, password expiry, as well as the handling of bad login attempts.

To change your own appliance user password

1. Connect to the appliance via SSH or a serial connection, and log in to LunaSH using your username and password (see "Logging In to LunaSH" on page 101).
2. Change your user password.

   lunash:> **my password set**

To change the password for a different user

1. Connect to the appliance via SSH or a serial connection, and log in to LunaSH as **admin** or a custom user with an **admin** role (see "Logging In to LunaSH" on page 101).
2. Change the password for a specified user.

   lunash:> **user password** <username>

> **NOTE** **admin**-level users can also use this command to change their own password.

Manage Appliance User Passwords

> **TIP** This page concerns authentication and management of roles that govern *network administrative access **to the appliance***.
>
> That is, access, management, and use of the cryptographic module and its application partitions, are distinct from access to the physical platform (and operating system) in which the HSM resides. This is true:
>
> - for Luna PCIe HSM 7 installed in a workstation that you provide, and
> - for the same cryptographic module inside a Luna Network HSM 7 appliance with hardened operating system and administrative access restricted to the limited Luna shell command set.
>
> On the appliance, the cryptographic module has its own separate and distinct authentication roles and requirements; see hsm init , hsm login, and partition init, partition init co, partition init cu, partition createchallenge, partition changepw, partition activate, and audit changepwd, audit login among the various other administrative operations on the SSH-accessible appliance command path, or via the equivalent REST APIs, as well as the client-side equivalent commands (in LunaCM) partition init, partition login, partition logout, and all the partition role commands.

Configuring appliance user password parameters and behavior

Luna Appliance Software 7.9.0 and newer includes enhanced password management and configuration for administrative roles on the Luna Network HSM 7 appliance. You can now configure:

- password length constraints
- the number of previous passwords that are remembered and not permitted to re-use (password history)
- the lifetime of a user password (expiry)
- handling of bad login 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

- If you reimage the appliance to an earlier version, these appliance-user password-management commands and operations will no longer exist; nor will their effects on users' passwords and handling.

  Firmware rollback and firmware upgrade would have no effect, because the HSM (the cryptographic module) and its firmware are not involved in appliance-level (the host machine) user accounts.
- The appliance user password configuration settings described here **are not preserved** by the sysconf config backup and sysconf config export and sysconf config restore operations.

Password history

You can optionally set a password history for users of the appliance, such that:

- the minimum number of passwords that are remembered (and forbidden to reuse) is one(1), while
- the maximum remembered passwords for the appliance is ten (10), and
- the default is four (4).

If the history option is disabled, then no previous passwords are excluded at password change, meaning that a user can continue [re-]using the same password indefinitely.

Setting a default (4) password history

To set a default number of passwords for the appliance to exclude, next time users change their passwords, do the following:

1. Run the sysconf user password history command *without* a number.

```
lunash:>sysconf user sh

Password policies:
==================
History : disabled
Expire after : disabled
Minimum length : 8 characters
Login policy : disabled

Command Result : 0 (Success)
[localhost] lunash:>sysconf user password history

Password history set to 4 successfully.

Command Result : 0 (Success)
```

2. [Optional] view the new setting.

```
lunash:>sysconf user sh

Password policies:
==================
History : 4
```

```
Expire after : disabled
Minimum length : 8 characters
Login policy : disabled


Command Result : 0 (Success)
```

3. [Optional] Verify by performing some password changes.

```
[localhost] lunash:>user password

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 the following 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)
[localhost] lunash:>
:
:<another change>
:
:<another change>
:
[localhost] lunash:>user password

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 the following 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)
```

The current user has now accumulated at least 4 prior passwords that should be forbidden to reuse.

4. Try a password change, reusing any of the most recent 4 passwords.

```
lunash:>user password

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 the following 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:
Password has been already used. Choose another.
passwd: Have exhausted maximum number of retries for service

Failed to set password.

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

Any password that has been used in the past 'n' password changes (in this case the default 4 prior passwords) is rejected.

5. Then try with a unique password, or a password that is older than the number remembered by the history.

```
lunash:>user password

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 the following 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)
```

A unique password, or a password that was used before the most recent (in this example, 4) is accepted.

Setting a specific password history

To set a desired number of passwords for the appliance to exclude, when appliance users change their passwords, do the following:

1. Run the sysconf user password history command with a number.

```
lunash:>sysconf user show

Password policies:
==================
History : disabled
Expire after : disabled
Minimum length : 8 characters
Login policy : disabled

Command Result : 0 (Success)
```

```
[localhost] lunash:>sysconf user password history 6

Password history set to 6 successfully.

Command Result : 0 (Success)
```

2. [Optional] view the new setting.

```
lunash:>sysconf user show

Password policies:
==========
History : 6
Expire after : disabled
Minimum length : 8 characters
Login policy : disabled

Command Result : 0 (Success)
```

Password length

You can optionally set a minimum password length for users of the appliance, such that:

- the **minimum** number of characters allowed in passwords can be set between eight (8) and thirty (30)
- the default is eight (8).

Setting a specific minimum permitted password length

To set a desired minimum number of characters permitted in any new appliance user passwords, do the following:

1. Run the sysconf user password length command with a number.

```
lunash:>sysconf user show

Password policies:
==========
History : disabled
Expire after : disabled
Minimum length : 8 characters
Login policy : disabled

Command Result : 0 (Success)


lunash:>sysconf user password length 15

Minimum password length set to 15 characters

Command Result : 0 (Success)
```

2. [Optional] view the new setting.

```
lunash:>sysconf user show

Password policies:
==========
History : disabled
Expire after : disabled
```

```
Minimum length : 15 characters
Login policy : disabled

Command Result : 0 (Success)
```

Setting the default minimum password length

To set the default minimum number of characters permitted in any new appliance user passwords, do the following:

1. Run the sysconf user password length command with **no** number specified.

```
lunash:>sysconf user show

Password policies:
==================
History : disabled
Expire after : disabled
Minimum length : 15 characters
Login policy : disabled

Command Result : 0 (Success)


lunash:>sysconf user password length

Minimum password length set to 8 characters

Command Result : 0 (Success)
```

2. [Optional] view the new setting.

```
lunash:>sysconf user show

Password policies:
==================
History : disabled
Expire after : disabled
Minimum length : 8 characters
Login policy : disabled

Command Result : 0 (Success)
```

> **NOTE** For security reasons it is not possible to disable the requirement for a minimum password length.

Password expiry

After software upgrade, the password expiry option is in a "never enabled" state with a value of 99999 days.

```
lunash:>sysconf user show

Password policies:
==================
History : disabled
Expire after : 99999 days
Minimum length : 8 characters
```

```
Login policy : disabled

Command Result : 0 (Success)
```

Setting a *default* 90 day expiry period for passwords

To set a password expiry to the default value, do the following:

1. Run the command sysconf user password -expire *without* a number.

```
lunash:>sysconf user password expire

User password expiration set to 90 days successfully.

Command Result : 0 (Success)
```

2. [Optional] Verify that the 90 day value is in force.

```
lunash:>sysconf user show

Password policies:
==================
History : disabled
Expire after : 90 days
Minimum length : 8 characters
Login policy : disabled

Command Result : 0 (Success)
```

Setting a specific expiry period for passwords

To set a password expiry, do the following:

1. Run the command sysconf user password -expire with a number between 1 and 365.

```
lunash:>sysconf user password expire 30

User password expiration set to 30 days successfully.

Command Result : 0 (Success)
```

2. [Optional] Verify that the value is in force.

```
lunash:>sysconf user show

Password policies:
==================
History : disabled
Expire after : 30 days
Minimum length : 8 characters
Login policy : disabled

Command Result : 0 (Success)
```

Disabling expiry for appliance user passwords

To disable password expiry, do the following:

1. Run the command sysconf user password -expire with no number and include the **-disable** flag.

```
lunash:>sysconf user password expire -disable

User password expiration disabled.

Command Result : 0 (Success)
```

2. [Optional] Verify that expiry is disabled.

```
lunash:>sysconf user show

Password policies:
==================
History : disabled
Expire after : disabled
Minimum length : 8 characters
Login policy : disabled

Command Result : 0 (Success)
```

Bad login / failed login handling

The sysconf user login command lets you set how the appliance reacts when login attempts fail.

- An **-interval** option can be set (a number of seconds), during which bad login attempts are counted.
- A number 'n' of attempts is set with the **-attempt** option, for counting during the interval.
- The **attempt** count and the **interval** start at the first failed login attempt when no interval or lockout period is in effect.
- If 'n' failed attempts occur within the window/interval, then the account is locked out until the lockout is released (where the lockout duration is a number of seconds imposed by the **-release** option).
- A bad-login interval, in progress, has these effects:
  - If fewer than 'n' failed attempts are detected before the end of the window/interval is reached, then no lockout occurs. No action is taken and the interval and the count simply end.
  - The next failed login after the interval closes, starts a new interval and starts the failed login attempt count at one (1).
  - If a successful login occurs during a bad-login counting interval, before the configured number of bad-attempts is reached, then the interval is ended and the count is reset to zero (0).
  - If attempts simply stop (no more failed attempts *or* successful attempts), then the interval proceeds to its time-out value and ends and the count is reset to zero (0)
- The first failed attempt after a window/interval expires launches a new window/interval with the failed-attempt count incremented to one (1)
- Lockout configuration applies to all appliance users, but lockout action is specific to the user account that triggered it and does not affect other users.
- Bad login attempts during a lockout period are refused.
- Correct login attempts during a lockout period are refused.
- Ability for the affected user to log into their account on the appliance resumes after a lockout period ends.

Password example of bad-login behavior

1. Set the parameters for password handling.

```
lunash:>sysconf user login -attempts 5 -release 600 -interval 300

Restarting ssh...

Login policy set successfully.

Command Result : 0 (Success)


lunash:>sysconf user show

Password policies:
==================
History : disabled
Expire after : disabled
Minimum length : 8 characters
Deny attempts : 5
Release interval : 600 seconds
Detection window : 300 seconds

Command Result : 0 (Success)
```

2. Make five login attempts with incorrect passwords.

```
Keyboard-interactive authentication prompts from server:
| Password:
End of keyboard-interactive prompts from server
Access denied
Keyboard-interactive authentication prompts from server:
| Password:
End of keyboard-interactive prompts from server
Access denied
Keyboard-interactive authentication prompts from server:
| Password:
End of keyboard-interactive prompts from server
Access denied
Keyboard-interactive authentication prompts from server:
| Password:
End of keyboard-interactive prompts from server
Access denied
Keyboard-interactive authentication prompts from server:
| Password:

Remote side sent disconnect message
                                type 2 (protocol error):
                                                        "Too many authentication
failures"
```

Radius example of bad-login behavior

1. Start by ensuring that Radius is enabled, with a server deployed.

```
lunash:>sysconf radius show

RADIUS for SSH is enabled with the following deployed servers:

                                                  server:port     timeout
                                                -------------------------
```

```
                                          10.124.143.226:1812          30

Command Result : 0 (Success)
```

2. Verify that a suitable user exists on the appliance.

```
lunash:>user list

                  Users       Roles      Status      RADIUS
    --------------------    --------    --------    --------
                  admin       admin     enabled          no
                  audit       audit    disabled          no
                monitor     monitor    disabled          no
               operator    operator    disabled          no
                 radius     monitor     enabled         yes

Command Result : 0 (Success)
```

3. For this example, the password-related user settings start in the default conditions:

```
lunash:>sysconf user sh

Password policies:
======================
History : disabled
Expire after : disabled
Minimum length : 8 characters
Login policy : disabled

Command Result : 0 (Success)
```

Apply some configuration settings.

```
lunash:>sysconf user login -attempt 4 -release 300 -interval 600

Restarting ssh...

Login policy set successfully.

Command Result : 0 (Success)

lunash:>sysconf user show

Password policies:
====================
History : disabled
Expire after : disabled
Minimum length : 8 characters
Deny attempts : 4

Release interval : 300 seconds
Detection window : 600 seconds

Command Result : 0 (Success)
```

4. Try some bad login attempts via the Radius server

```
Keyboard-interactive authentication prompts from server:
| Password:
End of keyboard-interactive prompts from server
Access denied
Keyboard-interactive authentication prompts from server:
```

```
| Password:
End of keyboard-interactive prompts from server
Access denied
Keyboard-interactive authentication prompts from server:
| Password:
End of keyboard-interactive prompts from server
Access denied
Keyboard-interactive authentication prompts from server:
| Password:

Remote side sent disconnect message
                                type 2 (protocol error):
                                                          "Too many authentication
failures"
```

5. Attempt a correct login immediately after lockout was triggered (that is, within the set lockout period).

```
########################## Correct logins Within fail lockout
################################################


Keyboard-interactive authentication prompts from server:
|
| Too many failed login attempts have been detected.
|
| Please try again later.
| Password:
End of keyboard-interactive prompts from server
Access denied
Keyboard-interactive authentication prompts from server:
|
| Too many failed login attempts have been detected.
|
| Please try again later.
| Password:
End of keyboard-interactive prompts from server
Access denied
Keyboard-interactive authentication prompts from server:
|
| Too many failed login attempts have been detected.
|
| Please try again later.
| Password:
```

6. After the lockout window expires (3 minutes for this example), login with correct credential again becomes possible.

Creating Custom Appliance User Accounts

> **TIP** This page concerns authentication and management of roles that govern *network administrative access **to the appliance***.
>
> That is, access, management, and use of the cryptographic module and its application partitions, are distinct from access to the physical platform (and operating system) in which the HSM resides. This is true:
>
> - for Luna PCIe HSM 7 installed in a workstation that you provide, and
> - for the same cryptographic module inside a Luna Network HSM 7 appliance with hardened operating system and administrative access restricted to the limited Luna shell command set.
>
> On the appliance, the cryptographic module has its own separate and distinct authentication roles and requirements; see hsm init , hsm login, and partition init, partition init co, partition init cu, partition createchallenge, partition changepw, partition activate, and audit changepwd, audit login among the various other administrative operations on the SSH-accessible appliance command path, or via the equivalent REST APIs, as well as the client-side equivalent commands (in LunaCM) partition init, partition login, partition logout, and all the partition role commands.

LunaSH allows you to create custom, named user accounts on the Luna Network HSM 7 appliance. These users are assigned one of the standard appliance roles, or a custom role that you create (see "Creating Custom Appliance Roles" on the next page). Use this procedure to create custom user accounts.

To create a custom user account

1. Connect to the appliance via SSH or a serial connection, and log in to LunaSH as **admin** or a custom user with an **admin** role (see "Logging In to LunaSH" on page 101).
2. Create the custom user account by specifying a name.

   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.

   lunash:> **user add -username** <username>

   ```
   lunash:>user add -username james

   Stopping sshd:                                             [  OK  ]

   Starting sshd:                                             [  OK  ]


   Command Result : 0 (Success)
   ```

3. Assign a role to the new user account.

   lunash:> **user role add -username** <username> **-role** <rolename>

```
lunash:>user role add -username james -role admin

User james was successfully modified.

Command Result : 0 (Success)
```

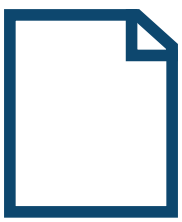
The user of this account can now log in to LunaSH with the account name and the initial password you just created for them (formerly, default password was "PASSWORD"). See "Logging In to LunaSH" on page 101.

Creating Custom Appliance Roles

> **TIP** This page concerns authentication and management of roles that govern *network administrative access **to the appliance***.
>
> That is, access, management, and use of the cryptographic module and its application partitions, are distinct from access to the physical platform (and operating system) in which the HSM resides. This is true:
>
> - for Luna PCIe HSM 7 installed in a workstation that you provide, and
> - for the same cryptographic module inside a Luna Network HSM 7 appliance with hardened operating system and administrative access restricted to the limited Luna shell command set.
>
> On the appliance, the cryptographic module has its own separate and distinct authentication roles and requirements; see hsm init , hsm login, and partition init, partition init co, partition init cu, partition createchallenge, partition changepw, partition activate, and audit changepwd, audit login among the various other administrative operations on the SSH-accessible appliance command path, or via the equivalent REST APIs, as well as the client-side equivalent commands (in LunaCM) partition init, partition login, partition logout, and all the partition role commands.

LunaSH allows you to create custom roles that can be assigned to custom users, to specify exactly which commands that user is able to access. This allows you to delegate specific tasks to personnel according to your organization's security needs. An **admin**-level user can use the following procedure to create custom roles.

See LunaSH Command Summary for a complete list of available commands. Thales recommends using the following template file to create your custom role; simply delete all commands that you want to restrict:



NOTE The template file (CustomRoleTemplate.txt), as provided here, contains multiple commands that are not available in all versions of LunaSH -- you must delete the commands that do not apply to your version of the Luna Appliance Software.

For example, the cluster and keyring commands are available only if you have installed the **lnh_cluster** package; presence of other commands depends on the HSM firmware version, and the appliance software version, being new enough to support a given command and the related functionality.

If you include commands that are not available in your installed version of LunaSH, the returned output for user role import lists the commands that prevent you from creating the role.

CustomRoleTemplate

TIP Lettercase/spelling is important when creating a role definition file. If you adjust an existing role file, to add some commands, we recommend that you do so by copy/pasting from the above template sample file, to ensure that commands you add are correct.

If your role definition file is rejected, it could be

- because you included some commands for a newer appliance software or cryptographic module firmware version that supports additional commands not supported in your appliance's or crypto module's version as installed, or
- because you included some commands for features that need separate package installation, that are not on the current appliance or its crypto module, or
- because you included some commands with typographical errors, including incorrect lettercase.

The rejection message will identify the commands that were not acceptable for any of those reasons, allowing you to correct the issue.

The following commands allow you to import, add, or remove a custom user role to your Luna Network HSM 7 appliance:

- user role import
- user role add
- user role delete

> **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.)

To create a custom appliance role and assign it to a user

1. Create a text file on your local workstation that lists each command that you want the role to be able to access (the role definition file), one command per line.

   For example, if you wanted the user **Alex** to be able to perform backup operations on your HSM but not restore operations, you would create a role definition file including partition backup and token backup commands, and not partition restore.

   > **NOTE** All lines must end with a UNIX-style linefeed (lf) character. If you create your file in Windows, be sure to convert it to use UNIX line endings before transferring it to an HSM appliance.

2. Transfer the role definition file to the appliance using **pscp** or **sftp**. You require the Luna Network HSM 7 appliance **admin** password (or an account with an **admin** role) to complete this step. The file is automatically placed in the appropriate directory on the appliance; do not specify a target directory.
3. Log into LunaSH as **admin** (or the user you specified when transferring the file).
4. Import the role definition file and specify a name for the new role.

   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.

   lunash:> **user role import -file** <filename> **-role** <rolename>

   ```
   lunash:>user role import -file backuprole -role backup

   "backuprole" was successfully imported.

   Command Result : 0 (Success)
   ```

5. Create the user account that you want to assign the role to, if it does not already exist.

   lunash:> **user add -username** <username>

6. Assign the role to the desired user.

   lunash:> **user role add -username** <username> **-role** <rolename>

Creating a One-Step NTLS Registration Role

> **TIP** This page concerns authentication and management of roles that govern *network administrative access **to the appliance***.
>
> That is, access, management, and use of the cryptographic module and its application partitions, are distinct from access to the physical platform (and operating system) in which the HSM resides. This is true:
>
> - for Luna PCIe HSM 7 installed in a workstation that you provide, and
> - for the same cryptographic module inside a Luna Network HSM 7 appliance with hardened operating system and administrative access restricted to the limited Luna shell command set.
>
> On the appliance, the cryptographic module has its own separate and distinct authentication roles and requirements; see hsm init , hsm login, and partition init, partition init co, partition init cu, partition createchallenge, partition changepw, partition activate, and audit changepwd, audit login among the various other administrative operations on the SSH-accessible appliance command path, or via the equivalent REST APIs, as well as the client-side equivalent commands (in LunaCM) partition init, partition login, partition logout, and all the partition role commands.

Creating NTLS links between a client and partition using the one-step method (see One-Step NTLS Connection Procedure) usually requires administrative access to the Luna Network HSM 7 appliance. You can set up a custom role that allows a third party to use only the commands necessary for one-step NTLS.

To create a one-step NTLS registration role

1. Create a role definition .txt file on your local workstation, listing the following commands:

```
scp
partition list
client list
client register
client assignPartition
sysconf forceSOlogin show
```

> **NOTE** All lines must end with a UNIX-style linefeed (lf) character. If you create your file in Windows, be sure to convert it to use UNIX line endings before transferring it to an HSM appliance.

   These are the commands necessary for creating one-step NTLS links. You can include any other commands for your registration purposes. See **client** for the complete set of commands.

2. Transfer the role definition file (**registerclient.txt** in the example below) to the appliance using **pscp** or **sftp**.

   pscp registerclient.txt admin@<server_host/IP>**:**

3. Log in to the appliance by SSH as the **admin** user.

4. Import the role definition file to create the **registerclient** role.

   lunash:> **user role import -file registerclient.txt -role registerclient**

5. Create the **register** user account.

lunash:> **user add -username register**

6. Assign the role to the **register** user.

   lunash:> **user role add -username register -role registerclient**

7. Open a new SSH connection to the appliance and log in as **register** with the default password "PASSWORD".

   ```
   login as: register
   register@192.168.0.123's password:
   ```

   You will be prompted to set a new password for the **register** user. This will be the password you provide to the third-party client. Ensure it is both secure and distinct from the **admin** user 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): `!@#$%^&*()-_=+[]{}\|/;:'",.<>?`~`

8. If you are using Luna Network HSM 7 Appliance Software 7.0.0, custom users do not automatically have access to the appliance's Server Certificate (**server.pem**). You must transfer the certificate from the appliance's **admin** account to the custom **register** account. This step is unnecessary if you have installed Luna Network HSM 7 Appliance Software 7.1.0 or newer.

   pscp admin@<server_host/IP>**:server.pem .**

   pscp server.pem register@<server_host/IP>**:**

9. Provide the **register** password and the partition name to the client operator. The client can now establish a one-step NTLS connection by specifying the **register** user and password in LunaCM.

   lunacm:> **clientconfig deploy -server** <server_host/IP> **-client** <client_host/IP> **-partition** <name> **-user register**

Backing Up/Restoring the Appliance User Role Configuration

TIP This page concerns authentication and management of roles that govern *network administrative access **to the appliance***.

That is, access, management, and use of the cryptographic module and its application partitions, are distinct from access to the physical platform (and operating system) in which the HSM resides. This is true:

- for Luna PCIe HSM 7 installed in a workstation that you provide, and
- for the same cryptographic module inside a Luna Network HSM 7 appliance with hardened operating system and administrative access restricted to the limited Luna shell command set.

On the appliance, the cryptographic module has its own separate and distinct authentication roles and requirements; see hsm init , hsm login, and partition init, partition init co, partition init cu, partition createchallenge, partition changepw, partition activate, and audit changepwd, audit login among the various other administrative operations on the SSH-accessible appliance command path, or via the equivalent REST APIs, as well as the client-side equivalent commands (in LunaCM) partition init, partition login, partition logout, and all the partition role commands.

LunaSH allows you to store a snapshot of the administrative user database (the names and status of all named LunaSH users) that can later be restored if desired.

CAUTION! Restoring from backup restores the database of user profiles that existed at the time the backup was made. You will lose any user accounts created since the backup; passwords of existing users could be reverted without their knowledge; enabled users might be disabled; disabled users might be enabled; and any user accounts removed since that backup will be restored.

Your records should indicate when user-profile changes were made, and what those changes were. Any time you restore a config backup, reconcile the changed statuses and inform anyone who is affected. For example, users need to know to use their previous password, and to change it immediately.

NOTE While the built-in **admin**, **operator**, and **monitor** accounts are not deleted or added by a restore operation (those accounts are permanent), both their enabled/disabled status and their passwords are changed to whatever prevailed at the time the backup was originally taken.

To back up the appliance user role configuration

1. Connect to the appliance via SSH or a serial connection, and log in to LunaSH as **admin** or a custom user with an **admin** role (see "Logging In to LunaSH" on page 101).
2. Back up the user role configuration, specifying a description for the backup file.

   lunash:> **sysconf config backup -description** <description>

   ```
   lunash:>sysconf config backup -description "Configuration Backup 17-03-01"
   ```



```
Created configuration backup file: myLuna_Config_20170301_1200.tar.gz


Command Result : 0 (Success)
```

To restore the appliance user role configuration

1. Connect to the appliance via SSH or a serial connection, and log in to LunaSH as **admin** or a custom user with an **admin** role (see "Logging In to LunaSH" on page 101).
2. List the available configuration backup files.

   lunash:> **sysconf config list**

   ```
   Configuration backup files in file system:

   Size    |  File Name                                                    |  Description
   ------------------------------------------------------------------------------------------
   ---------
   34099   |  myLuna_Config_20180507_1629.tar.gz                           |  Configuration Backup
   2018-05-07

   Command Result : 0 (Success)
   ```

3. Restore the user role configuration. If you only wish to restore the user configuration, excluding other services on the appliance, specify **-service users**.

   lunash:> **sysconf config restore -file** <filename> [**-service users**]

   ```
   lunash:>sysconf config restore -file myLuna_Config_20180507_1629.tar.gz -service users


   WARNING !! This command restores the configuration from the backup file: myLuna_Config_
   20180507_1629.tar.gz.
   It first creates a backup of the current configuration before restoring: myLuna_Config_
   20180507_1629.tar.gz.
   If you are sure that you wish to proceed, then type 'proceed', otherwise type 'quit'.

   > proceed
   Proceeding...


   Created configuration backup file: myLuna_Config_20180507_1634.tar.gz


   Restore the users configuration: Succeeded.

   You must either reboot the appliance or restart the service(s) for the changes to take
   effect.
   Please check the new configurations BEFORE rebooting or restarting the services.
   You can restore the previous configurations if the new settings are not acceptable.

   Command Result : 0 (Success)
   ```

4. Reboot the Luna Network HSM 7 appliance.

   lunash:> **sysconf appliance reboot**

Recovering the Admin Account Password

> **TIP** This page concerns authentication and management of roles that govern *network administrative access **to the appliance***.
>
> That is, access, management, and use of the cryptographic module and its application partitions, are distinct from access to the physical platform (and operating system) in which the HSM resides. This is true:
>
> - for Luna PCIe HSM 7 installed in a workstation that you provide, and
> - for the same cryptographic module inside a Luna Network HSM 7 appliance with hardened operating system and administrative access restricted to the limited Luna shell command set.
>
> On the appliance, the cryptographic module has its own separate and distinct authentication roles and requirements; see hsm init , hsm login, and partition init, partition init co, partition init cu, partition createchallenge, partition changepw, partition activate, and audit changepwd, audit login among the various other administrative operations on the SSH-accessible appliance command path, or via the equivalent REST APIs, as well as the client-side equivalent commands (in LunaCM) partition init, partition login, partition logout, and all the partition role commands.

The **recover** account is a limited-purpose account that has the permanent (fixed) password "PASSWORD". The **recover** account's only purpose is to reset the password of the **admin** user, if the **admin** password is lost/forgotten.

> **NOTE** The password recovery procedure does not affect the contents of the HSM or its application partitions. If you suspect that the **admin** account has been compromised, you can perform a factory reset of the HSM and appliance after recovery (see Resetting to Factory Condition).

As a security measure, **recover** can log in via the local serial connection only. The **admin** user's account password can be changed remotely by anyone who already knows it, but the **admin** user's password cannot be arbitrarily reset unless the person doing so has physical access to the appliance, to make the serial connection.

> **CAUTION!** The exception to this rule is where you have your appliances connected to a "terminal server" that aggregates serial links and makes them accessible via telnet or similar. This configuration is useful in a test lab, where access control is not critical, and it can be very convenient when setting up and tearing down appliances for various test and verification scenarios. However, connection of your Luna Network HSM 7 appliances to a remotely accessible terminal server could expose an additional avenue of attack, and therefore Thales recommends that you avoid allowing this potential security opening in a production environment.

The **recover** account cannot be locked out, and its default password does not expire.

To reset the admin account password

1. Connect a serial terminal to the serial console connector on the Luna Network HSM 7 rear panel.

2. Log in to LunaSH as **recover**, using the fixed password "PASSWORD".

> **NOTE** If the HSM is initialized, you are required to present the HSM Security Officer (SO) credential. Therefore, only the SO can perform this operation. If you have not initialized the HSM prior to resetting the **admin** password, then no credential is required.
>
> If you have also lost the HSM SO credential, your only alternative is to zeroize the HSM using the emergency decommission button. Refer first to Consequences of Losing PED Keys for guidelines on how to recover your partitions and cryptographic material after this action, and then to "Decommissioning the Luna Network HSM 7 Appliance" on page 190.

You are prompted to set a new **admin** password (see "Do Not Cancel Out" below).

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

If you are confident that your Luna Network HSM 7 has not been compromised, you can resume using it as before (taking care to both remember and secure the **admin** password).

Do Not Cancel Out

Use of the **recover** account sets the password of the **admin** account back to the factory value, and then forces a password change. Do not attempt to bypass the password change.

To prevent the **admin** account being accessible over the network with a known password during the recover procedure, SSH is disabled when the recover process begins. The SSH service is re-enabled only after the password is changed. Interrupting the process and avoiding the password change leaves SSH service off at boot time. If you cancel out partway through the process in order to retain the default password, instead of changing it when prompted, you might find that you no longer have SSH access.

If you encounter the problem, reconnect a local terminal and log into the **recover** account again, this time allowing it to complete the full process, ending with a proper, non-default password. If SSH service is still not available, contact Technical Support.

> **CAUTION!** During recovery, the network service is stopped and other services are affected. The minimum-effort resumption would be to reboot the system, which causes all services to restart with current configuration. However, for safety, you should consider manually restarting services from the local (serial) console, until all passwords have been changed from their default values.

Name, Label, and Password Requirements

This page describes length and character requirements for setting names, labels, domains, passwords, and challenge secrets on the Luna Network HSM 7. This information can also be found in relevant sections throughout the documentation. Refer to the applicable section below:

Custom Appliance User Accounts

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.

Custom Appliance Roles

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.

Appliance User Passwords

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

HSM Labels

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_
```


Cloning Domains

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.

Partition Names

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.

Partition Labels

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.

In LunaCM, the partition 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. The following characters are allowed:

```
abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789 !@#$%^&*()-_=+[]{}\|/;:',.<>`~
```

Spaces are allowed; enclose the label in double quotation marks if it includes spaces.

HSM/Partition Role Passwords or Challenge Secrets

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.

CHAPTER 5: System Logging

Luna Network HSM 7 gathers logs about appliance events, separate from events on the HSM itself. This chapter contains the following sections about system logging:

For HSM event logging, see Audit Logging.

About System Logging

Logs are managed with the **syslog** commands (see syslog), where you set rotation and other parameters to suit your own monitoring and management schedule. You can configure flexible logs to gather only information you consider relevant, or send different logs to different remote hosts.

> **NOTE** See Syslog Introduction for information on reading and interpreting system log messages.

Log Severity Levels

Event logs are categorized according to the severity of their impact on the system. The table "syslog Severity Levels" below defines the different categories from most to least severe. You can customize logging to include events based on their severity.

Table 1: syslog Severity Levels

Severity Keyword	Severity Description
emerg/panic	System is unusable
alert	Action must be taken immediately

Severity Keyword	Severity Description
critical	Critical condition
err/error	Error condition
warn/warning	Warning condition
notice	Normal but significant condition
info	Informational message
debug	Debug-level message

Hardware Monitoring and Logging

1. SMART technology monitors the hard disk.
2. IPMI technology monitors CPU fan speed and temperature, as well as PSU (power supply unit) voltage, fan speed and temperature.

   The system logs temperature changes of 2 degrees in either direction.

Comparing Syslog vs Audit log

> **TIP** The distinction, between an HSM (or cryptographic module) and its host, is obvious when an HSM is a circuit board/card that you install in a computer, or a USB-connected external unit. However, when an HSM card is an integral part of a network HSM appliance, it can be common usage to refer to the whole unit as "the HSM".
>
> For management of the devices it is important to differentiate between the configuration and operation of the host and the configuration and operation of the cryptographic module within, such as when addressing
>
> - the *system* logs of the host and
> - the *audit* logs of the cryptographic module.

Function or Characteristic	Syslog	Audit Log
Managed by	Managed by Luna Network HSM 7 appliance **admin user** via Luna Shell "syslog" commands.	Managed byLuna Network HSM 7 appliance **audit user** via Luna Shell "audit log" commands.

Function or Characteristic	Syslog	Audit Log
Source of log messages	Captures events in the host system, *not including* any activity within the embedded HSM/cryptographic module.	Captures events that occur inside the HSM/cryptographic module.
Control of behavior	Behavior is broadly standardized but specifics depend on the host and its operating system. See "Configuring System Logging" on page 134.	Behavior is controlled by HSM firmware, modified by configuration settings. See Audit Logging.
Location where log records are stored	Events are logged to the host file system, and can be sent to a remote logging server. Default is plain-text, but TLS encryption is a wise option.	Events are initially logged only to a dedicated space of approximately 16MB within the cryptographic module, but can be exported, in encrypted state, to the host file system, and can further be sent to a remote logging server.
	Remote logging is generally a best practice. The receiving host and port configuration must not be the same for both remote syslog and remote audit log. See syslog remotehost add and audit remotehost add.	
Security of logs	Appliance *host* logs are stored in plain text in the default log file location. They are as secure as the physical and digital access protection that you provide for the host and for any Remote Log Server you choose to use, and can be protected in transit by invoking TLS.	*Audit logs* are protected by layers of encryption where they are created and initially reside, within the cryptographic module. They are encrypted when they move from the limited storage of the cryptographic module to the host file system, and remain encrypted if forwarded to a Remote Log Server. Their integrity is assured and the audit logs can be verified and unlocked by an HSM in the same security/cloning domain as the originating cryptographic module.

Function or Characteristic	Syslog	Audit Log
Log record and file accumulation	The appliance protects itself by deleting the oldest log files when/if they are allowed to accumulate to the point of filling the allotted space (see below). This allows the most recent logs to always be available. [* Remote logging is a best practice in virtually any logging scenario.] See "Exporting System Logs" on page 137 and "Deleting System Logs" on page 138 and "Rotating System Logs" on page 134. Log rotation on the Luna Network HSM 7 appliance ensures that cleanup occurs on a daily or weekly or monthly basis. **NOTE** The space in the syslog folder in the Luna Network HSM 7 appliance is 9.7GB; if you reach or exceed that, you begin losing the oldest logs, and your syslog configuration might be in need of adjustment for log rotation and remote logging.	Audit log records accumulate in the limited space inside the HSM/cryptographic module (approximately 16MB in NVRAM) until that space approaches being full, at which time the cryptographic module *stops performing cryptographic functions and partition creation*, recording only audit log messages until the audit logs are rotated out (in encrypted form) to the host file system. Obviously, it should never be allowed to get to that state in a production environment. **NOTE** The space in NVRAM that is allocated to *audit logs* can handle in the range of a couple of hundred thousand entries. That might sound like a lot, and it is if you are prudent with audit configuration. However, see below. The space in the Luna Network HSM 7 file system for exported Audit logs is 220GB.

Function or Characteristic	Syslog	Audit Log
		Once the crypto module's audit-log space is unclogged, cryptographic operations can resume. This design strategy protects the continuity of the audit logs - the audit trail - that is so important in compliance audits and forensic investigations. See Configuring Audit Logging.

Function or Characteristic	Syslog	Audit Log
Logging best practices	*Syslog* is ubiquitous, as are compendia of best practices and advice. Confer with your organization's security and compliance teams for their requirements and wishes, regarding logging for network-connected equipment. At a minimum, consider automatic sending to a remote logging server, and invoking TLS for the transfer. Where both udp and tcp network protocols are available: • udp is faster, but can drop packets/records • tcp is slower, but verifies and resends if packets are missed or dropped. If you are in the financial industry, choose RELP for Remote Syslog, perhaps with a TLS wrapper.	For *Audit Logging*, best practice is very application dependent. For (say) a certification authority you might configure • "First Asymmetric Key Usage Only" (value "='first'), • "HSM management" (value 'manage'), • access attempts (value 'access'), and • Key management events (value 'keymanage') -- Security and Compliance auditors are likely to want to know when the key was first used, but might not need a record of every usage, which would generate a lot of audit records. But, if a record of every usage *is* a requirement, then certainly configure for it, but also configure audit log export and rotation (and remote logging*) on a schedule that keeps the audit-log corner of the cryptographic module's NVRAM from filling up with the probable high volume of audit logs. In contrast, for an application that performs *many key generations,* ongoing operation would generate huge numbers of logs, and it might be sufficient to configure the crypto module to log only failures. Generally, avoid logging all possible events; start small and increase logging scope until you achieve an acceptable balance between • coverage of cryptographic module activity and

Function or Characteristic	Syslog	Audit Log
		• performance of the of the cryptographic module (logging activity does consume or divert HSM resources). [* Remote logging is a best practice in virtually any logging scenario.]

Configuring System Logging

Logs are managed in LunaSH with the **syslog** commands. You can set rotation and other parameters to suit your own monitoring and management schedule. You can also configure flexible logs to gather only information you consider relevant, or to send different logs to different remote syslog hosts. Check the current logging configuration with lunash:> **syslog show**.

This section contains the following system logging procedures:

> "Rotating System Logs" below
> "Customizing Severity Levels" on the next page
> "Reading System Logs" on page 136
> "Exporting System Logs" on page 137
> "Deleting System Logs" on page 138

Rotating System Logs

System logs are gathered in a current log file that is periodically rotated and saved on the appliance. This allows you to easily search for logs from a specific relevant time period. You can customize the frequency of log rotation and how many rotated log files are saved. You can also rotate logs manually.

The syslog directory on the appliance will fill up over time, depending on how many old logs you choose to keep. LunaSH displays warnings when the system reaches 50%, 75%, and 90% of log capacity. If you see one of these warnings, export your old logs to a client workstation to clear space in the syslog directory.

> **NOTE** NTP logs are not included in the periodic log rotations. They accumulate in one continuous file over a long period of time (**ntp.log**). Events are infrequent enough that the NTP log file is unlikely to fill the entire log directory.

To change the frequency of log rotation

You can configure the logs to rotate daily, weekly, or monthly.

lunash:> **syslog period** <syslogperiod>

```
lunash:>syslog period daily

Log period set to daily.

Command Result : 0 (Success)
```

To change the number of rotated log files saved on the appliance

You can save up to 100 rotated log files on the appliance. This command allows you to define how long to keep old logs on the appliance (maximum: 100 logs, rotated monthly).

lunash:> **syslog rotations** <#_of_rotations>

```
lunash:> syslog rotations 5

Log rotations set to 5.

Command Result : 0 (Success)
```

To manually rotate the current log file

This command ensures that the most recent logs are included when exporting them off the appliance.

lunash:> **syslog rotate**

```
lunash:>syslog rotate

Command Result : 0 (Success)
```

Customizing Severity Levels

You can customize the logs stored on the appliance by setting the log severity level (see "Log Severity Levels" on page 128 for a description of the different levels). If you are concerned about the log directory filling up, you can configure the appliance to store only the most severe events (**emergency**) and send the rest of the logs to a remote syslog server (see "Remote System Logging" on page 138).

> **NOTE** This feature requires minimum Luna Network HSM 7 Appliance Software 7.2.0.

To customize severity levels

1. Set the severity level for the desired log type (**lunalogs**,**messages**,**cron**,**secure**,**boot**).

   lunash:> **syslog severity set -logname** <logname> **-loglevel** <loglevel>

   ```
   lunash:>syslog severity set -logname lunalogs -loglevel emergency

   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: "emergency" will be logged.
   ```

```
Stopping syslog:                                           [  OK  ]

Starting syslog:                                           [  OK  ]

Command Result : 0 (Success)
```

2. Optionally, confirm the new setting.

   lunash:> **syslog show**

```
Local Configured Log Levels:
----------------------------
lunalogs        emergency
messages        *
cron            notice
secure          *
boot            *

Note: '*' means all log levels.
```

3. Repeat Step 1, specifying the severity level of each log type you wish to customize (**lunalogs**,**messages**,**cron**,**secure**,**boot**).

Reading System Logs

You can search the current log rotation for recent events without exporting log files. Rotated logs must be exported to a client workstation to be read. For a detailed guide to reading and interpreting system log messages, see About the Syslog and SNMP Monitoring Guide.

To search the current rotation of system logs

You can search the entire current log file, specify the number of recent entries you want to see, or search for specific types of entries.

lunash:> **syslog tail -logname** <logname> **-entries** <#entries>

```
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)
```


HSM Alarm Logging

The HSM card produces logs pertaining to the card status, including alarm messages for events such as zeroization, tamper events, and changes to Secure Transport Mode. The **syslog tail** command allows you to search for this type of message in the logs.

To search the system logs for HSM alarm messages

Search for log messages containing the string "ALM".

lunash:> **syslog tail -logname messages -entries** <#entries> **-search ALM**

For example, this command will display all alarm messages from the last 200000 log entries:

```
lunash:>syslog tail -logname messages -entries 200000 -search ALM

2017 Apr 17 11:00:45 local_host kern info kernel: k7pf0: [HSM] ALM2006: HSM decommissioned by
FW
2017 Apr 17 11:00:48 local_host kern info kernel: k7pf0: [HSM] ALM2014: Auto-activation data
invalid - HSM deactivated
2017 Apr 17 11:01:12 local_host kern info kernel: k7pf0: [HSM] ALM2006: HSM decommissioned by
FW
2017 Apr 17 11:01:14 local_host kern info kernel: k7pf0: [HSM] ALM2011: HSM unlocked - tamper
clear done
2017 Apr 17 11:02:47 local_host kern info kernel: k7pf0: [HSM] ALM2007: HSM zeroized
2017 Apr 17 11:02:47 local_host kern info kernel: k7pf0: [HSM] ALM2005: HSM deactivated
2017 Apr 17 11:15:32 local_host kern info kernel: k7pf0: [HSM] ALM2013: HSM recovered from
secure transport mode

Command Result : 0 (Success)
```

Exporting System Logs

If you are managing the logs locally, you must transfer them to a client workstation in order to read them. After you have exported the log records, you can clear them from the syslog directory on the appliance.

To transfer system logs from the appliance to a client

1. Create the log archive file.

   lunash:> **syslog tarlogs**

   ```
   lunash:>syslog tarlogs

   The tar file containing logs is now available via scp as filename 'logs.tgz'.

   Command Result : 0 (Success)
   ```

2. Transfer **logs.tgz** from the appliance to a client using **pscp**/**scp**.

   >**pscp admin@**<applianceIP>**:logs.tgz .**

3. If you have configured NTP, transfer the **ntp.log** file from the appliance to a client.

   >**pscp admin@**<applianceIP>**:ntp.log .**

Deleting System Logs

Once you have exported the log files to a client, you can clear the appliance's syslog directory. This process creates an archive of all the stored logs before deleting the original files.

> **CAUTION!** Ensure that you have retrieved a copy of **ntp.log** before you run **syslog cleanup**. It is not archived with the rest of the logs.

To delete the stored system logs

lunash:> **syslog cleanup**

```
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 scp as filename "logs_cleanup_20170301_
1443.tgz".
Please copy "logs_cleanup_20170301_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)
```

Remote System Logging

Remote system logging allows you to send logs from your Luna Network HSM 7 to a central syslog server on the network.

You can use lunash:> **syslog remotehost** to specify the central syslog server.

> "Configuring a Remote Syslog Server" below

> "Customizing Remote Logging Severity Levels" on page 140

Configuring a Remote Syslog Server

Use the following procedure to configure remote system logging. Most Linux distributions include rsyslog as the standard syslog daemon. Refer to your Linux documentation for instructions that describe how to configure rsyslog on Linux.

> **NOTE** The remote server must have the appropriate port open to receive the logs (UDP port 514 by default). Refer to your operating system and firewall documentation for more information. If you need to use a different port or TCP protocol, specify it when you add the remote server's IP or hostname.

To send logs to a remote syslog server

1. Add the remote server's IP or hostname to the remote logging configuration.

   lunash:> **syslog remotehost add -host** <hostname/IP> [**-protocol** <protocol>] [**-port** <port>]

   ```
   lunash:>syslog remotehost add -host 192.10.10.101

   Stopping syslog:                                           [  OK  ]

   Starting syslog:                                           [  OK  ]

   192.10.10.101 added successfully
   Make sure the rsyslog service on 192.10.10.101 is properly configured to receive the logs

   Command Result : 0 (Success)
   ```

   By default, the remote server will now receive lunalogs, messages, secure, and boot logs at the **info** level and above, and cron logs at the **notice** level and above. See "Customizing Remote Logging Severity Levels" on the next page to specify which logs to send to which remote server.

2. On the receiving or target system, start the rsyslog daemon or service to allow it to receive logs from your Luna Network HSM 7 appliance(s).
   Refer to your receiving/logging platform's operating system documentation for more information on configuring and [re]starting the rsyslog daemon or service.

3. Optionally, confirm the remote logging settings.

   lunash:> **syslog show**

   ```
   Remote Configured Log Levels:
   -----------------------------
   lunalogs:
     192.10.10.100       info
     192.10.10.101       info
   messages:
     192.10.10.100       info
     192.10.10.101       info
   cron:
     192.10.10.100       notice
     192.10.10.101       notice
   secure:
     192.10.10.100       info
     192.10.10.101       info
   boot:
     192.10.10.100       info
     192.10.10.101       info
   ```


Customizing Remote Logging Severity Levels

There is no limit on the number of remote logging servers you can add, and you can configure the severity level for each server and log type independently (see "Log Severity Levels" on page 128 for a description of the different levels). For example, you could send all log entries produced by the appliance to one remote server, and only entries marked **critical** or higher to another server.

> **NOTE** This feature requires minimum Luna Network HSM 7 Appliance Software 7.2.0.

To customize remote logging severity

1. Set the severity level for the desired log type (**lunalogs**,**messages**,**cron**,**secure**,**boot**), specifying a remote server you already added to the configuration.

   lunash:> **syslog severity set -logname** <logname> **-loglevel** <loglevel> **-host** <hostname/IP>

   ```
   lunash:>syslog severity set -logname lunalogs -loglevel critical -host 192.10.10.101

   This command sets the severity level of lunalogs remote log messages.
   Only messages with the severity equal to or higher than the new
   log level: "critical" will be sent to 192.10.10.101.

   Stopping syslog:                                          [  OK  ]

   Starting syslog:                                          [  OK  ]

   Command Result : 0 (Success)
   ```

2. Optionally, confirm the new settings.

   lunash:> **syslog show**

   ```
   Remote Configured Log Levels:
   -----------------------------
   lunalogs:
     192.10.10.100       info
     192.10.10.101       critical
   messages:
     192.10.10.100       info
     192.10.10.101       info
   cron:
     192.10.10.100       notice
     192.10.10.101       notice
   secure:
     192.10.10.100       info
     192.10.10.101       info
   boot:
     192.10.10.100       info
     192.10.10.101       info
   ```

3. Repeat step 1, specifying each log type severity level you wish to customize (**lunalogs**,**messages**,**cron**,**secure**,**boot**).

Syslog Encryption

TLS support is added to the Luna Network HSM 7 syslog implementation, to encrypt log messages being sent to a remote server. This improves security of your logs by preventing their interception during transit. Such protection is desirable to safeguard details that could reveal the current state of the appliance.

> **NOTE** This feature requires minimum Luna Network HSM 7 Appliance Software 7.8.3.

Revised existing commands, and new commands, under syslog remotehost support

- Server authentication with self-signed certificates.
- Server authentication with CA-signed certificates.
- Mutual authentication with self-signed certificates.
- Mutual authentication with CA-signed certificates.

This feature is implemented in Luna Network HSM 7 appliance software, and does not require update of the HSM firmware, nor of the Luna HSM Client.

Caveats

The use of NTP is advised, to keep the Luna Network HSM 7 and remote syslog servers in sync.

In the initial implementation, all CA-signed server and client certificates must be signed by the same entity. That is a consideration if you are configuring multiple remote syslog servers.

> **NOTE** The Luna Network HSM 7 appliance is the client in the syslog interaction, and so the CA certificate used to encrypt communication with a remote syslog server is *not shown* when performing "client addCA" for connections from clients looking to access the HSM.

Remotehost cannot be added for the same host and the same port, using TCP and UDP at the same time.

Mulitple remote host syslog servers with CA-signed certificates can be used. For self-signed certificates, a single remote host syslog server, only is accepted.

Commands

The following commands are added under lunash:>syslog remotehost cert to support the use of TLS while connecting to remote syslog servers.

- syslog remotehost cert delete
- syslog remotehost cert deleteCA
- syslog remotehost cert gen
- syslog remotehost cert install
- syslog remotehost cert installCA

The following pre-existing commands were modified to support the use of TLS while connecting to remote syslog servers.

syslog remotehost add adds **-mode**, **-name**, and **-tls** options

Sample workflows

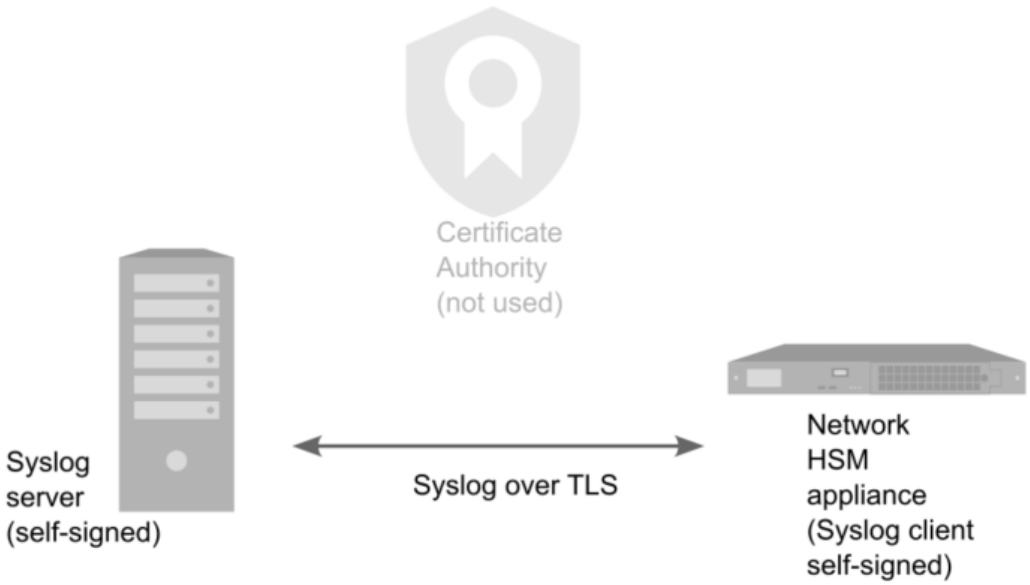
Example: Configure for Server authentication with self-signed certificates.

> The remote syslog server generates a private key and self-signed certificate.

> The remote syslog server passes the root certificate to the Luna Network HSM 7 appliance.

> Luna Network HSM 7 appliance adds this certificate to its trust store.

> User configures server information.



1. Generate a self-signed certificate on the syslog server.
2. Copy this certificate to the Luna Network HSM 7 appliance in the user space of the user, having admin or operator role, that will be handling system logging.

```
#scp -O server_self_cert.pem admin@192.168.10.93:
 admin@192.168.10.93's password:

 server_self_cert.pem                                                    100% 1318
1.2MB/s   00:00
```

3. Add the remote server configuration.

```
lunash:>syslog remotehost add -host 192.168.140.45 -protocol relp -port 514 -mode mutual -tls -
name server.rsyslog.com

       Stopping syslog:                                          [  OK  ]

       Starting syslog:                                          [  OK  ]

       192.168.140.45 added successfully
       Make sure the rsyslog service on 192.168.10.45 is properly configured to receive the logs

Command Result : 0 (Success)
[lnh93] lunash:>syslog remotehost list
```

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

        [192.168.140.45]:514, relp, tls

Command Result : 0 (Success)
```

4. Execute a lunash command and ensure that the log entry from the LNH is received on the remote server.

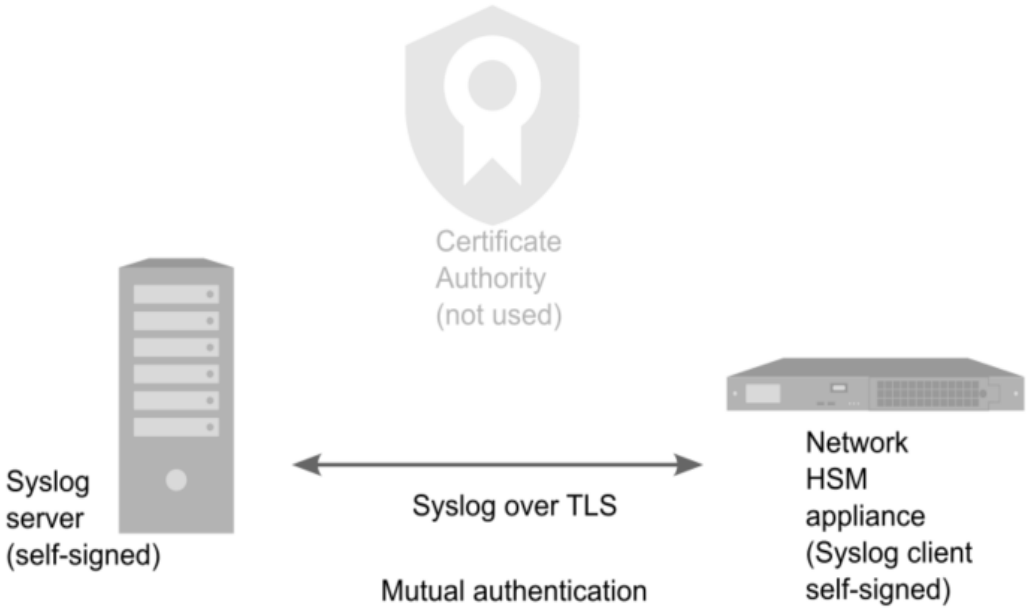
```
[lnh93] lunash:>hsm show


        Appliance Details:
        ==================
        Software Version:                   7.8.3-288


        HSM Details:
        ============
        HSM Label:                          Pri_LNH1
        Serial #:                           593658
        Bootloader:                         1.1.5
        Firmware:                           7.8.2
        HSM Model:                          Luna K7
        HSM Part Number:                    808-000073-001
        Authentication Method:              Password

:
:
 etc...

Command Result : 0 (Success)
[lnh93] lunash:>
```

... and on the server...

```
2023-07-11T12:01:40.444982-04:00 192.168.141.93 [localhost] hsm[29662]: info : 0 : Command:
hsm show  : admin : 192.168.53.104/56001
```

Remote server authentication with mutual authentication and self-signed certificates.

- The Luna Network HSM 7 appliance generates a self-signed client certificate.
- The remote syslog server retrieves the self-signed certificate from the Luna Network HSM 7 appliance.
- The remote syslog server generates a private key and self-signed certificate.
- The remote syslog server passes the root certificate to the Luna Network HSM 7 appliance.
- Luna Network HSM 7 appliance adds this certificate to its trust store.
- User configures server information.



Example: Configure a remote server with mutual authentication and self-signed certificates

1. Generate a certificate.

```
lunash:>syslog remotehost cert gen -san DNS:foo.com

                        Certificate generated successfully.

                        The syslog service needs to be (re)started before a secure connection can be

                Command Result : 0 (Success)
```

2. Import this certificate to the server and add it to the server configuration. The client certificate file is in the file area reserved to the user, having the admin or operator role, that generated it, so that user's credentials are required when the remote syslog server requests the file via scp/pscp.

   From a remote logging server

   ```
   scp admin@192.168.141.93:client_syslog.pem <localFileLocation>
   ```

   and you are prompted for the password of the named user on the Luna Network HSM 7 that created the file
   (or use pscp on Windows, with the same syntax).

   At the remote server add the client_syslog.pem file to the server configuration as appropriate to your remote syslog instance.

3. Import the server certificate and add it.

```
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)
```

4. Add the remote server configuration.

```
lunash:>syslog remotehost add -host 192.168.10.45 -protocol relp -port 514 -mode mutual -tls -
name server.rsyslog.com

       Stopping syslog:                                          [  OK  ]

       Starting syslog:                                          [  OK  ]

       192.168.140.45 added successfully
       Make sure the rsyslog service on 192.168.10.45 is properly configured to receive the logs

Command Result : 0 (Success)
[lnh93] lunash:>syslog remotehost list

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

       [192.168.140.45]:514, relp, tls

Command Result : 0 (Success)
```

5. Execute a lunash command and ensure that the log entry from the LNH is received on the remote server.

```
[lnh93] lunash:>hsm show


       Appliance Details:
       ==================
       Software Version:                  7.8.3-288


       HSM Details:
       ============
       HSM Label:                         Pri_LNH1
       Serial #:                          593658
       Bootloader:                        1.1.5
       Firmware:                          7.8.2
       HSM Model:                         Luna K7
       HSM Part Number:                   808-000073-001
       Authentication Method:             Password

:
:
 etc...

Command Result : 0 (Success)
[lnh93] lunash:>
```

... and on the server...

```
2023-07-11T12:01:40.444982-04:00 192.168.141.93 [localhost] hsm[29662]: info : 0 : Command:
hsm show  : admin : 192.168.53.104/56001
```

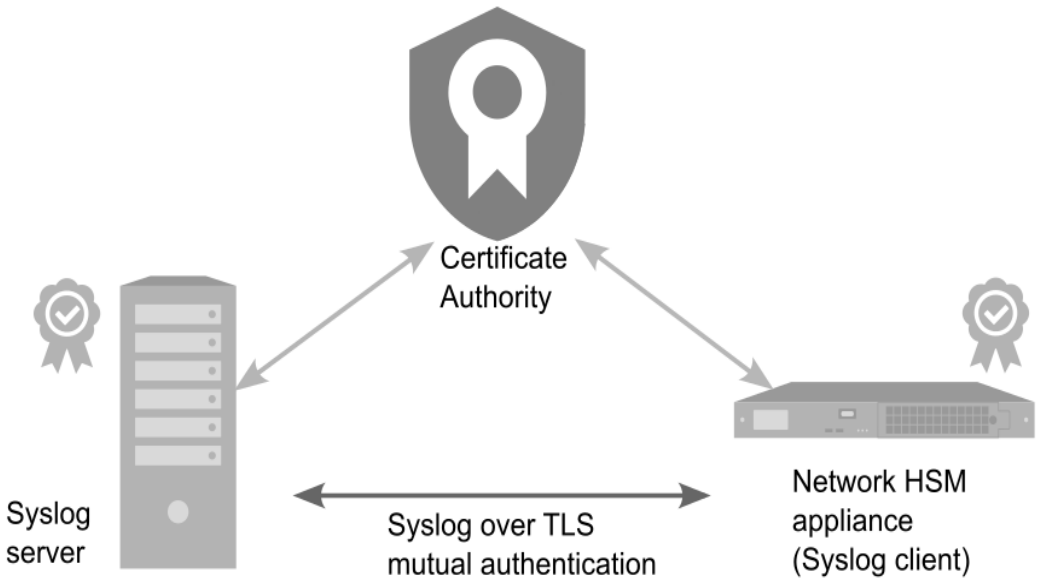
Mutual authentication with CA signed certificates.

> The remote syslog server and the Luna Network HSM 7 appliance each generate a private key and CSR.

> The remote syslog server and the Luna Network HSM 7 appliance add the received signed certificates.

> The remote syslog server and Luna Network HSM 7 appliance add the CA certificate to their trust store.

> User configures server information.



Example: Configure a remote server with mutual authentication, tcp and CA-signed certificates

1. Generate a CSR.

```
lunash:>syslog remotehost cert gen -csr
```

2. Export the CSR and sign it with the CA certificate.

3. At the CA server receive the CSR, sign the cert from the Luna Network HSM 7 appliance and return it.

```
[CAserver]# scp operator@192.168.14.93:client_syslog_csr.csr .
[CAserver]# <CAserver-side command(s) to sign the cert>
[CAserver]# scp ca.pem operator@192.168.14.93:
[CAserver]#  scp client_sign.pem operator@192.168.14.93:
```

4. Add the CA certificate to the Luna Network HSM 7 appliance.

```
lunash:>syslog remotehost cert installCA ca.pem

       Attempting to install ca.pem

       CA certificate installed successfully.
       The syslog service needs to be (re)started before a secure connection can be established.

Command Result : 0 (Success)
```

5. Import the signed client certificate to the Luna Network HSM 7 appliance and add it.

```
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)
```

6. Add the remote server configuration.

```
lunash:>syslog remotehost add -host 192.168.140.45 -protocol tcp -port 514 -mode mutual -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)
```

7. Execute a command in lunash and ensure that the log entry from the Luna Network HSM 7 appliance is received on the server.

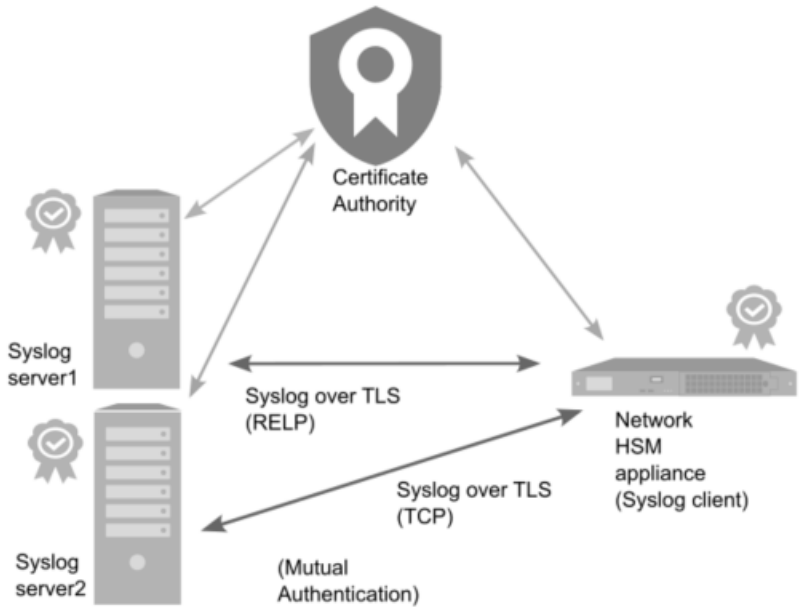
```
lunash:>syslog remotehost list

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

       [192.168.140.45]:514, tcp, tls

Command Result : 0 (Success)
```

...at the server...

```
Jun 21 14:25:37 192.168.141.93 [localhost] hsm[13889]: info : 0 : Command: syslog remotehost
list  : admin : 192.168.106.144/62166
```

Mutual authentication multiple servers, with CA signed certificates.

- The remote syslog servers each generate a private key and CSR and get the CSR signed from the CA.
- The Luna Network HSM 7 appliance generates a private key and CSR and gets the CSR signed from the CA.
- The remote syslog servers add the acquired certificate.
- Luna Network HSM 7 appliance adds the CA certificate to its trust store.
- User configures server information.



Example: Configure multiple remotehost syslog servers with mutual authentication and CA-signed certificates (all servers active)

Prerequisite

Two remote syslog servers are used in this example.

To configure a Luna Network HSM 7 appliance with two remote syslog servers

1. At the Luna Network HSM 7 (IP address 192.168.14.93 in this example), which is to be the client to the remote syslog server(s), generate a certificate and certificate signing request.

   ```
   lunash:>syslog remotehost cert gen -csr
   ```

2. At the CA server receive the CSR, sign the cert from the Luna Network HSM 7 appliance and return it.

   ```
   [CAserver]# scp operator@192.168.14.93:client_syslog_csr.csr .
   [CAserver]# <CAserver-side command(s) to sign the cert>
   [CAserver]# scp ca.pem operator@192.168.14.93:
   [CAserver]# scp client_sign.pem operator@192.168.14.93:
   ```

3. Add the CA certificate to the Luna Network HSM 7 appliance.

   ```
   lunash:>syslog remotehost cert installCA ca.pem
   ```

4. Import the signed client certificate to the Luna Network HSM 7 appliance and add it.

   ```
   lunash:>syslog remotehost cert install client_sign.pem
   ```

5. At the first remote syslog server, configure to receive logs from the Luna Network HSM 7

6. At the Luna Network HSM 7 appliance add the CA certificate, from the first remote syslog server, to the appliance's trust store.

   ```
   lunash:>syslog remotehost add -host 192.168.143.48 -protocol relp -port 514 -tls -name
   server.rsyslog.com -mode mutual
   lunash:>syslog remotehost list
   ```

```
Remote logging server(s):
=========================
 [192.168.13.48]:514, relp, tls
```

7. At the second remote syslog server, configure to receive logs from the Luna Network HSM 7
8. At the Luna Network HSM 7 appliance add the CA certificate, from the second remote syslog server, to the appliance's trust store.

```
lunash:>syslog remotehost add -host 192.168.143.45 -protocol tcp -port 514 -tls -name
server.rsyslog.com -mode mutual
```

9. At the Luna Network HSM 7 appliance run commands that can be logged to the remote syslog servers.

```
lunash:>syslog remotehost list
Remote logging server(s):
=========================
 [192.168.14.45]:514, tcp, tls
 [192.168.13.48]:514, relp, tls

Command Result : 0 (Success)

lunash:>hsm show
```

10. Verify that both remote syslog servers are working with this client Luna Network HSM 7 by checking for log entries for the commands that were just run.

Server1

```
2023-06-28T10:44:34.538875-04:00 192.168.141.93 [localhost] hsm[31002]: info : 0 : Command:
syslog remotehost list  : operator : 192.168.106.144/56917
2023-06-28T10:45:29.734290-04:00 192.168.141.93 [localhost] hsm[31002]: info : 0 : Command:
hsm show  : operator : 192.168.106.144/56917
```

Server2

```
2023-06-28T10:44:34-04:00 192.168.141.93 [localhost] hsm[31002]: info : 0 : Command: syslog
remotehost list  : operator : 192.168.106.144/56917
2023-06-28T10:45:29-04:00 192.168.141.93 [localhost] hsm[31002]: info : 0 : Command: hsm
show  : operator : 192.168.106.144/56917
```

CHAPTER 6: Client Connections

This chapter provides information about client connections to the Luna Network HSM 7 appliance. It contains the following sections:

Connections to the Appliance - Limits

Here are the considerations, for a Luna Network HSM 7 appliance, regarding client registrations and connections.

Maximum number of clients I can register against one Luna Network HSM 7 appliance
No hard limit is set.

Maximum number of clients that can connect to one Luna Network HSM 7 appliance, at the same time
Using Luna Appliance Software 7.8.5 or newer, the Luna Network HSM 7 appliance can support up to 4000 simultaneous NTLS connections. Using older versions, the limit is 800 connections.

Maximum number of connections per registered client
No hard limit is set, but see below.

Maximum number of connections, in total, to a single Luna Network HSM 7 appliance
No hard limit is set. Luna Network HSM 7 limits the number of connections according to system resources. The number of simultaneous connections that can be established with the appliance is dependent upon the various client applications.

> **TIP** If your application needs a large number of connections, there should not usually be any issue sustaining concurrent connections that have already been set up and are in-progress. However, if a network incident breaks the connections and a large number of clients attempt reconnection simultaneously, some might be in queue long enough to time out and need to retry, to achieve successful reconnection. Once connections are reestablished, clients resume their sessions in their respective registered partitions of the cryptographic module.

Luna Network HSM 7 Port Usage

The table below describes the Luna Network HSM 7 appliance's default port settings.

Standard Ports

Port	Protocol	Feature	Configurable	Session Initiation
22	TCP	Secure Shell (SSH)	Yes	inbound
123	UDP	Network Time Protocol (NTP)	No	outbound
161	UDP	Simple Network Management Protocol (SNMP) daemon	Yes	inbound
162	UDP	Simple Network Management Protocol (SNMP) trap	Yes (lunash:> **sysconf snmp notification add**)	outbound
514	UDP	Remote Syslog Service	Yes	outbound
1501	TCP	Callback Service (CBS)	No	inbound
9697	TCP	Callback Service (CBS)	No	inbound (Remote PED enhanced)
1503	TCP	Remote PED multifactor quorum authentication	Yes	outbound
1792	TCP	NTLS (Network Trust Link Service)*	No	inbound
5656	TCP	Secure Trusted Channel (STC)*	No	inbound
8443	TCP	REST API webserver	Yes	inbound

* Applications use the client connection to obtain service from the HSM. Service is available only to client systems that are registered with HSM partitions.

Additional Ports

For each remote syslog host that is added (lunash:> syslog remotehost add), three outbound ports are opened for the **rsyslogd** process to connect to the remote syslog server. These ports are assigned randomly by the Luna Network HSM 7 appliance in the range of **32768-60999**.

Cluster Ports

The ports listed below are associated with the **cluster** service, which is available only if the **cluster** secure package is installed (see Installing the Cluster Update). 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.

> **NOTE** All the ports below must remain open for communication between cluster members.

Port	Protocol	Feature	Configurable	Session Initiation
50000	TCP	Cluster service management and inter-member discovery	No	inbound/outbound
50005	TCP	Cluster service configuration and inter-member communication	No	inbound/outbound
50052	TCP	Crypto operations on cluster (default)	Yes (50055-50059)	inbound
50053	TCP	Cluster administration (inter-member)	No	inbound/outbound
50070	TCP	Cluster administration (REST API and inter-member) (default)	Yes (50075-50079)	inbound/outbound
50085	TCP	Cluster messaging service (inter-member)	No	inbound/outbound
50088	TCP	Cluster messaging service management (inter-member)	No	inbound/outbound

Luna Network HSM 7 Appliance Port Bonding

Luna Network HSM 7 has four physical network interface devices: eth0, eth1, eth2, and eth3. You can bond eth0 and eth1 into a single virtual interface, bond0, or eth2 and eth3 into bond1, to provide a redundant active/standby interface. The primary purpose of the service is a hot standby mode for network interface failure, no performance or throughput gains are intended.

The following conditions and recommendations apply to the port bonding feature:

- Bonded interfaces must both be attached to the same network segment. For example, if a bonded interface of IP 192.168.9.126 is chosen, both interfaces must be connected to devices that can access the 192.168.9.* network.
- Bonded interfaces must use static addressing.
- Avoid executing bonding commands while clients are running applications against the Luna Network HSM 7. Where a bonding interface has the same IP as the IP of eth0 or eth2, no ill effects have been observed on running clients other than normal fail-over/recover behavior.
- Avoid executing bonding commands over SSH, which can result in the closure of the active SSH session.

Once bonding is configured, client connections as well as SSH connections continue uninterrupted if either of the bonded interfaces fails.

Using Port Bonding

Use LunaSH to configure, enable, or disable port bonding, and to display the current port bonding status. See network interface bonding for a list of the port bonding commands.

To bond eth0 and eth1 to the bond0 or eth2 and eth3 to the bond1 virtual interface

1. Specify a static IP address, subnet mask, and gateway for the bonded interface.

   NOTE To avoid breaking the NTLS connection to the appliance, ensure that the IP address you specify for the bonded interface is the IP address used for the current NTLS connection. For bond0 use the IP address for eth0 or eth1. For bond1 use the IP address for eth2 or eth3.

   lunash:> **network interface bonding config -ip** <IP_address> **-netmask** <netmask> **-name** {**bond0** | **bond1**} [**-mode broadcast**] **-gateway** <IP_address>

   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.

2. Ensure that the affected network devices are both Activated and that links are detected.

   lunash:> **network show**

3. Enable the bonded interface.

   lunash:> **network interface bonding enable -name** <netbond>

Setting the Default Route on a Bonded Interface

Using older versions of the Luna Appliance Software, each network device can be configured with its own default route. Using Luna Network HSM 7 Appliance Software 7.3.3, **Luna Appliance Software 7.4.2**, or Luna Network HSM 7 Appliance Software 7.7.0 and newer, only one default route may be configured on the appliance. The first network route configured (either automatically using DHCP, or by specifying a valid **-gateway** option when configuring a static IP on a network device) becomes the default route. If you wish to change this default route, you must first delete the original default route. This applies if the default route has been applied on a network interface and you want to enable it on a different interface. The default route remains constant if you switch the device between static and DHCP address selection.

When setting up network devices on your Luna Network HSM 7, the first device you configured with a gateway received the default route automatically. When you enable the bond, if one of the secondary interfaces within the bond has the default route, the bonded interface receives the default route.

If you wish to transfer the default route to the other bonded interface (or a secondary device within the other bonded interface), use the following prodecure.

> **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" below.

To move the default route from eth0 to bond1

1. [Optional] Display the current network settings.

   lunash:> **network route show**

2. Remove the default route from **eth0**. When the default route is removed from a network device or bonding interface, the gateway is automatically dropped.

   lunash:> **network route delete network** <IP_address> **-device eth0 -gateway 0.0.0.0**

3. Disable **bond1**. When a bonding interface is disabled, its gateway value is automatically dropped.

   lunash:> network interface bonding disable **-name bond1**

4. Re-configure **bond1**. Assign the gateway to add the default route to **bond1**.

   lunash:> network interface bonding config **-ip** <IP_address> **-netmask** <netmask> **-name bond1 -gateway** <gateway>

5. Enable **bond1**.

   lunash:> **network interface bonding enable -name bond1**

   Now you can add manual network or host routes as required for your desired network flow.

Disabling a Bonded Interface

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**). If you did not do this, you will need to reconnect using a serial connection after disabling the bond.

To disable a bonded interface

1. Disable **bond0**.

   lunash:> network interface bonding disable **-name bond0**

   The network connection will drop once the bond is disabled.

2. Open a new SSH session to the IP address of **eth0** or another secondary interface, or reconnect to the appliance using a serial connection.

Setting bonding mode to "broadcast"

To set the bonding mode to "broadcast":

1. For each bonded interface, disable first.

   Disable **bond0**.

   lunash:> network interface bonding disable **-name bond0**

   Disable **bond1**.

   lunash:> network interface bonding disable **-name bond1**

2. For each interface, configure *with* the **-mode** broadcast option

   lunash:> **network interface bonding config -name** bond0 **-ip** <ip of interface> **-netmask** <netmask> **-mode** broadcast **-gateway** <ip of gateway>

   lunash:> **network interface bonding config -name** bond1 **-ip** <ip of interface> **-netmask** <netmask> **-mode** broadcast **--gateway** <ip of gateway>

3. For each bonded interface, re-enable.

   Enable **bond0**.

   lunash:> network interface bonding enable **-name bond0**

   Enable **bond1**.

   lunash:> network interface bonding enable **-name bond1**

Setting bonding mode back to "active-backup"

To set the bonding mode to back to the default "active-backup":

1. For each bonded interface, disable first.

   Disable **bond0**.

   lunash:> network interface bonding disable **-name bond0**

   Disable **bond1**.

   lunash:> network interface bonding disable **-name bond1**

2. For each interface, set the bonding mode back to the default "active-backup" mode, configure *without* the **-mode** broadcast option

   lunash:> **network interface bonding config** **-name** bond0 **-ip** <ip of interface> **-netmask** <netmask> **-gateway** <ip of gateway>

   lunash:> **network interface bonding config** **-name** bond1 **-ip** <ip of interface> **-netmask** <netmask> **--gateway** <ip of gateway>

3. For each bonded interface, re-enable.

   Enable **bond0**.

   lunash:> network interface bonding enable **-name bond0**

   Enable **bond1**.

   lunash:> network interface bonding enable **-name bond1**

Setting bonding mode to "lacp"

To set the bonding mode to "lacp":

1. For each bonded interface, disable first.

   Disable **bond0**.

   lunash:> network interface bonding disable **-name bond0**

   Disable **bond1**.

   lunash:> network interface bonding disable **-name bond1**

2. For each interface, configure *with* the **-mode** broadcast option

   lunash:> **network interface bonding config** **-name** bond0 **-ip** <ip of interface> **-netmask** <netmask> **-mode** lacp **-gateway** <ip of gateway>

   lunash:> **network interface bonding config** **-name** bond1 **-ip** <ip of interface> **-netmask** <netmask> **-mode** lacp --**gateway** <ip of gateway>

   > **NOTE** If you choose the lacp mode, the relevant switch(es) on your network ***must*** be configured to support IEEE 802.3ad dynamic link.

3. For each bonded interface, re-enable.

   Enable **bond0**.

   lunash:> network interface bonding enable **-name bond0**

   Enable **bond1**.

   lunash:> network interface bonding enable **-name bond1**

Crypto Traffic Controller for QoS

The Crypto Traffic Controller (CTC) service on the Luna Network HSM 7 is an optional feature that allows you to regulate the bandwidth that is consumed by each client. A client here refers to any machine communicating with the Luna Network HSM 7 through one of its network interfaces. Named classes (defined by you) predetermine sets of minimum and maximum bandwidth parameters. Clients are then assigned, one or more, to appropriate classes. This feature helps to address the noisy neighbor problem, wherein one or more clients, connected to a network interface of the Luna Network HSM 7, dominate the bandwidth thus restricting others. A lack of control over the network bandwidth allocation could result in failure to meet QoS constraints established for your operations, or mandated by your industry niche.

By default, any client that is not explicitly assigned to a named class (for a given interface) falls into the "default" class and is therefore *not bound by any bandwidth limitations*. See "Default class" on the next page.

If you already have an overview of problematic high usage, by time-frame or by other activity patterns, you can quickly impose general constraints to limit the worst offenders, and then fine-tune at leisure.

Monitoring the volumes of bandwidth usage provides the factual information you need

- when applying constraints on excess bandwidth usage for some clients,
- when applying assurance of minimum bandwidth availability for other clients,
- when negotiating with your users/clients, such as for adjustments of contracts, or
- when tracking respective usage to guide decisions around additional resources and their allocation.

The CTC service is added to the service and status commands, and the commands for implementing and managing CTC are at sysconf ctc.

Bandwidth sharing

The service is referred-to as "crypto" traffic control, because whether you reserve an interface for administrative traffic, or allow it on any interface, client traffic resulting from cryptographic operations by the HSM is expected to greatly exceed the occasional administrative exchange, and therefore will be the bulk of any contention among users for bandwidth. If a connection is being used for SSH, that device would be visible under the "measurement show" output (see below), though only if such traffic is exchanged during the measurement period. Typically SSH pings the client at intervals to keep a session alive, but this is unlikely to be a high-frequency exchange compared with client crypto traffic.
CTC guarantees a specific level of bandwidth, defined as a class minimum amount. CTC controls egress traffic. Allotment of ingress traffic bandwidth is not addressed.

CTC gives you tools:

- to measure average bandwidth-usage values per connected client during the time span of interest,
- to measure peak bandwidth usage by connected clients during that time span,
- to configure relative weights, that we call classes, of a client's entitlement out of the total supported bandwidth (for an individual interface eth0, eth1, eth2, eth3, bond0, bond1),
- to assign specific clients to become members of a class, sharing that defined minimum and maximum entitlement of the total bandwidth provided by the particular interface.

Different clients can be assigned to different classes for a given interface.

The class provides instructions to the underlying system to treat the members as fairly as possible. Together with other classes, CTC might ensure that members of a class X are each able to access at least the minimum bandwidth defined for class X, by borrowing unused capacity from other classes. So, any capacity of (say) class Y and class Z that exceeded the minimums defined for those classes might be borrowed to provide class X with at least the minimum processing of its packets. CTC will continue to allot and reassign bandwidth, according to your settings, as long as there is any capacity to do so. Bandwidth could also be borrowed from Default class, as any Clients not explicitly assigned to named classes are unprotected.

For a class to be effective for a client, it must be applied against an interface that is being used for egress traffic *to* the client. See "Impact of route metric on CTC" on page 162 and "Impact of default route on CTC" on page 163

Default class

The default class is a special case. Clients of the Luna Network HSM 7 fall into the default class if they are not assigned to a defined (named) class. Clients in the default class have no pre-imposed restrictions. This means that even if CTC is active, if no clients are assigned to a named class, then they are all in the default class and bandwidth usage is free-for-all. That would be the initial stage when you might be measuring to see what the actual bandwidth usage is, before deciding how to determine the weighting for named classes that you will create.

If you have a clear idea of how all clients are using the HSM, and a given network interface in particular, then create a class that restricts the offending "noisy neighbor" to reasonable bandwidth usage, and just leave the other clients in default class.

However, to be prudently conservative, if, for example, service-level-agreements promise availability of bandwidth to some or all clients, or if there is doubt about what demands some other clients might make, then in addition to the class for the high-volume user(s), consider also creating a class or classes for the other users, so that all are under constraints, and all have minimum-bandwidth allotments to rely on, to avoid surprises for everyone.

What is the basic approach?

With CTC classes you are instructing the system how to address egress-traffic packet handling for members of the class, relative to other users. You can approach the use of CTC in whatever way works for you (within the limits) but the original intent is that:

> You have some number of clients that are using a particular interface on your Luna Network HSM 7.

> Most of those clients have steady small-to-moderate bandwidth usage - the timely availability of that much bandwidth is important to their functioning, but the nature of their usage is that they generally don't demand more; they are consistent.

> Then, you have (for example) one or two clients

- that might have spikes of very high usage, or
- their overall constant demand is growing

(these are the noisy neighbors), and they are putting pressure on the smaller-usage clients, sometimes crowding them out.

> So, you address the issue by

- verifying the bandwidth usage of your clients during a representative time to gain insight into normal and problematic usage

- creating a class that applies to the clients that are heavy or erratic users, ensuring them of a suitable high minimum amount of bandwidth, but *capping their maximum usage*, to prevent excess usage that crowds out the other clients;
- creating a class or classes for the lower-volume users, with suitable *minimum* and maximum settings, to ensure that everyone is treated fairly when bandwidth becomes tight.

All of this takes place within the context of the total bandwidth that the given device supports.

That is:

> for the big-usage clients, **-min** is important to *them*, because they obviously need a lot of bandwidth; **-max** for the big users curtails their high usage enough to let *smaller* users have some needed bandwidth (as determined by the next point)

> for the smaller steady-usage clients, **-min** is most important because they need consistency of access to bandwidth, but **-max** is less important; they are unlikely to require that much more than they normally use.

The CTC service can provide insight and control for best management of bandwidth usage among your clients.

CTC is a service

CTC is an appliance service, added to the Luna Network HSM 7 beginning with appliance software version 7.8.3. An appliance *admin* or *operator* role can control the state of the service with the usual service commands, service start, service stop, and service restart. CTC measures and controls egress traffic from the Luna Network HSM 7 and does not address inbound traffic.

This section discusses the use and behavior of CTC in the context of other networking commands.

Executing any of the following network commands restarts CTC. Network-level changes affect the interface state, which flushes the underlying traffic rules. The restart of CTC service reinstates your rules. When the CTC service has been started, then as long as the Luna Network HSM 7 continues running, the CTC service automatically resumes after any of the silent restarts invoked by these commands:

network dns add nameserver

network dns add searchdomain

network dns delete nameserver

network dns delete searchdomain

network interface delete

network interface dhcp

network interface slaac

network interface static

network route add

network route clear

network route delete

network route metric

An implication of this behavior is that the restart (due to those network commands) also immediately launches any new CTC rules you might have added, without waiting for you to explicitly issue service restart ctc. That is worth keeping in mind if you had any reason to delay your new CTC rules coming into force.

Separately, the sysconf ctc enable command does include a start of CTC service at the time it is run, but the intended use of sysconf ctc enable is only to include CTC among services that are relaunched at reboot or system power-up. We recommend that you use the service start and service stop commands for CTC while you are setting up classes and clients, and use sysconf ctc enable one time, when you are satisfied that your configuration is working as you want it. Thereafter, use **service start ctc** and **service stop ctc** whenever you want to make adjustments during normal operation.

> **NOTE** After making CTC configuration changes, restart the service, to have those changes become operational.

For other network commands, noteworthy behavior includes:

- If you run network interface bonding enable, then CTC is disabled over the slave interfaces upon successful command execution. However, in case of failure of bonding enable, CTC is restarted on the slave interfaces, if it was already running. You must explicitly start CTC on the bonded interface if needed.
- If you run network interface bonding disable, then CTC is disabled for the bond, upon successful command execution. In case of failure of bonding disable, CTC is restarted on the bond, if it was already running.
- Restarting the network service (service restart network) stops CTC and you must restart it (service start ctc). For the same reason, it is not advisable to restart network service while measurement is running.

> **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 to resume CTC operation.
>
> Using Luna Appliance Software 7.8.4 or newer, NTLS service stops after command sysconf config factoryReset.

Included in backup of services configuration

CTC service configuration is included in the information that is backed-up and restored with the sysconf config backup and sysconf config restore commands.

Measurement

Traffic measurement requires that CTC service is running, and is controlled by sysconf ctc measurement enable, sysconf ctc measurement disable, and sysconf ctc measurement show commands. Two values are important to the traffic measurement aspect of CTC:

Parameter	Which command	Description
-interval	sysconf ctc measurement enable	Sets the time between consecutive measurements, when CTC measurement is enabled.

Parameter	Which command	Description
-duration	sysconf ctc measurement show	Uses the duration value to calculate the starting point from which the minimum/maximum and average bit rates for clients are to be calculated, for display by the 'show' command. The -duration value determines how far back in time, before the present moment (the moment that the show command is launched), the starting point for measurement collection should be set, for display. In other words, it's the span of recent time over which you want to collect and summarize measurements of bandwidth-usage, per interface.

Measurements are stored as log entries in memory, so sysconf ctc measurement show can look back in time as far as such entries are available, or as far back as the span of time indicated by **-duration**, whichever is less.

> **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 first, to capture bandwidth usage information that is about to be deleted.

Two options for starting CTC

Issue the **service start -ctc** command to have CTC service running for current session only. With that launch method, the service stops and does not resume if the appliance is restarted or the power is cycled.
For resilient, persistent CTC service, start the service with **sysconf ctc enable** command, in which case the service resumes after restarts or power cycles, and requires that you issue **sysconf ctc disable** command when you want the service to no longer resume automatically after reboot. But see above about the CTC service does not automatically restart after a service restart network command has been run.

The intended approach is to initially run **sysconf ctc enable** to establish ongoing CTC, and then use **service start -ctc** and **service stop -ctc** commands if needed for short-term adjustments, because using the enable command performs additional background operations that are not needed every time the service is started or stopped.

Ongoing measurement (started with **sysconf ctc measurement enable**) allows you to quantify how well you are meeting Service Level Agreements with your clients, and helps suggest the scope of changes that might be necessary, before action becomes urgent.

Records

Measurements are recorded in appliance memory, while the service is active. The records reside in memory only, and do not go to syslog, as is done for other services. For example, if you set an **-interval** of 5, then every 5 seconds, a traffic measurement entry would be added to memory. That goes on as long as measurement is active. Recording is independent of the **sysconf ctc measurement show** command, that tells CTC to go back **-duration** seconds from the moment the **sysconf ctc measurement show** command is run, to gather however many measurements have been taken over that timespan, for display in the command output.

> **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.

Caveats

The memory available for CTC measurement records is part of appliance system memory and therefore finite. If the measurement records begin to approach the limit of reserved memory, CTC begins overwriting earliest entries.

The number of records being generated depends on:

- the interval you set - obviously the smaller the interval, the more frequent the addition of records to CTC memory
- the number of clients that connect and generate traffic.

The memory usage and availability are dynamic, so we cannot provide specific numbers. Therefore, if you set a very short interval, against an interface that is seeing high usage, and let measurement run for days, the earliest records might be lost. Calculations are made against available records at the time the **sysconf ctc measurement show** command is run.

Who can access CTC?

The CTC commands are accessible by the built-in appliance *admin* and *operator* users, or by any custom-named administrative users that you create with roles that are given explicit access to the CTC commands. See "Appliance Users and Roles" on page 96. and "Creating Custom Appliance Roles" on page 117. View/show commands can be run by users with the *monitor* role privileges.

How to use CTC to measure and manage client usage of HSM appliance communication bandwidth

Recommended approach

- Perform a measurement first, to assess the situation.
- Find the egress interface for a given client. See "Impact of route metric on CTC" below and "Impact of default route on CTC" on the next page
- Create a class over that interface, with initial low and high (min and max) bandwidth boundaries.
- Assign the client to the class.
- Perform further measurements and adjust the class parameters, or create additional classes for other clients or groups of clients until the bandwidth usage by all clients is suitably managed.

Impact of route metric on CTC

The metric for each route in a routing table is an estimate of the cost associated with using that route in terms of link speed, hop count, or time delay. When the client is *on the same subnet* as the interface through which traffic is entering the Luna Network HSM 7, then, the client is served through the interface with the lowest metric.

For example, say that a client (at address 192.168.143.92) is assigned to ETH1 (192.168.143.1) and ETH2 (192.168.142.20) has the lowest metric value. Then, the egress traffic for this client flows out of ETH2, and this occurs even if ETH0 is set as a default route. The result is that there is no restriction for this client on ETH2. and this client can have unlimited bandwidth. You would need to create a class over the actual egress-traffic route and assign the client to that class to control its usage of that interface.

You can see the current metric values applied to each interface in the output of the network show command. If needed, you can adjust metric values with network route metric, but consult with your network administrator.

Impact of default route on CTC

When the client is *on a different subnet* from the interface through which traffic is entering, then, the client is served through the interface configured as the default route.

For example, say that a client (192.168.79.157) is assigned to ETH2 (192.168.142.20), and ETH0 (192.168.143.184) is the default route. Then, the egress traffic for this client flows out of ETH0. For such clients, you would need to create classes over that interface (the default route).

Preconditions

Partitions are already created and configured.

Clients are already registered and connected.

Operations by your client applications against respective partitions are proceeding normally.

To perform ongoing measurement of bandwidth usage to track the success of your class definitions and client assignments

1. Enable CTC to take a measurement, every <interval>.

   sysconf ctc measurement enable-interval <how often measurements are made>

   (This automatically restarts the service)

2. Once measurement has been going on long enough to have a useful accumulation of measurements, view the usage summary over a recent time period.

   sysconf ctc measurement show -duration <time span to view and summarize measurements>

3. Measurement continues until you explicitly disable. That is, you can leave it running and making entries indefinitely, until you run:

   sysconf ctc measurement disable

To manage bandwidth usage by clients on a network interface

1. Configure classes. (This can be done without starting CTC service. The service uses any defined classes to determine action applied to assigned clients, and does not perform any management of Default clients [clients not assigned to a defined class].)

   sysconf ctc class define -class <name of new class> **-interface** <eth?|bond?> **-minimum** <minimum_bandwidth> [**-maximum** <maximum_bandwidth>]

   CAUTION! Avoid setting CTC limits so low that normal services like NTLS cannot function.

2. Assign clients to classes, by reference to the **-ip** address from which each client connects, and the **-interface**/device they use to connect.

   sysconf ctc class assign -interface <eth#> -class <classname> **-ip** <ip address of client>

   > **TIP** This is where you would check the routing table portion of the network show output (while keeping in mind "Impact of route metric on CTC" on page 162 and "Impact of default route on CTC" on the previous page) to determine the interface to which this class should be assigned.

3. Start the CTC service.
   Use **sysconf ctc enable**if CTC service has not previously been enabled, or if you have since run **sysconf ctc disable**.
   Otherwise, use **service restart** ctc, if CTC has been enabled and not disabled.

   > **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.

4. Keep track of *classes* you have created, according to the interface to which they apply.

   sysconf ctc class show -interface <ethX or bondX>

5. Keep track of *clients* you have created, and the classes to which they have been assigned.

   sysconf ctc client show -interface <ethX or bondX>

Example

A partition exists and is registered with a client. We could start by checking the CTC situation.

```
[local_host] lunash:>sysconf ctc client   show

No clients are configured

Command Result : 0 (Success)
[local_host] lunash:>sysconf ctc class show

No class configured.

Command Result : 0 (Success)
[local_host] lunash:>service status ctc

  ctc@eth0 is inactive
  ctc@eth1 is inactive
  ctc@eth2 is inactive
  ctc@eth3 is inactive
   CTC is inactive on all interfaces


Command Result : 0 (Success)
```

Create (define) a class and assign a client to that class.

```
[local_host] lunash:>sysconf ctc class define -class Test@0 -interface eth0 -min 10 -max 20


Command Result : 0 (Success)
[local_host] lunash:>sysconf ctc class assign -class Test@0 -interface eth0 -ip
```

```
192.168.143.48


Command Result : 0 (Success)
[local_host] lunash:>sysconf ctc class show

eth0:
          class            min            max
-------------------------------------------
         Test@0         10kbit         20kbit
-------------------------------------------

Command Result : 0 (Success)
[local_host] lunash:>sysconf ctc client   show

eth0:
         client          class
------------------------------
  192.168.143.48         Test@0
------------------------------


Command Result : 0 (Success)
```

Start the CTC service.

```
[local_host] lunash:>service start ctc

Please be patient while the operation is running...
Starting ctc@eth0:                                         [  OK  ]
Starting ctc@eth1:                                         [  OK  ]
Starting ctc@eth2:                                         [  OK  ]
Starting ctc@eth3:                                         [  OK  ]

Command Result : 0 (Success)
```

Enable CTC measurement.

```
[local_host] lunash:>sysconf ctc measurement enable -interval 5


Command Result : 0 (Success)
```

On the client, we generate some traffic for this example.

```
[root@AA3578 bin]# ./multitoken -mode rsasigver -slots 0
multitoken (64-bit) v10.6.0-402. Copyright (c) 2023 Thales Group. All rights reserved.


Warning: packet size not specified.  Using default packet size of 16.

Warning: Key size not specified.  Using default key size of 2048.

Initializing library...Finished Initializing
...done.


Do you wish to continue?

Enter 'y' or 'n': y
```

```
Constructing thread objects.
Logging in to tokens...
  slot 0...
  Enter password: ********

    Serial Number 1335066958556


Please wait, creating test threads.

Test threads created successfully. Press ENTER to terminate testing.

     RSA sign/verify  2048-bit : (packet size = 16 bytes)

     Using token objects.

     Logged in as Crypto Officer.

        + operations/second | elapsed
 0,  0 |   total   average  | time (secs)
------ | ------- ---------- | ------------
   2.0 |     2.0     2.100* |           70


Waiting for threads to terminate.
```

Back at the Luna Network HSM 7 we can take a look at what CTC has recorded.

```
[local_host] lunash:>sysconf ctc measurement show -duration 60

Measurement status: enabled

eth0:
client             min          max          avg          class
-------------------------------------------------------------------------------
192.168.143.48      6400         8552         7004         Test@0

-------------------------------------------------------------------------------
eth1:
client             min          max          avg          class
-------------------------------------------------------------------------------
-------------------------------------------------------------------------------
eth2:
client             min          max          avg          class
-------------------------------------------------------------------------------
-------------------------------------------------------------------------------
eth3:
client             min          max          avg          class
-------------------------------------------------------------------------------
-------------------------------------------------------------------------------

Command Result : 0 (Success)
```

If necessary, modify the class by repeating the sysconf ctc class define command for the same class name and interface, but with a different -min or -max value. This is equivalent to an edit/overwrite of the relevant parameters of the existing class. The change goes into effect as soon as the CTC service is restarted.

Client Startup Delay Across Mixed Subnets

Where a client computer and Luna Network HSM 7 are on different networks, any application (for example, our multitoken utility, or your client application program) that is started on the client computer takes 20 seconds (the NTLS network timeout) to start up. Once running, the application operates normally. On Luna Network HSM 7, an error is logged.

When both Luna Network HSM 7 and client are on the same subnet, the connection occurs without delay.

SSH Public-Key Authentication

In its default configuration, the Luna Network HSM 7 appliance Administrator account (userid admin) uses standard password authentication (userid/password). You can also choose to use Public Key-based Authentication for SSH access. The relevant commands to manage Public Key Authentication are described here.

Public Key Authentication to a Luna Network HSM 7 Appliance Using UNIX SSH Clients

The following is an example exercise to illustrate the use of Public-Key Authentication.

1. From any UNIX client, generate a public key identity to be used for authentication to the Luna appliance:

```
[root@mypc /]# ssh-keygen -b 2048 -t rsa
Generating public/private rsa key pair.
Enter file in which to save the key (/root/.ssh/id_rsa):
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /root/.ssh/id_rsa.
Your public key has been saved in /root/.ssh/id_rsa.pub.
The key fingerprint is:
6e:7a:7e:e1:2a:54:8f:99:3e:6a:56:f8:38:22:fb:a6 root@pinky
```

   Two files are created, a private key file (which stays on the client) and a public key file that we now securely copy to the Luna appliance.

2. SSH to the Luna appliance and verify that the default functionality is a password prompt:

```
[root@mypc /]# ssh admin@myLuna
admin@myLuna's password:
```

3. Use **pscp**/**sftp** to transfer the client's public key to the appliance:

```
[root@mypc /]# sftp /root/.ssh/id_rsa.pub  admin@myluna:
admin@myluna's password:
id_rsa.pub           100%
 |*****************************|   220        00:00
```

4. On the Luna Network HSM 7 appliance, verify the default settings of the Public Key Authentication service:

   lunash:> **sysconf ssh show**

```
[myLuna] lunash:>sysconf ssh show

 SSHD configuration:

 SSHD Listen Port: 22 (Default)
```

```
 SSH is unrestricted.

 Password   authentication is enabled
 Public key authentication is enabled

Command Result : 0 (Success)
```

5. Verify that there are no public key entries by default:

   lunash:> **my public-key list**

```
[myLuna] lunash:>my public-key list

SSH Public Keys for user 'admin':
Name             Type      Bits  Fingerprint
--------------------------------------------------------------------------------

Command Result : 0 (Success)
```

6. Add the public key that you sent over earlier (from server mypc in our example):

   lunash:> **my public-key add** <filename>

```
[myLuna] lunash:>my public-key add id_rsa.pub

Command Result : 0 (Success)
```

7. Check the list again:

   lunash:> **my public-key list**

```
[myLuna] lunash:>my public-key  list

SSH Public Keys for user 'admin':
Name             Type      Bits  Fingerprint
--------------------------------------------------------------------------------
id_rsa.pub       ssh-rsa   1024 6e:7a:7e:e1:2a:54:8f:99:3e:6a:56:f8:38:22:fb:a6

Command Result : 0 (Success)
```

   Notice that the fingerprint reported is the same as was generated back on mypc.

8. From mypc, SSH into myLuna; you should not be password prompted:

```
[root@mypc /]# ssh admin@myluna
Luna Network HSM 7.0 Command Line Shell - Copyright (c) 2001-2017 Gemalto, Inc. All rights
reserved.
```

9. Verify that you are still password prompted if you ssh from other clients:

```
bash-2.05b# ./ssh admin@myLuna
admin@myLuna's password:
```

10. Disable public key authentication on myLuna, and verify the current status of the service:

    lunash:> **sysconf ssh publickey disable**

    lunash:> **sysconf ssh show**

11. SSH in again from mypc, and verify that you are password prompted:

```
[root@mypc /]# ssh admin@myLuna
admin@myLuna's password:
```

Summary
The above example illustrates enabling and disabling Public-Key Authentication for SSH connections to your Luna appliance.

> **NOTE** Console (serial port) access still requires the userid and password.

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!

To further explore/confirm the Public-Key Authentication functions, you could SSH in again from Windows and other UNIX clients, and verify that you are still password prompted as normal for those clients.

Verify that the client list is always accurate.

Delete one or two of your public key clients. Verify that those clients are password prompted again.

Clear all public key clients with the -clear sub-command. Verify that all clients are password prompted again.

Obviously, most of the above has been an extended example, to show various aspects of the function, and you do not need to go through all those steps just to set up Public-Key Authentication for a client/admin computer.

Set up Public-Key SSH access for other Luna Network HSM 7 users

Here are the high level steps to set up SSH pubkey access for a non admin user:

- As admin, create the user and assign the desired role to that new user.
- Log on to Luna Network HSM 7 as the new user. You are prompted to change the default password.
- Transfer (**pscp**/**sftp**) the SSH pubkey to the Luna appliance using the new user account (example $ pscp id_rsa_pub op-number1@lunasa7:).
- Log in with the new account.
- Add your SSH key (lunash:> **my public-key add** (<filename>)

Here is an example session:

```
operator@mypc:~/.ssh$ pscp id_rsa.pub op-number1@lunasa7:
op-number1@lunasa7's password:
id_rsa.pub                                    100%  392     0.4KB/s   00:00
operator@mypc:~$ ssh op-number1@lunasa7
op-number1@lunasa7's password:
Last login: Wed Mar  11 08:51:46 2015 from 192.168.10.18
Luna Network HSM 7.0 Command Line Shell - Copyright (c) 2001-2017 Gemalto, Inc. All rights
reserved.
[lunasa7] lunash:>my publickey add id_rsa.pub

Command Result : 0 (Success)
```

Setting and Clearing SSH Restrictions

Restrictions according to selected Ethernet device

Luna Network HSM 7 has two Ethernet devices, eth0 and eth1 that can be used for SSH connections. If your environment requires that SSH be restricted to one or the other, use the command `sysconf ssh device eth0` or `sysconf ssh device eth1`.

To remove the restriction, use the command `sysconf ssh device all`.

Restrictions according to originating client host IP

If your situation requires that you restrict client access against a named appliance user ID, such that only specified host IP addresses are permitted to make SSH connections, then you can create an allowlist of acceptable host IPs for each user ID on your appliance.

Use the sysconf ssh client list command to see the connection permission status of :

- any of the default appliance user IDs, and
- any named user IDs that you have created on the appliance.

Use the sysconf ssh client add, sysconf ssh client delete, and sysconf ssh client clear commands to manage allowlists of host IPs permitted to make SSH connections to any or all of the appliance user IDs.

If a user ID has "All clients" beside it in the **sysconf ssh client list** output, then there are no restrictions (by the appliance) regarding which external client host IPs can make SSH connections to that user ID.
If a user ID has one-or-more IP addresses beside it in the **sysconf ssh client list** output, then no external client host IPs, other than those explicitly named, can make SSH connections to that user ID.

> **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.

When to Restart NTLS

Here are the situations where NTLS needs restarting.

> **NOTE** All client connections must be stopped before you restart NTLS.

- When you regenerate the server certificate (the interface prompts you to restart NTLS after regenerating the server cert)
- If you delete Partitions
- If you change binding settings (lunash:> **ntls bind**)

In all other circumstances, NTLS should remain running. If there are problems with clients connecting to the Luna Network HSM 7 appliance, other methods of debugging should be attempted before restarting NTLS.

Examples are:

- Confirming the fingerprint of the client certificate and the server certificate at both the client and the server (the Luna Network HSM 7 appliance).
- Verifying that the client is registered and has at least one Partition assigned to it.

Impact of the service restart ntls Command

If you perform lunash:> **service restart ntls** on a live, or production Luna appliance, any active sessions would be lost. That is, HSM Partitions would remain active, but Clients would need to re-connect and re-authenticate.

As a general rule, an NTLS restart is required immediately after a server certificate regeneration on a Luna appliance. This occurs under the following circumstances only:

- As part of original installation and setup.
- If you have reason to suspect that the Luna appliance's server certificate (private key) has been compromised.

In the former case, there is no impact. In the latter case, the brief disruption of active Clients would be overshadowed by the seriousness of the compromise.

Timeouts

Your network connections will timeout after a period of inactivity, as described below.

SSH Timeout

The Luna Network HSM 7 appliance pings SSH clients with TCP keepalive to ensure clients are still reachable. Idle SSH sessions remain open, but are terminated if the client is unreachable for 15 seconds. This timeout is not configurable. If your session times out, you must open a new SSH session.

If you are using Luna Network HSM 7 Appliance Software 7.7.1 or newer, SSH sessions timeout after 30 minutes of inactivity.

If you want idle SSH sessions to be terminated when running an appliance software version older than Luna Network HSM 7 Appliance Software 7.7.1, you must configure a timeout on your network switch or firewall.

NTLS Timeout

As a general rule, do not adjust timeout settings (either via the interface or in config files) unless instructed to do so by Thales Technical Support.

Changing some settings can appear to improve performance until a situation is encountered where a process does not have time to complete due to a shortened timeout value.

Making timeouts too long will usually not cause errors, but can cause apparent performance degradation in some situations (HA).

Default settings have been chosen with some care, and should not be modified without good reason and full knowledge of the consequences.

> **CAUTION!** Never insert TAB characters into the crystoki.ini (Windows) or crystoki.conf (UNIX) file.

Network Receive Timeout

One timeout value that might require change is the ReceiveTimeout value in the "LunaSA Client" section of the configuration file. This timeout value is the period that the Luna Network HSM client will wait for a response from the Luna Network HSM 7 before determining that the appliance is off-line. The default value of 20 seconds provides a worst-case scenario over a larger WAN, but may be inappropriate for some Luna Network HSM 7 deployments (such as Luna HSMs in an HA configuration) where a quicker determination of the health of the Luna Network HSM 7 system is required. This value can be set in the Luna Network HSM 7 configuration file as follows:

Windows (crystoki.ini)

```
[LunaSA Client]
:
  ReceiveTimeout=<value in milliseconds> //default is 20000 milliseconds
:
```

UNIX (etc/Chrystoki.conf)

```
LunaSA Client = {
:
  ReceiveTimeout=<value in milliseconds>;
:
}
```


CHAPTER 7: Copying Files to and from the Appliance

Historically, file transfers between Luna Network HSM 7 appliance and clients or between the appliance and other servers (certificate exchanges, log files, update packages, etc.) have used the scp protocol via scp command on Linux/Unix hosts and PSCP or other utilities on Windows hosts.

SCP has reached its limits and is being supplanted across the internet by the secure ftp (SFTP) protocol, which has scope for future adaptability for general improvements to functionality and for keeping up with advancing security requirements. On Luna Network HSM 7 appliances, the change is part of a larger refresh/update of the the onboard base (hardened) operating system with Luna Appliance Software 7.9.0 and newer.

Many customers are using earlier versions, so for compatibility, any commands or operations that transfer files in-and-out of the appliance, and any instructions and examples that refer to such transfers, might still reference SCP. However, the default protocol that is actually called is SFTP. Whether the operation negotiates the SFTP protocol or needs to downgrade to SCP, this occurs transparently to the user - your scripts should continue to work.

> **NOTE** As cryptographic algorithms age, and might eventually be deemed unsafe, the suite of ciphers available and selectable for securing SCP/SFTP operations is subject to change and individual ciphers might be dropped in future, which could affect scripted automated tasks. In general, Thales will warn you via mention in the CRN that a cipher is being discontinued for SSL, SSH, or SCP/SFTP.

Disallowed filepaths for SFTP

Using Luna Appliance Software 7.9.0 or newer, the following criteria apply to file transfers to the Luna Network HSM 7:

Filepath	Allowed/Disallowed
Any file path with "../" in it	Disallowed
server.pem	Only allowed to get. Cannot replace **server.pem** on the Luna Network HSM 7 appliance.
client_syslog.pem	Only allowed to get. Cannot replace **client_syslog.pem** on the Luna Network HSM 7 appliance.
File name with a length less than 1 or greater than 64	Disallowed

Filepath	Allowed/Disallowed
Any file name with "/" in it	Disallowed
File name that ends with a space	Disallowed
File name with "-" (dash)	Allowed
File name that starts with a space	Disallowed
File name with special characters other than letters, digits, underscores, periods, spaces, or hyphens. Such as @,#,$,%,^,&,*	Disallowed
Empty file names	Disallowed

Files can be sent to/from only the current user's "my files".

Backing Up and Restoring the Appliance Configuration

> **TIP** This page concerns authentication and management of roles that govern *network administrative access **to the appliance***.
>
> That is, access, management, and use of the cryptographic module and its application partitions, are distinct from access to the physical platform (and operating system) in which the HSM resides. This is true:
>
> - for Luna PCIe HSM 7 installed in a workstation that you provide, and
> - for the same cryptographic module inside a Luna Network HSM 7 appliance with hardened operating system and administrative access restricted to the limited Luna shell command set.
>
> On the appliance, the cryptographic module has its own separate and distinct authentication roles and requirements; see hsm init , hsm login, and partition init, partition init co, partition init cu, partition createchallenge, partition changepw, partition activate, and audit changepwd, audit login among the various other administrative operations on the SSH-accessible appliance command path, or via the equivalent REST APIs, as well as the client-side equivalent commands (in LunaCM) partition init, partition login, partition logout, and all the partition role commands.

The appliance **admin** can create a backup of configuration settings for various services running on the Luna Network HSM 7 appliance, and save it to the appliance file system. This allows you to easily restore the configuration after a factory reset, ensuring that existing clients can connect to the restored appliance with all services functioning correctly. You can create multiple backup files and provide a description for each, to store different configurations. You can store your configuration backup files on the appliance filesystem, save them to the internal HSM, or export them to an external backup HSM.

- "Backing Up the Appliance Configuration" on page 176
- "Restoring the Appliance Configuration" on page 176

> "Managing Configuration Backup Files" on page 177

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

Configuration file size for Backup and Restore

Previously, appliance configuration files could be backed up and restored to-and-from an internal HSM, or a Backup HSM, as long as the configuration file size did not exceed 64 kilobytes. Using Luna Appliance Software 7.8.5 or newer, the file size constraint is removed, and you can backup and restore configuration files very much larger than 64K bytes in size. A possible use for this ability is if you have a large number of clients configured for the current appliance.

Compatibility with previous practice is preserved.

> If your backup file is less than 64 KB, the **sysconf config backup** command detects that immediately and carries on with the one file (no different than in prior releases).
Example: lnh202_Config_ntls_20240403_1023.tar.gz

> If your backup file is greater than 64 KB, the **sysconf config backup** command alerts you that it will be breaking the file into several smaller chunk files.

- The chunk files are named as the full-size file would be named, but with the addition of a sequential number, appended to each.
- After the last chunk is created, a SHA512 hash is created and saved under the same name. This is used to verify the chunk files and guide their reassembly, later.

Example:

lnh202_Config_ntls_20240403_1023.tar.gz_00

lnh202_Config_ntls_20240403_1023.tar.gz_01

lnh202_Config_ntls_20240403_1023.tar.gz_sha512

- You must retain all the chunk files and the hash file, in order to reassemble into the original file, so do not lose, erase, or rename any in a set.

Configuration Backup and Restore - Individual Services

Previously, appliance configuration could be backed up as all services together in one file. Using Luna Appliance Software 7.8.5 or newer, the **-service** option is added, allowing you to specify that

> any single service can be backed up to a file, or

> all services can be backed up in one file.

Backing Up the Appliance Configuration

Backing Up the Appliance Configuration

Use the following procedure to back up your appliance configuration to the appliance filesystem.

> **CAUTION!** This procedure does not back up HSM or partition configurations. It applies only to the Luna Network HSM 7 appliance settings configurable in LunaSH.

Prerequisites

> You must be logged in to LunaSH as **admin** to back up the appliance configuration.

To back up the appliance configuration

Back up the appliance configuration, specifying an optional description for the backup file. Use quotes to include spaces in your description. To save a copy of the initial factory configuration instead of the current configuration, include the **-factoryconfig** option. If you are using Luna Appliance Software 7.8.5 or newer, you can optionally specify the individual service you want to back up.

lunash:> **sysconf config backup** [**-description** <description>] [**-service** <one of network, ssh, ntls, syslog, ntp, snmp, users, system, webserver, ctc>]

Refer to examples in the sysconf config backup command reference.

Restoring the Appliance Configuration

Use the following procedure to restore appliance services from a stored configuration backup. You can restore the entire configuration or select specific services to restore.

Prerequisites

> You must be logged in to LunaSH as **admin** to restore the appliance configuration.

> If you are restoring the network configuration, log in using a serial connection so that you do not lose contact with the appliance.

> The configuration backup file must be available on the appliance filesystem.

To restore the appliance configuration

1. [Optional] Check the list of configuration backup files available on the appliance.

lunash:> **sysconf config list**

2. Stop any services you wish to restore.

   lunash:> **service stop** <service>

3. Restore the configuration from backup by specifying the backup file and service you wish to restore.

   lunash:> **sysconf config restore -file** <filename> **-service** <service>

4. Restart the service or reboot the appliance to activate the restored configuration settings.

   lunash:> **service restart** <service>

   lunash:> **sysconf appliance reboot**

Managing Configuration Backup Files

If you wish, you can keep only the backup files that you find useful, and individually delete any others using the **sysconf config delete** command. You can also use the **sysconf config clear** command to delete all of your configuration backup files.

Note that the configuration backup file area is a special-purpose location, accessible only using the **sysconf config** commands. You will not see those files listed if you run the command **my file list**.

There is no limit on the size of individual backup files 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. Some size restrictions apply if you plan to export a backup file into your HSM using **sysconf config export**.

Backing Up the Appliance Configuration to the HSM

You can protect a configuration setup against the possibility of appliance failure by exporting a backup file into the internal HSM or an external backup HSM. The command **sysconf config export** allows you to place the configuration backup file onto an HSM and **sysconf config import** allows you to retrieve the file from that HSM, back to the appliance file system. The export command gives you two target options:

- The internal HSM of your Luna Network HSM 7 appliance. This could be useful if a component failed in the appliance, you sent the appliance back to Thales Group for rework under the RMA procedure, received it back repaired, and then retrieved the file from your HSM to restore your appliance settings.
- A locally-installed Luna Backup HSM. This could be useful if the current appliance failed and you wished to install a replacement. Similarly, you could use system configuration backup files restored from a Backup HSM to uniformly configure multiple Luna Network HSM 7 appliances with a standard set of parameters applicable to your enterprise.

If you are exporting a configuration backup to a Luna Network HSM 7, please note the following file size restrictions:

- The maximum size of individual exportable files is 64 KB.
- The maximum storage capacity of the Admin/SO partition is 384 KB.

Automatically generated configuration backup files

A configuration backup file is generated automatically when you run the **sysconf config restore** or **sysconf config factoryreset** commands. This allows you to revert to your current configuration if the restore operation did not achieve the expected results.

Listing your configuration backup files

You can use the **sysconf config list** command to list all of your backup files, complete with the description you provided for each one, as shown in the following example. The configuration settings file area will always contain the original factory file, and might additionally contain any number of intentionally created backups, and possibly one or more automatic backup files:

Upgrading the appliance software changes your configuration settings

If you upgrade your appliance software, your configuration settings may be changed as part of the upgrade process and, as a result, the original factory configuration no longer applies. Immediately after you upgrade your appliance, create a new configuration backup file and make note of the backup file created. Later, if you wish to restore to this configuration, use the **sysconf config restore** command with the file created after upgrade.

EXAMPLE of sysconf backup, export, import, and restore

First we see why the backup file might be large...

```
[local_host] lunash:>client list

registered client 1: 192.168.76.95
registered client 2: 192.168.76.45
registered client 3: 192.168.76.67
registered client 4: 192.168.76.121
registered client 5: 192.168.72.61
registered client 6: 192.168.78.66
... <lots more, trimmed for brevity>
registered client 287: 192.168.72.91
registered client 288: 192.168.72.92
registered client 289: 192.168.72.93
registered client 290: 192.168.72.94
registered client 291: 192.168.72.95
registered client 292: 192.168.72.87
registered client 293: 192.168.72.100

Command Result : 0 (Success)

[local_host] lunash:>
```

Perform the backup, to create the backup file in the host file system...

```
[local_host] lunash:>sysconf config backup -service ntls -description "taking backup of NTLS
configuration with ipcheck disabled"

Created configuration backup file: local_host_Config_ntls_20240510_0145.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:>

[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:>
```

We're here... why not verify it...

```
[local_host] lunash:>sysconf config show -file local_host_Config_ntls_20240510_0145.tar.gz


System information when this backup was created:

hostname: local_host
eth0 IP Address: 192.168.75.8
eth1 IP Address:
eth2 IP Address:
eth3 IP Address:
Software Version: Luna Network HSM v7.8.5-250 [Build Time: 20240507 14:42]
HSM Firmware Version: 7.8.4
HSM Serial Number: 532016
uptime:  01:45:45 up 15:45,  3 users,  load average: 2.06, 1.92, 1.89
Current time: Fri May 10 01:45:45 EDT 2024

Service backed up: ntls
Description: taking backup of NTLS configuration with ipcheck disabled


Command Result : 0 (Success)

[local_host] lunash:>
```

We need a place to put it (export)...

```
[local_host] lunash:>token backup list

   Token Details:
   =============
   Token Label:                        G5Backup
   Slot:                               1
   Serial #:                           7001966
   Firmware:                           6.28.0
   HSM Model:                          G5Backup


Command Result : 0 (Success)

[local_host] lunash:>token backup login -serial 7001966


  Please enter Token Administrator's password:
  > ********

'token backup login' successful.

Command Result : 0 (Success)

[local_host] lunash:>
[local_host] lunash:>sysconf config list -deviceType token -serialNumber 7001966
```

```
 Data objects not found.

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

Looks like a clean landing spot, so we start the export...

```
[local_host] lunash:>sysconf config export -file local_host_Config_ntls_20240510_0145.tar.gz -
deviceType token -serialNumber 7001966 -force


Force option used. Proceed prompt bypassed.

local_host_Config_ntls_20240510_0145.tar.gz is too large. Maximum allowed size for an export to
HSM/backup HSM is 64KB

Your backup file will be exported in smaller chunks. (You can still import these using the
original backup file name)

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

> proceed
Proceeding...
Files exported:
local_host_Config_ntls_20240510_0145.tar.gz_00
local_host_Config_ntls_20240510_0145.tar.gz_01
local_host_Config_ntls_20240510_0145.tar.gz_02
local_host_Config_ntls_20240510_0145.tar.gz_sha512


Command Result : 0 (Success)

[local_host] lunash:>
```

Export was successful so, for this example clear any config backups from the file system...(not necessary, except to illustrate unambiguously)

```
[local_host] lunash:>sysconf config clear -force

Force option used. Proceed prompt bypassed.

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
-------------------------------------------------------------------------------------------------
------

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

Perform the import...(notice that the filename provided is as it would be for a single file, *without* the added chunk-numbering)...

```
[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:>
```

Did it work?...

```
[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:>
```

Looks good, but here is the crucial test...

```
[local_host] lunash:>sysconf config restore -s ntls -file local_host_Config_ntls_20240510_
0145.tar.gz

WARNING !! This command restores the configuration from the backup file: local_host_Config_
ntls_20240510_0145.tar.gz.
It first creates a backup of the current configuration before restoring: local_host_Config_
ntls_20240510_0145.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_ntls_20240510_0456.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 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.
If the service being restored was disabled prior to restoring, then the user needs to manually
enable it.

Command Result : 0 (Success)

[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
9654            |  local_host_Config_ntls_20240510_0456.tar.gz                                |  Automatic Backup
Before Restoring: ntls

Command Result : 0 (Success)
[local_host] lunash:>
[local_host] lunash:>client list

registered client 1: 192.168.76.95
registered client 2: 192.168.76.45
registered client 3: 192.168.76.67
registered client 4: 192.168.76.121
registered client 5: 192.168.72.61
registered client 6: 192.168.78.66
  < and again, hundreds trimmed from this list>
registered client 290: 192.168.72.94
registered client 291: 192.168.72.95
registered client 292: 192.168.72.87
registered client 293: 192.168.72.100

Command Result : 0 (Success)
```

Yes.

CHAPTER 8: Updating the Luna Appliance Software

The Luna Network HSM 7 appliance software consists of the LunaSH command-line shell and its underlying software components. Use the following procedure to install the Luna Network HSM 7 appliance software update.

The update package includes an image of the latest HSM firmware, which you must install to take advantage of all the new features in this release. When you install the appliance software update, the latest firmware image is stored on the appliance file system but not installed.

CAUTION! The system can hold only one firmware version in standby at a time. Updating the appliance software version also updates the firmware version held in reserve on the HSM, overwriting the version that was stored there before. If you are keeping a specific firmware version in reserve (for example, awaiting a FIPS validation announcement for that version), do not update the appliance software.

If you have a Luna Network HSM 7 that was shipped before December 2019, you must install the Luna Network HSM 7 Reboot Patch before updating to Luna Network HSM 7 Appliance Software 7.7.0 or newer. If this patch is not installed, the appliance software update will not proceed.

A change to network routing when updating to Luna Network HSM 7 Appliance Software 7.7.0 or newer, from any prior 7.x version, can cause your appliance to become unreachable via network connection. Older appliance versions permitted the existence of multiple default routes. Beginning with Luna Network HSM 7 Appliance Software 7.7.0, only one instance of the default route can exist.

Options for a successful update with minimal disruption are:

> Remove all but one instance of the 'default route', using the **network route delete** command, *before* upgrading from any appliance software version older than Luna Network HSM 7 Appliance Software 7.7.0.

> Connect locally via serial cable to perform the update, so your access to the network appliance is not lost when network connection becomes temporarily unavailable (pending proper network configuration).

Note also that if you re-image, going back to a version older than Luna Network HSM 7 Appliance Software 7.7.0, the routing table goes back to the old format and you must apply one of the above precautions again, to update.

If the above precautions are not taken and the appliance becomes unreachable, complete the following steps to restore connection to the appliance:

1. Connect locally via serial cable.
2. Delete all network interfaces. See network interface delete.
3. Configure a network interface to use a default route by doing one of the following:
   - Configure the network interface to use a static IP configuration while specifying the **-gateway** option. See network interface static.
   - Configure the network interface to use DHCP. See network interface dhcp.

After you complete the above steps, network connectivity to the appliance is restored and any remaining interfaces that are configured do not have a default route set.

NOTE The appliance software update cannot be rolled back directly. You can re-image to a predetermined configuration and then update to a desired appliance software version (see "Re-Imaging the Appliance to Baseline Software/Firmware Versions" on page 186). The HSM firmware, however, can be rolled back to the previously-installed version (see Rolling Back the Luna HSM Firmware).

Firmware installation is a separate procedure (see Updating the Luna HSM Firmware).

To update the appliance software and firmware, you must transfer and apply a secure package file to the Luna Network HSM 7. You require:

> Luna Network HSM 7 appliance software update package file (<filename>**.spkg**)

> the secure package authentication code, provided in a text file accompanying the update package

To upgrade the Luna Appliance Software

1. Transfer the secure package update file to the Luna Network HSM 7 using **pscp** or **sftp**.

   pscp <path>/<filename>**.spkg admin@**<appliance_host/IP>**:**

2. Stop all client applications to the Luna Network HSM 7 appliance.
3. Using a serial or SSH connection, log in to the appliance as **admin** (see "Logging In to LunaSH" on page 101).
4. Log in as HSM SO (see Logging In as HSM Security Officer).

   lunash:> **hsm login**
5. [Optional Step] Verify that the secure package file is present on the Luna Network HSM 7.

   lunash:> **package listfile**
6. [Optional Step] Verify the package file, specifying the authorization code you received from Thales.

   lunash:> **package verify** <filename>**.spkg -authcode** <code_string>
7. Install the update on the Luna Network HSM 7.

   lunash:> **package update** <filename>**.spkg -authcode** <code_string>

   The installation/update process takes approximately one and a half minutes. A series of messages shows the progress of the update. At the end of this process, a message `Software update completed!` appears.
8. Reboot the Luna Network HSM 7 appliance.

   lunash:> **sysconf appliance reboot**

   > **NOTE** If you are updating the appliance software from version 7.4.x or older to Luna Network HSM 7 Appliance Software 7.7.0 or newer, the appliance reboots automatically.

   The latest firmware update package is now stored in reserve on the appliance, waiting to be installed. See Updating the Luna HSM Firmware to install the firmware.

CHAPTER 9: Re-Imaging or Decommissioning the HSM Appliance

During the lifetime of a Luna Network HSM 7, you might have cause to take the HSM out of service, and wish to perform actions to ensure that no trace of your sensitive material remains. Those events might include:

- Placing the unit into storage, perhaps as a spare
- Shipping to another location or business unit in your organization
- Shipping the unit back to Thales for repair/re-manufacture
- Removing the HSM permanently from operational use, for disposal at end-of-life

You also have the option of restoring the HSM appliance to its factory baseline state, erasing all sensitive material and restoring the base appliance software and HSM firmware.

This chapter describes the available options in the following sections:

- "Re-Imaging the Appliance to Baseline Software/Firmware Versions" below
- "Decommissioning the Luna Network HSM 7 Appliance" on page 190
- "RMA and Shipping Back to Thales" on page 191
- "End of Service and Disposal" on page 192

For more information about the effects of these procedures, see Comparing Zeroize, Decommission, Re-image, and Factory Reset.

Re-Imaging the Appliance to Baseline Software/Firmware Versions

The Luna Network HSM 7 appliance software update includes two versions: the newest version, and a baseline version that is stored in reserve on the appliance. If you find that the latest software does not suit your organization's purposes, you can re-image the appliance to its factory baseline. This procedure formats the Luna Network HSM 7 file system, zeroizes the HSM, erases the appliance configuration, and resets the software/firmware to the baseline version.

This capability is useful if you are re-purposing an HSM for a project that has standardized on an earlier software/firmware configuration, or if you need to format the appliance completely and remove all traces of its prior configuration (to securely return control of the appliance to a cloud provider, for example).

Appliance re-image also allows you to roll back the appliance software, which was not possible in previous Luna releases.

If you have a Luna Network HSM 7 that you have updated to Luna Network HSM 7 Appliance Software 7.3.0 at least once, the baseline consists of:

- Luna Network HSM 7 Appliance Software 7.2.0
- Luna HSM Firmware 7.0.3

After you re-image the appliance, you can update to whichever software/firmware version you wish. For valid update paths, refer to the Customer Release Notes for the version you wish to install. Download your preferred software/firmware version from the Thales Support Portal (see "Support Contacts" on page 12).

> **CAUTION!** Re-imaging to an older appliance software version might expose vulnerabilities that were fixed in newer releases.
>
> Appliance re-image formats the Luna Network HSM 7 appliance file system and zeroizes the HSM. All files and settings on the appliance will be destroyed, including:
>
> - All roles, partitions, and cryptographic objects on the HSM (except for partition licenses); the HSM must be re-initialized
> - All existing client and remote PED server registrations, as well as the Remote PED Vector (RPV), which should be reinitialized following re-image, in order to proceed remotely
> - All appliance built-in roles, including the **admin** role return to default passwords, and must be given new, secure passwords
> - Any custom appliance roles (deleted completely)
> - All appliance configuration settings.
> - All files stored on the appliance, including upgrade packages and audit logs (lunash:> **my file list**)

After the appliance re-image procedure, only the following information is preserved:

- Using Luna Appliance Software 7.8.5 or older, the network configuration is preserved; if you are accessing the appliance remotely via SSH connection, you will not permanently lose contact with the appliance. 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 via a serial connection or a physical network interface (**eth0**/**eth1**/**eth2**/**eth3**) to avoid losing contact with the Luna Network HSM 7.
- Partition licenses purchased via the Thales License Portal, unless you included the **-base** option (lunash:> **sysconf reimage start**)

To re-image the appliance to baseline software/firmware versions

1. Ensure that you have backed up all important cryptographic objects, appliance files, and appliance logs. Each user of the appliance (**admin**, **operator**, **monitor**, **audit**, and any custom users) must back up any important files by using **pscp**/**sftp** to transfer them off the appliance file system. Ensure that application partitions are not being used by any client before proceeding.
2. Ensure that you have previously initialized the Auditor role and configured audit logging on the HSM. By default, audit logs for critical events are stored in the HSM's on-board memory. These logs are only accessible to the Auditor, and therefore cannot be erased by the re-image procedure. If you have never configured audit logging on the HSM, these logs remain in the HSM memory. If you are re-imaging the appliance for another party (or returning control of the appliance to a cloud provider), the next Auditor could access these logs.

   To prevent this, configure audit logging on the HSM before re-imaging the appliance (see Configuring Audit Logging). This procedure will transfer the existing audit logs to the appliance file system, where they can be retrieved and then erased by the re-image process.

If you have not previously configured audit logging, you are prompted with a warning about this when you initiate the re-image process.

3. Ensure that the Luna Network HSM 7 is connected to an uninterruptible power supply.

> **CAUTION!** Loss of power during the re-image operation may leave the appliance in an unrecoverable state.

4. Log in to LunaSH as **admin**, and then log in to the HSM as HSM SO.

   lunash:> **hsm login**

5. Re-image the appliance to the baseline version.

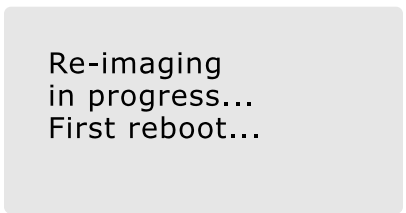
   lunash:> **sysconf reimage start**

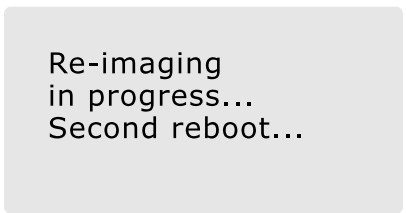
> **CAUTION!** The operation takes 15-20 minutes, and the appliance reboots twice. Do not manually reboot the appliance, tamper/decommission the HSM, or otherwise interrupt the operation during this time.

```
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.
```

During the re-image operation, the following messages appear on the front-panel LCD display to help track the progress:





6. When the process is complete, log in as **admin** via SSH, using the default password **PASSWORD**, and set up the appliance as if it were new.
7. [Optional] The **admin** user can view a summary file of the re-image operation and initial startup. Use **pscp**/**sftp** to transfer the file to a client workstation.

   lunash:> **my file list**

   ```
   lunash:>my file list

        4134 Jun 19 13:27 firstboot.log

   Command Result : 0 (Success)
   ```

Troubleshooting

If the re-image operation fails before the appliance reboots, retrieve the re-image log.

lunash:> **sysconf reimage tarlog**

```
lunash:>sysconf reimage tarlog

'hsm reimage tarlogs' successful
```

```
Use 'sftp' from a client machine to get file named:
Baseline_Re_image_logs.20180614_14.40.40.tar.gz

Command Result : 0 (Success)
```

The log file now appears in the **admin** user's files on the appliance (lunash:> **my file list**). Use **pscp**/**sftp** to transfer it to a client workstation. Thales Customer Support may request this log to help assess the issue.

> **NOTE** 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.

Decommissioning the Luna Network HSM 7 Appliance

This section describes how to decommission the appliance to remove all current key material and configurations, so that it can be safely redeployed.

To decommission the Luna Network HSM 7

For full decommission (removing the unit from service, clearing the HSM of all your material, clearing the appliance of all identifying information) of a Luna Network HSM 7 appliance, and assuming that you can power the appliance and gain **admin** access, follow these steps in LunaSH, using a serial connection:

1. Rotate all logs:

   lunash:> **syslog rotate**

2. Delete all files in the SCP directory:

   lunash:> **my file clear**

3. Delete all logs:

   lunash:> **syslog cleanup**

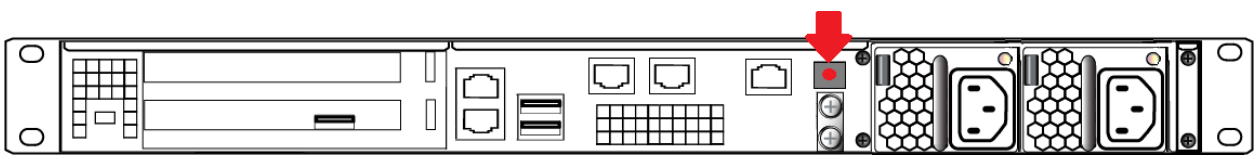
4. Return the appliance to factory-default settings:

   lunash:> **sysconf config factoryreset -service all**

5. Delete any backups of settings:

   lunash:> **sysconf config clear**

6. Push the decommission button (refer to "HSM Emergency Decommission Button" on page 48 for a full description of what happens).



7. Power down the appliance.

8. Power up the appliance. At this point, the HSM internally issues and executes a **zeroize** command to erase all partitions and objects. This step takes about five minutes. The KEK is already gone at that point – erased as soon as the button is pressed – so the step of erasing partitions and objects is for customers subject to especially rigid decommission protocols.

Disabling Decommissioning

You can disable the decommissioning feature if you have the factory-installed **HSM Capability 46: Allow Disable Decommission** (see HSM Capabilities and Policies). The primary reason for disabling decommissioning is to prevent the HSM from being automatically decommissioned due to loss of battery (see Tamper Events). If decommissioning is disabled, you can continue to use the Luna Network HSM 7 after the battery has been depleted, but this is not recommended by Thales.

To disable decommissioning

Set **HSM Policy 46: Disable Decommission** to **1**(ON).

lunash:> **hsm changepolicy-policy 46 -value 1**

RMA and Shipping Back to Thales

Although rare, it could happen that you need to ship a Luna Network HSM 7 back to Thales. Contact your Thales representative to obtain the Return Material Authorization (RMA) and instructions for packing and shipping. You might wish (or your security policy might require you) to take maximum precaution with any contents in your HSM before it leaves your possession.

RMA Process for Thales Luna HSM Devices Containing Sensitive Customer Key Material

Thales Luna Hardware Security Modules (HSMs) are designed, manufactured and tested to the highest level of quality. On occasion, a product may fail in the field after use by the customer. Products that fail in the field, when covered by a maintenance agreement or during the warranty period, may be eligible for an RMA.

Secure RMA Without Access to Key Material

Thales recognizes that Luna HSMs may contain sensitive customer key material. In case of an RMA, Thales does not have access to key material:

- Keys stored in the HSM are encrypted using a master key based on the customer's authentication method.
- It is impossible for Thales to retrieve or use sensitive customer key material from either a functioning or a failed HSM without the password or PED keys.
- Without these authentication devices or passwords, Thales cannot access key material in the device, even by reading the flash memory, as per FIPS 140-2 Level 3 and Common Criterial EAL4+ validation processes.

HSM Decommissioning

The general practice before returning a Luna HSM under an RMA is to decommission the HSM following the instructions in the user documentation (see "Decommissioning the Luna Network HSM 7 Appliance" on the previous page for instructions). This deletes the master key.

NOTE Ensure you have a backup of your keys.

End of Service and Disposal

Luna HSMs and appliances are deployed into a wide variety of markets and environments. Arranging for the eventual disposal of a Luna Network HSM 7 that is no longer needed can be a simple accounting task and a call to your local computer recycling service, or it can be a complex and rigorous set of procedures intended to protect very sensitive information.

Needs Can Differ

Some users of Luna HSMs employ cryptographic keys and material that have a very short "shelf life". A relatively short time after the HSM is taken out of service, any objects that it contains are no longer relevant. The HSM could be disposed of, with no concern about any material that might remain in it.

The majority of our customers are concerned with their keys and objects that are stored on the HSM. It is important to them that those items never be exposed. The fact is that they are never exposed, but see below for explanations and actions that address the concerns of auditors who might be more accustomed to other ways of safeguarding HSM contents.

Luna HSM Protects Your Keys and Objects

The design philosophy of our Luna HSMs ensures that contents are safe from attackers. Unlike other HSM products on the market, Luna HSMs never store sensitive objects, like cryptographic keys, unencrypted. Therefore, Luna HSMs have no real need - other than perception or "optics" - to perform active erasure of HSM contents, in case of an attack or tamper event.

Instead, the basic state of a Luna HSM is that any stored keys and objects are strongly encrypted. They are decrypted only for current use, and only into volatile memory within the HSM.

If power is removed from the HSM, or if the current session closes, the temporarily-decrypted objects instantly evaporate. The encrypted originals remain, but they are unusable by anyone who does not have the correct HSM keys to decrypt them.

How the HSM encryption keys protect your sensitive objects

In addition to encryption with the user specific access keys or passwords, all objects on the HSM are encrypted by the HSM's global key encryption key (KEK) and the HSM's unique Master Tamper Key (MTK).

If the HSM experiences a Decommission event (pressing of the small red button on back of Luna Network HSM 7, or shorting of the pins of the decommission header on the HSM card, then the KEK is deleted.

If the HSM experiences a tamper event (physical intrusion, environmental excursion), then the MTK is destroyed.

Destruction of either of those keys instantly renders any objects in the HSM unusable by anyone. In the case of a Decommission event, when the HSM is next powered on, it requires initialization, which wipes even the encrypted remains of your former keys and objects.

We recognize that some organizations build their protocols around assumptions that apply to other suppliers' HSMs - where keys are stored unencrypted and must be actively erased in the event of an attack or removal from

service. If your policies include that assumption, then you can re-initialize after Decommission - which actively erases the encrypted objects for which no decrypting key existed. For purposes of security, such an action is not required, but it can satisfy pre-existing protocols that presume a weakness not present in Luna HSMs.

Our customers are often very high-security establishments that have rigorous protocols for removing a device from service. In such circumstances, it is not sufficient to merely ensure that all material is gone from the HSM. It is also necessary to clear any possible evidence from the appliance that contains the HSM, such as IP configuration and addresses, log files, etc.

If you have any concern that simply pressing the Decommission button and running **sysconf config factoryreset** is not sufficient destruction of potentially-sensitive information, then please refer to "Decommissioning the Luna Network HSM 7 Appliance" on page 190.

