SafeNet Luna Network HSM 7.2

APPLIANCE ADMINISTRATION GUIDE

Document Information

Product Version	7.2
Document Part Number	007-013576-004
Release Date	15 August 2018

Revision History

Revision	Date	Reason
Rev. B	15 August 2018	Initial release.

Trademarks, Copyrights, and Third-Party Software

Disclaimer

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

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

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

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

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

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

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

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

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

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

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 Gemalto-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 primarily for the SafeNet Luna Network HSM appliance, outside of the HSM. HSM administrative tasks are described in the *SafeNet Luna HSM Administration Guide*.Some activities might encompass both portions of the SafeNet Luna HSM server.

As an HSM Server, SafeNet Luna Network HSM provides increased operational flexibility over traditional HSMs. The SafeNet Luna Network HSM appliance includes an integrated FIPS 140-2 level 3 HSM, the SafeNet K6 Cryptographic Engine, which offers the same high level of security as traditional HSMs.

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

- Password Authentication version (equivalent to FIPS 140-2 level 2, using passwords, only, for authentication and access control.
- PED (Trusted Path) Authentication version that requires the PED and PED Keys for authentication and access control.

The HSM appliance adds a secure service layer (NTLS and STC) that allows the SafeNet 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:

This preface also includes the following information about this document:

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

Customer Release Notes

The customer release notes (CRN) provide important information about this release that is not included in the customer documentation. Read the CRN to fully understand the capabilities, limitations, and known issues for this release. You can view or download the latest version of the CRN from the Technical Support Customer Portal at https://supportportal.gemalto.com.

Audience

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

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

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

Document Conventions

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

Notes

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

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

Cautions

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

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

Warnings

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

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

Command Syntax and Typeface Conventions

Format	Convention
bold	The bold attribute is used to indicate the following: > 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 Gemalto Customer Support.

Gemalto Customer Support operates 24 hours a day, 7 days a week. Your level of access to this service is governed by the support plan arrangements made between Gemalto and your organization. Please consult this support plan for further information about your entitlements, including the hours when telephone support is available to you.

Customer Support Portal

The Customer Support Portal, at https://supportportal.gemalto.com, is where you can find solutions for most common problems. The Customer Support Portal is 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. You can also use the portal to create and manage support cases.

> **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 Support

If you have an urgent problem, or cannot access the Customer Support Portal, you can contact Gemalto Customer Support by telephone at +1 410-931-7520. Additional local telephone support numbers are listed on the support portal.

Email Support

You can also contact technical support via email at technical.support@gemalto.com.

CHAPTER 1: Appliance Hardware Functions

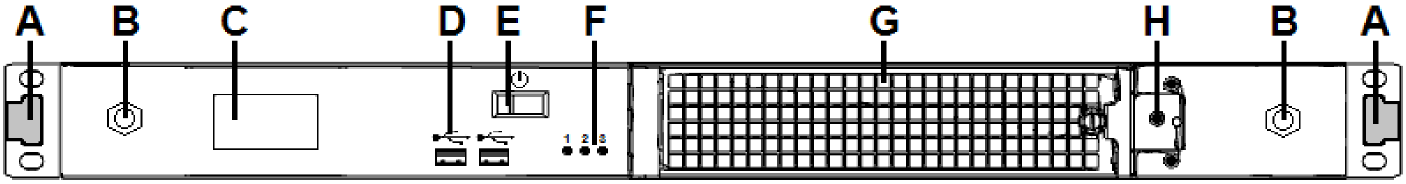
This chapter describes the administrative and maintenance tasks you can perform directly on the SafeNet Luna Network HSM hardware. It contains the following sections:

Physical Features

The SafeNet Luna Network HSM is 1U high and fits into standard 19-inch equipment racks.

Front Panel

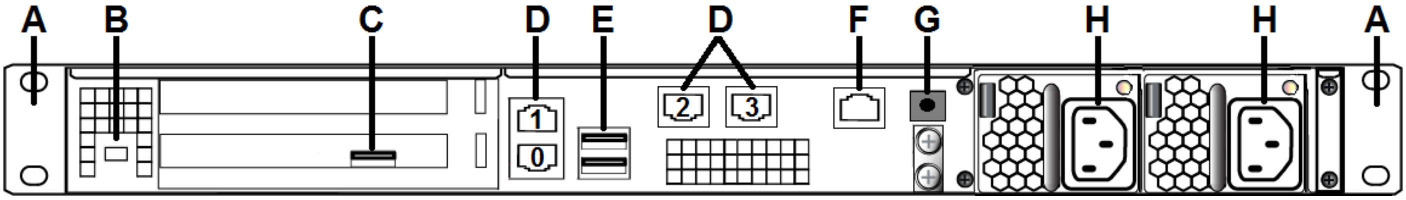
The front panel is illustrated below, with the secure locking bezel removed:



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 19-inch 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 the next page
D	USB 3.0 ports	The appliance has a total of four (4) USB 3.0 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 19.
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 21.
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 21.

Rear Panel

The rear panel is illustrated below:



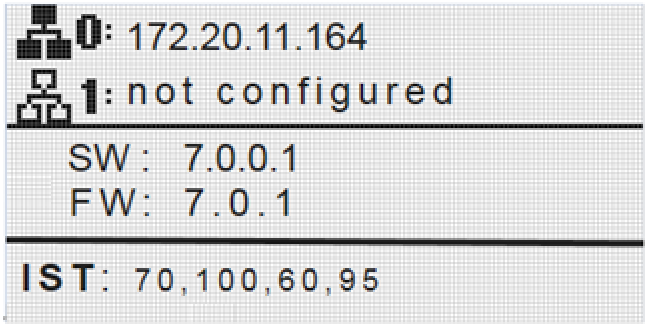
Item	Name	Description
A	Sliding rail brackets	Connect to the sliding rails mounted on the sides of the appliance chassis, allowing it to be mounted in a standard 19-inch appliance rack.
B	Kensington lock connector	Allows the appliance to be secured to a desk or equipment rack using a Kensington lock.
C	HSM card USB port	When authenticating with a PED, the PED must be connected directly to the HSM card. The other USB ports on the appliance will not work for PED connection.

Item	Name	Description
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 3.0 ports	The appliance has a total of four (4) USB 3.0 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 "SafeNet Luna Network HSM Required Items" on page 1). See also "Installing the SafeNet Luna Network HSM Hardware" on page 1.
G	Decommission button	This button should only be pressed as part of decommissioning and zeroizing the appliance. See also "Declassify or Decommission the HSM Appliance" on page 1.
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 21.

Front-panel LCD Display

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

Figure 1: The LCD display



```
■0: 172.20.11.164
□1: not configured

 SW:  7.0.0.1
 FW:  7.0.1

IST: 70,100,60,95
```

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 OFT OOS 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.
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.

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 the LunaSH **status sysstat code all** command 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.

State	Status	Description
ISO	0	In Service Operational. No trouble.
	60	In Service Operational. The eth0 interface is offline. Use the LunaSH **network show** and **service status network** commands to display more information about the status of the network interfaces.
	61	In Service Operational. The eth1 interface is offline. Use the LunaSH **network show** and **service status network** commands to display more information about the status of the network interfaces.
	62	In Service Operational. The eth2 interface is offline. Use the LunaSH **network show** and **service status network** commands to display more information about the status of the network interfaces.
	63	In Service Operational. The eth3 interface is offline. Use the LunaSH **network show** and **service status network** commands to display more information about the status of the network interfaces.
	80	In Service Operational. The STC service is not running. Use the LunaSH **service status stc** command 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 the LunaSH **service status webserver** command to display more information about the status of the webserver service.
	100	In Service Operational. The SNMP service is not running. Use the LunaSH **service status snmp** command to display more information about the status of the SNMP subsystem.
OOS	20	Out of Service. The NTLS service is not running. Use the LunaSH **service status ntls** command 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 the LunaSH **service status ntls** command to display more information about the status of the NTLS service, and the **syslog tail** command 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 the LunaSH **hsm information show** and **syslog tail** commands help troubleshoot the issue.
OFL	50	Off Line. None of the Ethernet interfaces are connected to the network. Use the LunaSH **network show** command to display more information about the status of the network, and the **syslog tail** command to view the system logs to help troubleshoot the issue.

State	Status	Description
IST	70	In Service Trouble. The syslog service is not running. Use the LunaSH **service status syslog** command to display more information about the status of the syslog service, and the **syslog tail** command to view the system logs to help troubleshoot the issue.
	90	In Service Trouble. The SSH service is not running. Use the LunaSH **service status ssh** command to display more information about the status of the syslog service, and the **syslog tail** command to view the system logs to help troubleshoot the issue.
	110	In Service Trouble. Hard disk utilization is too high. Use the LunaSH **syslog tarlogs** command to create a tar archive of the logs and then use **scp** to transfer the log archive from the appliance to a remote computer for archiving.

NOTE The LCD initially shows the Gemalto 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.

System Behavior with Hardware Tamper Events

The SafeNet appliance uses the Master Tamper Key (a key on the HSM that encrypts everything on the HSM) to deal with both hardware (physical) tamper events and Secure Transport Mode.

Tampering with the Appliance

Hardware tamper events are detectable events that imply intrusion into the appliance interior.

One such event is removal of the lid (top cover). The lid is secured by anti-tamper screws, so any event that lifts that lid is likely to be a serious intrusion.

Another event that is considered tampering is opening of the bay containing the ventilation fans.

You can use the thumbscrew to access the mesh air filter in front of the fans, without disturbing the system. However, if you open the fan-retaining panel behind that, which requires a Torx #8 screwdriver, then the system registers a tamper.

Therefore, cleaning of the filter is encouraged, especially if you work in a dusty environment, but fan module removal and replacement are discouraged unless you have good reason to suspect that a fan module is faulty. See "Power Supply and Fan Maintenance" on page 21 for more information.

Decommission

The red "Decommission" button recessed behind the back panel is not a tamper switch. Its purpose is different. See "HSM Emergency Decommission Button" on page 27 for a description.

What Happens When You Tamper - Including Opening the Fan Bay

The following sequence illustrates how a tamper event affects the HSM and your use of it. You do not need to perform all these steps. Many are included for illustrative purposes and to emphasize the state of the appliance and of the enclosed HSM at each stage.

Action	Result/State
First, we place the HSM in its basic operational condition (we reset only to have a clean starting point for this illustration).	
hsm factoryReset	Starting point
hsm initialize	Basic setup of HSM
Next, we illustrate a software "tamper" (destroying the MTK by setting the HSM into Transport Mode)	
stm transport	Enable Secure Transport Mode.
hsm show	Basic HSM info remains undisturbed.
partition list	None have been created since initialization, above.
partition create	Attempt to create a partition - doesn't work; must be logged in as SO.
hsm login	No, can't do that either: LUNA_RET_MTK_ZEROIZED
stm recover	Log in to the HSM and HSM SO and recover from Secure Transport Mode. Also, the PED presents the Transport Mode verification string.
hsm login	This time, it works.
partition create	Partition is created.
partition list	Confirm that the created partition is there - you have confirmed that you have successfully set Secure Transport Mode, then recovered from it. The HSM is unusable while in STM, but is fully restored to its previous state when you recover from STM.
Now, we illustrate a hardware tamper (by physically interfering with the appliance as an intruder might do)	
open the fan bay (with a Torx #8 screwdriver)	The HSM stops responding as the vkd (HSM driver) times out [the command-line prompt is still available until you issue a command that attempts to access the HSM, at which point the driver goes into time-out] - the entire system stops responding for approximately ten minutes (you can wait it out, or you can reboot) - the system has detected a tamper event
(system resumes) run **sysconf appliance reboot** or press the restart [Stop/Start] switch on the back panel	(If you wait until the system becomes responsive on its own, issue **sysconf appliance reboot**; if you simply restart with the switch, that's the same thing, but faster.)

Action	Result/State
when the system is back up, run hsm show	Check for HSM Tampered: Yes or No

view the logs	The **audit log** shows events like:
	`lunash:>audit log tail -f hsm_150073_00000001.log`
	
	`133098,13/01/28 14:39:37,S/N 150073 HSM with S/N 150073 logged the`
	` following internal event: LOG: resync(0x0000002e)`
	`133099,13/01/28 14:47:15,S/N 150073 HSM with S/N 150073 logged the`
	` following internal event: TVK was corrupted.(0x00000027)`
	`133100,13/01/28 14:47:15,S/N 150073 HSM with S/N 150073 logged the`
	` following internal event: Existing Auto-Activation data won't work(0x00000029)`
	`133101,13/01/28 14:47:15,S/N 150073 HSM with S/N 150073 logged the`
	` following internal event: Generating new TVK...passed(0x0000002a)`
	`133102,13/01/28 14:47:15,S/N 150073 HSM with S/N 150073 logged the`
	` following internal event: RESTART(0x0000002f)`
	`133103,13/01/28 14:47:35,S/N 150073 HSM with S/N 150073 logged the`
	` following internal event: LOG: resync(0x0000002e)`
	
	`Command Result : 0 (Success)`

hsm tamper show	WARNING - Tamper(s) Detected
hsm login	not permitted: LUNA_RET_MTK_ZEROIZED
hsm tamper clear	Clear the HSM tamper. The HSM SO must be logged in to issue this command.
hsm login	This time, it works.
partition list	Confirm that the pre-existing partition is present.
partition showContents	Confirm that any pre-existing partition contents are there.

Next, we illustrate what happens when a physical tamper occurs while the HSM is already in Secure Transport Mode

stm transport	Enter Secure Transport Mode.

hsm tamper show	`lunash:>hsm tamper show`
	
	`No active tampers.`
	
	`Command Result : 0 (Success)`

Action	Result/State
Open the appliance lid, or open the fan bay (opening the lid would damage the chassis and void your warranty, this is for example purposes only)	The HSM stops responding when you enter an HSM command, or it gives an error message (any of several, depending on what it was doing at the time) and then stops responding.

Summary of Your Responses to Tamper Events

If you have a password-authenticated HSM, or if you have a PED-authenticated HSM, then both splits of the MTK reside always on the HSM.

The MTK is destroyed by a tamper event, and the HSM becomes unresponsive. When you react to this by rebooting the appliance, the HSM has both splits available and can immediately reconstitute the MTK and go on operating normally, without further intervention from you.

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

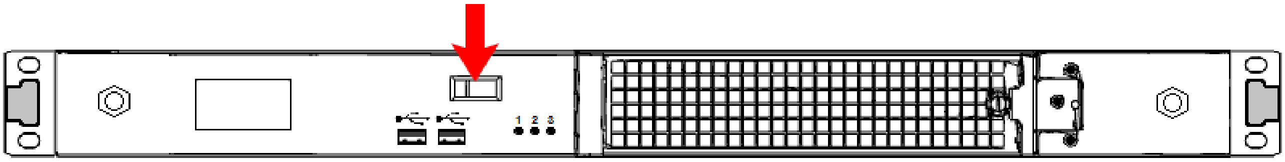
This section describes how to power-on, power-off, or reboot the appliance. It contains the following sections:

- "Power On" below
- "Power Off" on the next page
- "Reboot" on the next page
- "Hard Reboot" on the next page
- "Automatic Restart Following a Power Interruption" on page 21

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 13 in the *Appliance Administration Guide*.

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 the command **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 issue the **sysconf appliance reboot** command.

To switch off the system, issue the **sysconf appliance poweroff** command, or use the START/STOP switch on the SafeNet Luna Network HSM 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 **sysconf appliance reboot** and **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 **sysconf appliance hardreboot**.

- The disadvantage is that the shutdown is abrupt and not orderly - in a constrained and hardened system like SafeNet Luna Network HSM, 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 the **sysconf appliance poweroff** command, 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 SafeNet Luna Network HSM 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 SafeNet Luna Network HSM appliance with only one power supply, we recommend that you remove the second supply to silence the audible alarm.

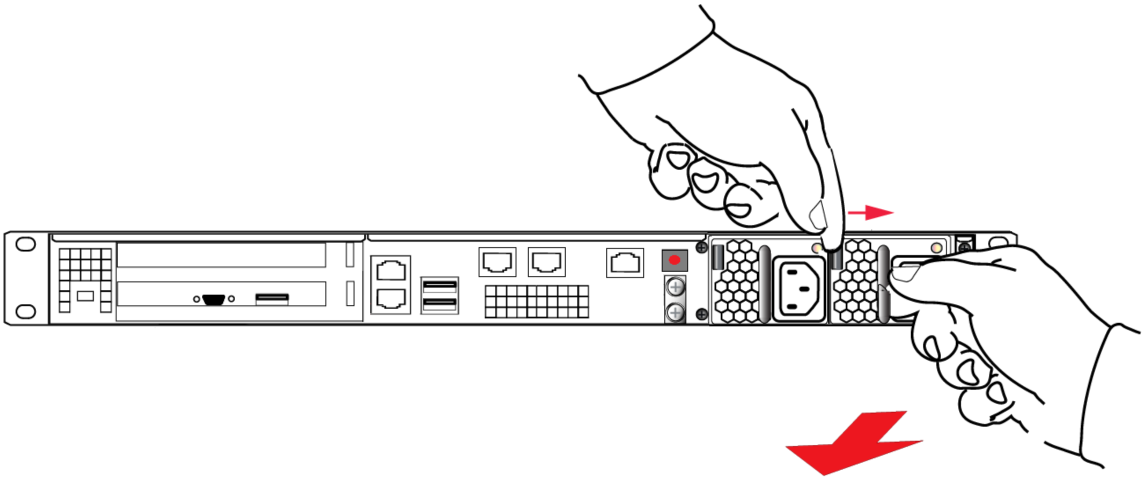
Replacing a Power Supply

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

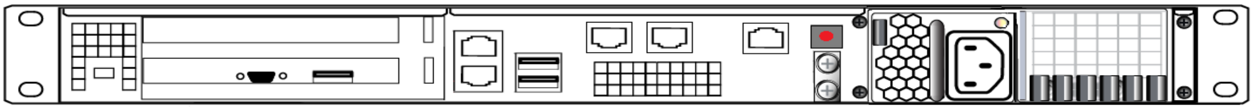
To remove a power supply:

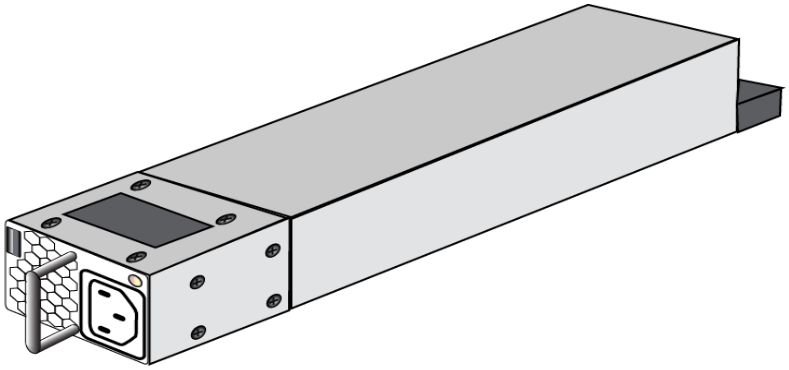
1. To remove a power supply, face the back of the appliance.
2. Disconnect/unplug the selected power supply.

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 Reinstall 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 (**sysconf appliance reboot**), or until you use the Stop/Start switch on the appliance rear panel.

Cleaning the Filter

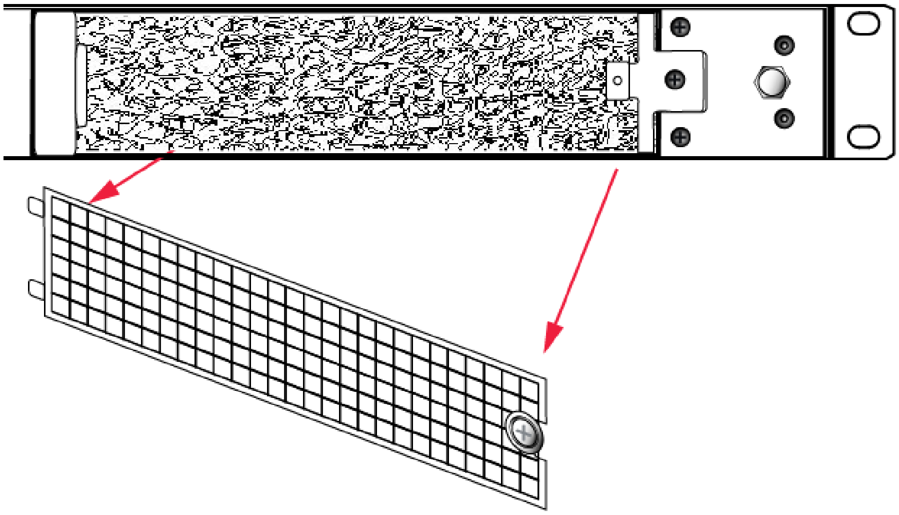
The ventilation grille, located to the right, on the appliance front panel, is secured in two parts, by two screws - a knurled, captive thumb-screw, and a Torx T8 screw. The knurled screw can be fastened or released without tools. It secures the lattice screen that in turn retains the mesh air filter.

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.

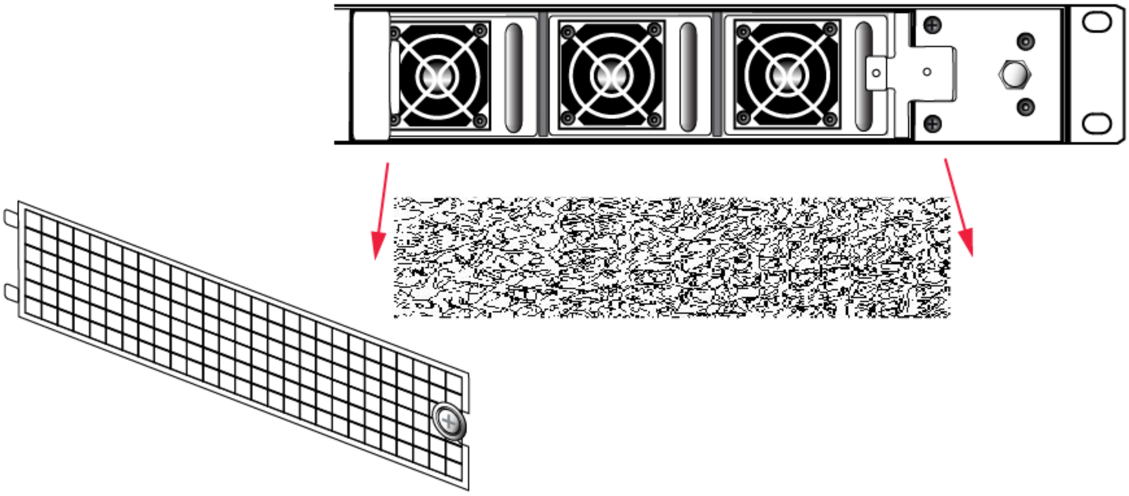
> **NOTE** Accessing the air filter mesh in front of the fans (using the thumbscrew to open the retaining grille) does not cause a tamper.

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. Do so.



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 the LunaSH command **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:

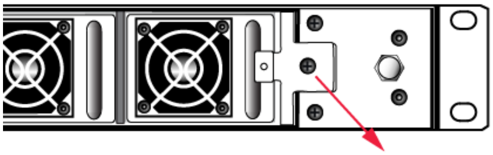
```
----------- Front Cooling Fans Status --------------
FAN1A   lnr      0 RPM   Unplugged or Failed
FAN1B   lnr      0 RPM   Unplugged or Failed
FAN2A   OK       3000 RPM
FAN2B   OK       2900 RPM
FAN3A   OK       2900 RPM
FAN3B   OK       3000 RPM
```

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.

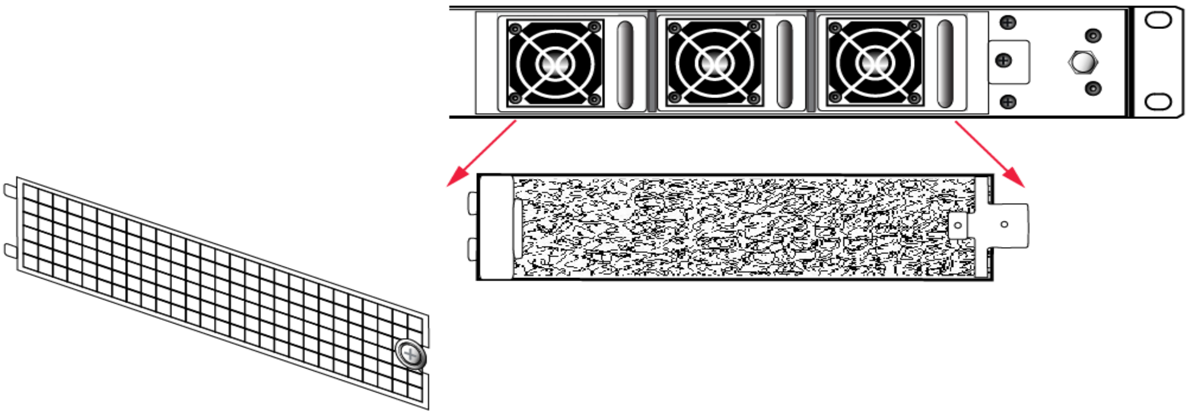
> **NOTE** Partition authentication data is de-cached by the tamper - you must execute **partition activate -partition** <name_of_partition> each of your HSM partitions before your clients can resume accessing them. Partition activation does not survive a tamper event. In either case, you can examine the log for tamper events: **syslog tail -search tamper -entries 200**

To replace a fan:

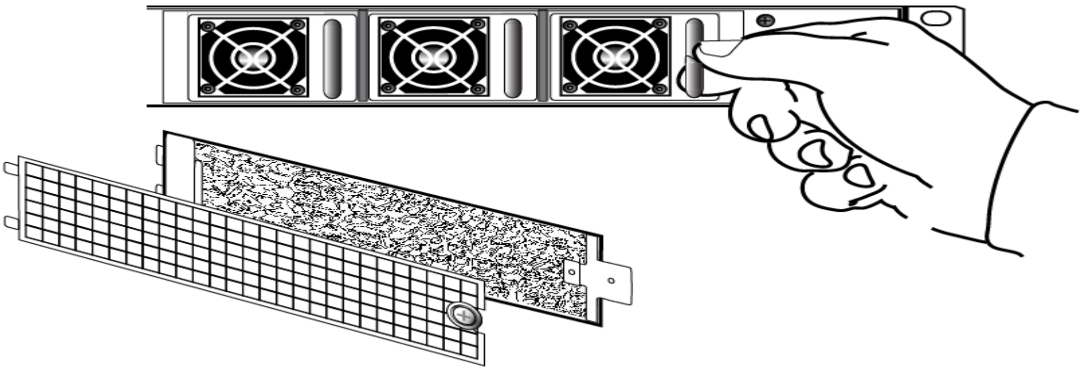
1. To open the fan bay, use a Torx number 8 screwdriver to remove the screw that secures the right-side tab of the fan retainer.



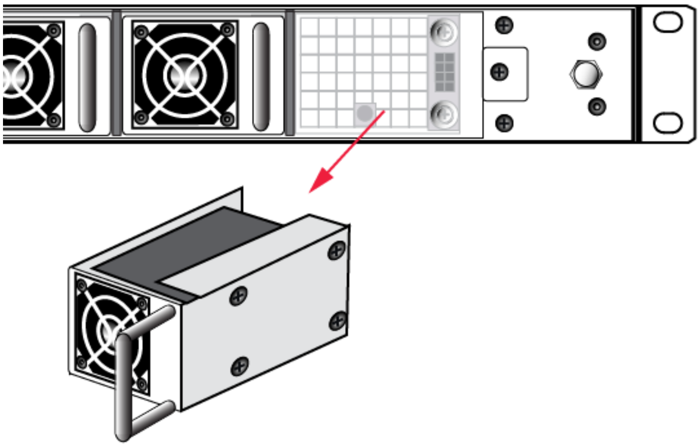
2. The fan retainer is anchored at its left by two tabs - swing the retainer out like a door, and remove it. There is no need to separate the filter mesh and its retainer from the larger fan retainer; the assembly can come out as one piece. The illustration below happens to show them separated.



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 (**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 HSM Partitions (**partition activate -partition** <name_of_partition>), so that they once more become available to your registered clients.

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.

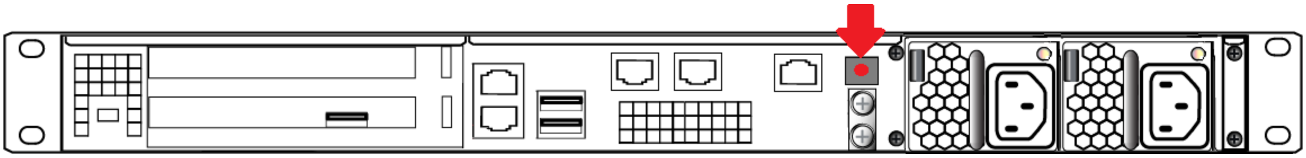
Opening the fan bay (behind the filter), by unscrewing that Torx screw, does cause a tamper and therefore some down-time for your Clients. If only one fan module is showing a defect, you can probably leave replacing it until scheduled down-time, during which there would be no unexpected disruption to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

HSM Emergency Decommission Button

The SafeNet 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 inside the SafeNet appliance, press and release the small red button on the front 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 screw-driver or other tool to reach the Emergency Decommission button. This is intentional, to preclude 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

Here is what you would observe after the button is depressed:

- The LCD on the appliance front panel freezes. Communication to the HSM key card is blocked, as is the software process that polls the HSM for status.
- At this point, you must power cycle the SafeNet 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.
- The LunaSH command **hsm show** displays the text "Manually Zeroized: Yes", to signify that the system executed the decommission process.
- The HSM key card must be reinitialized (**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" on page 1.

Disabling Decommissioning

You can disable the decommissioning feature if you have the factory-installed Capability 46: Allow Disable Decommission and Policy 46: Disable Decommission (see "HSM Capabilities and Policies" on page 1). The primary reason for disabling decommissioning is to prevent the HSM from being automatically decommissioned due to loss of battery (see "Tamper Events" on page 1). If decommissioning is disabled, the SafeNet Luna Network HSM has an indefinite shelf life, as far as the battery is concerned.

To disable decommissioning

1. Ensure that the Disable Decommissioning capability is installed on the HSM. To verify that the capability is installed, enter the following command:

   lunacm:> **hsm showpolicies**

   If the capability is installed, Capability 46: Allow Disable Decommission and Policy 46: Disable Decommission are listed.

2. Enter the following command to enable Policy 46: Disable Decommission

   lunacm:> **hsm changehsmpolicy -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 Gemalto, 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 SafeNet Luna Network HSM is being returned to Gemalto

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

Serial Connections

You can use a serial connection to connect a computer directly to the SafeNet Luna Network HSM to access the LunaSH command line.You must use a serial connection to perform your initial configuration. Once the network parameters are established, you can switch to an SSH session over your network.

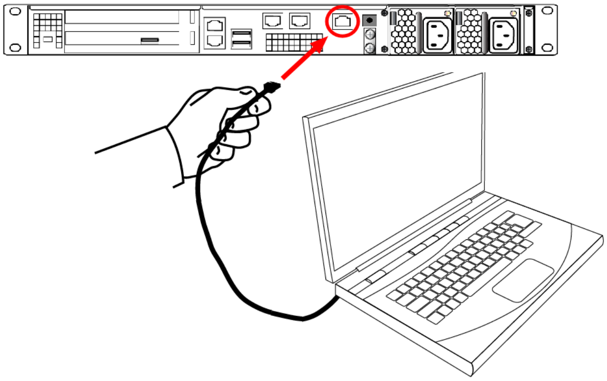
Direct administration connection via serial terminal is the method for initial configuration for the following reasons:

- The specific IP address, randomly assigned to your SafeNet appliance by an automated testing harness during final factory testing, is unknown.
- Configuring network settings via SSH, in addition to requiring the original IP address, necessarily involves losing that 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 **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.



2. If the driver for the Prolific Technology Inc. USB to RJ45 (with 8P8C connector) adapter did not download and install automatically, go to http://www.prolific.com to download and install the PL2303 USB-to-Serial Windows driver.

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:

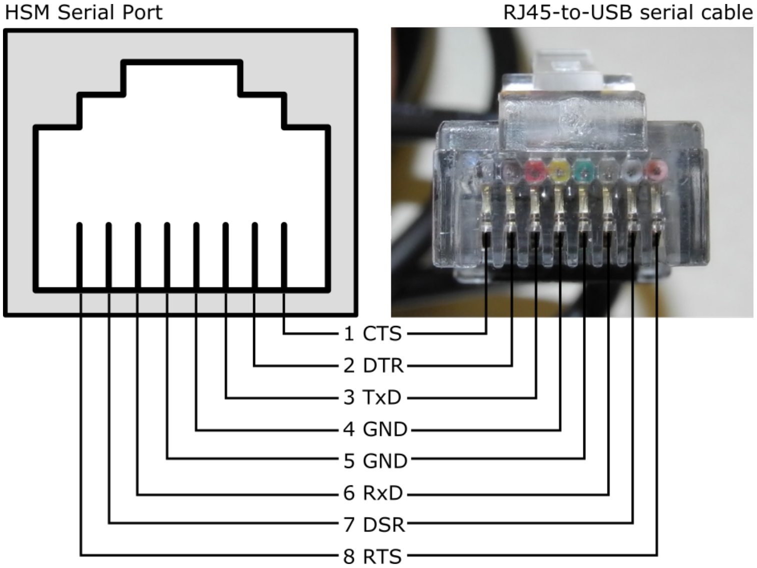
Baud rate	115200
Data bits	8
Parity	None
Stop bits	1

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.

Serial Pinout

The HSM 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:



Troubleshooting

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

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.

Front Locking Bezel

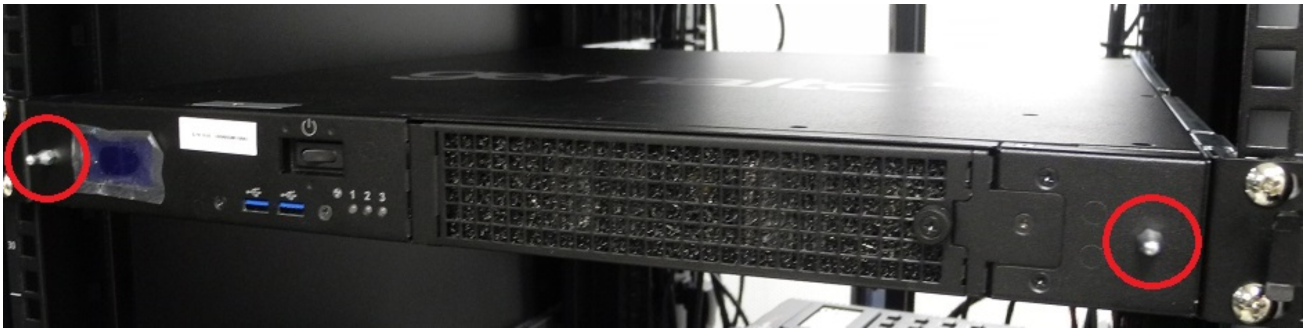
Your order may have included an optional front locking bezel (pictured below). The locking bezel fits over the HSM's faceplate for maximum physical access security. Certain security standards require the use of these physical access measures.

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.

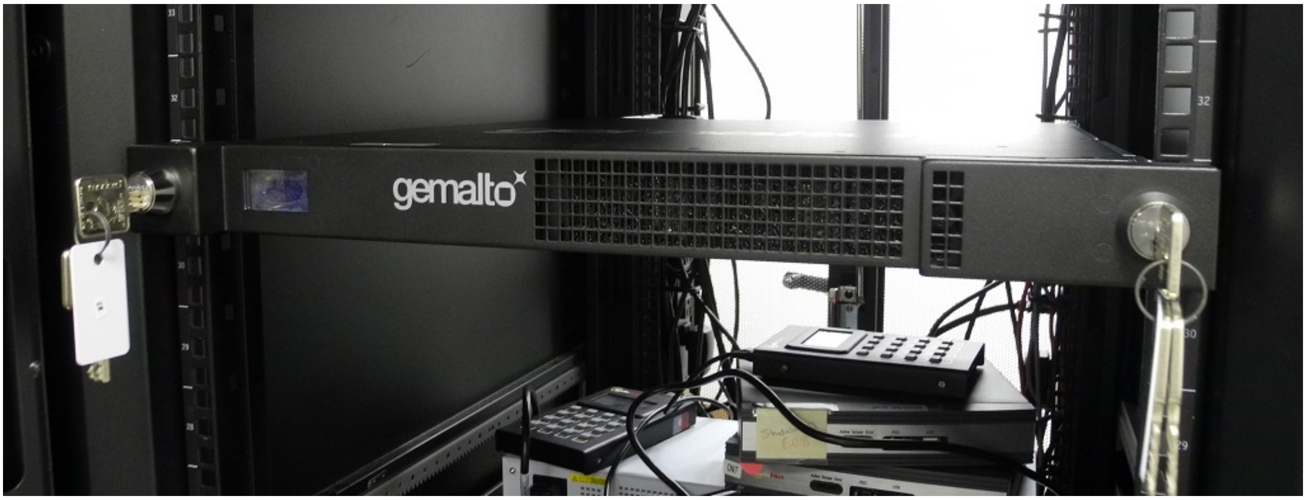
> **NOTE** The keys cannot be removed from the bezel when they are in the (horizontal) unlocked position.

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.

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

Replacement Keys

To obtain replacement keys, contact Technical Support (see "Support Contacts" on page 1). Please have the lock serial numbers ready. You can find these numbers on the bezel beneath each lock.

Power Consumption

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

Activity	Draw
Standby (connected to AC electrical mains but not powered on)	26W
Power-on Input Surge	15A
Active (under load from clients)	85W

All numbers are typical.

The SafeNet appliance has two power supplies, each rated at 350W, either of which is capable of running the system alone.

CHAPTER 2: Client Connections

This chapter provides information about client connections to the SafeNet Luna Network HSM appliance. It contains the following sections:

Connections to the Appliance - Limits

Here are the considerations, for a SafeNet Luna Network HSM appliance, regarding client registrations and connections.

Maximum number of clients I can register against one SafeNet Luna Network HSM appliance
No hard limit is set.

Maximum number of clients that can connect to one SafeNet Luna Network HSM appliance, at the same time
No hard limit is set, but see below.

Maximum number of connections per registered client
No hard limit is set, but see below.

Maximum number of connections, in total, to a single SafeNet Luna Network HSM appliance?
For SafeNet Luna Network HSM 5.2 and newer, no hard limit is set. SafeNet Luna Network HSM limits the number of connections according to system resources. We have verified that up to 1000 simultaneous connections can be established, in whatever combination of links per connected client. The number of simultaneous links that a given client might establish is dependent upon the application.

SafeNet Luna Network HSM Port Usage

The table below describes the SafeNet Luna Network HSM appliance's default port settings.

Port	Protocol	Feature	Configurable	Session Initiation
22	TCP	Secure Shell (SSH)	Yes	inbound
123	UDP	Network Time Protocol (NTP)	No	outbound
161 / 162	UDP	Simple Network Management Protocol (SNMP)	Yes	outbound
514	UDP	Remote Syslog Service	Yes	outbound
1503	TCP	Remote PED multi-factor authentication	Yes	inbound / 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 / outbound

* Applications use the client connection to obtain service from the HSM. Service is available only to client systems that are registered with HSM partitions.

SafeNet Luna Network HSM Appliance Port Bonding

SafeNet Luna Network HSM 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 SafeNet Luna Network HSM. 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" on page 1 in the *LunaSH Command Reference Guide* 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. Use the command "network interface bonding config" on page 1 to 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.

2. Use the command "network interface bonding enable" on page 1 to enable the bonded interface.

Client Startup Delay Across Mixed Subnets

Where a client computer and SafeNet Luna Network HSM 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 SafeNet Luna Network HSM, an error is logged.

When both SafeNet Luna Network HSM and client are on the same subnet, the connection occurs without delay.

SSH Public-Key Authentication

In its default configuration, the SafeNet 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 SafeNet 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 SafeNet 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 (**scp**) to the SafeNet appliance.

2. SSH to the SafeNet appliance and verify that the default functionality is a password prompt:

```
[root@mypc /]# ssh admin@myLuna
admin@myLuna's password:
```

3. Now, **scp** the client's public key to the appliance:

```
[root@mypc /]# scp /root/.ssh/id_rsa.pub  admin@myluna:
admin@myluna's password:
id_rsa.pub           100%
 |*****************************|   220        00:00
```

4. On the SafeNet Luna Network HSM appliance, verify the default settings of the Public Key Authentication service:

```
[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:

```
[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):

```
[myLuna] lunash:>my public-key add id_rsa.pub

Command Result : 0 (Success)
```

7. Check the list again:

```
[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
SafeNet 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:

```
[myLuna] lunash:>sysconf ssh publickey disable

 Public key authentication disabled

 Command Result : 0 (Success)

[myLuna] lunash:>sysconf ssh show
```

```
    SSHD configuration:

    SSHD Listen Port: 22 (Default)

    SSH is unrestricted.
    Password   authentication is enabled
    Public key authentication is disabled

   Command Result : 0 (Success)
```

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 SafeNet 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 SafeNet Luna Network HSM 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 SafeNet Luna Network HSM 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 SafeNet Luna Network HSM as the new user. You are prompted to change the default password.
- Transfer (**scp**) the SSH pubkey to the SafeNet appliance using the new user account (example $ scp id_rsa_pub op-number1@lunasa6:).
- Log in with the new account.
- Add your SSH key (lunash:>my public-key add …)

Here is an example session:

```
operator@mypc:~/.ssh$ scp id_rsa.pub op-number1@lunasa6:
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
SafeNet 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)
```

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 (with **ntls bind**)

In all other circumstances, NTLS should remain running. If there are problems with clients connecting to the SafeNet 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 SafeNet 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 a **service restart ntls** on a live, or production SafeNet 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 SafeNet appliance. This occurs under the following circumstances only:

- As part of original installation and setup.
- If you have reason to suspect that the SafeNet 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.

NTLS (SSL) Performance Issue

For modern HSM appliances, NTLS uses 2048-bit client/server certificates for client connections, rather than the 1024-bit certs that were considered secure in the past.

This larger certificate size requires more overhead/system resources than before. For a single connection or just a few simultaneous connection setups, the increased overhead is insignificant.

However, in a stress environment where (say) hundreds of concurrent connections are launched at once, you might see connections fail. The appliance attempts to get to all the incoming requests, but inevitably experiences delay on some. It eventually does get to all the session-open requests, but in a very intense flurry of session-opening, it might be returning responses to a given client after that client has timed out some of its own requests.

Once connections are set up, they can remain open and working with no problem up to the limit allowed by the appliance - 800 concurrent connections.

Workaround

Ensure that your application does not attempt to open hundreds of client connections all at the same time (space the setups over time - the problem is not how many sessions are open, but how many are in the startup process at the same time).

Or if high-volume simultaneous launch of sessions from a single client is unavoidable, then increase the receive timeout value (at the client) from the default 20 seconds to some larger value that eliminates the problem for you.

The obvious trade-off is that the higher the receive timeout value is set on each client, the longer it takes for failed connection attempts to be recognized and corrective measures to be taken.

Timeouts

Your network connections will timeout after a period of inactivity, as described below.

SSH Timeout

SSH connections to the appliance are cleaned up and torn down when no network activity has been detected for 15 seconds. This timeout is not configurable. If your session times out, you must open a new SSH session.

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 Gemalto 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 chrystoki.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 SafeNet Luna Network HSM client will wait for a response from the SafeNet Luna Network HSM 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 SafeNet Luna Network HSM deployments (such as SafeNet Luna HSMs in an HA configuration) where a quicker determination of the health of the SafeNet Luna Network HSM system is required. This value can be set in the SafeNet Luna Network HSM 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 3: Users and Passwords

The HSM has its own access controls and identities, which are covered in the *HSM Administration Guide* and in the *Configuration Guide*. This chapter deals with the various identities that access, observe, and control the networked appliance surrounding the HSM. The groups can overlap, to greater or lesser degree, reporting to different organizations within your overall enterprise.

This chapter contains the following sections:

HSM Login [PED-Authenticated]

Before you can create HSM Partitions, perform an HSM backup, or perform other administrative functions on the HSM, you must login to the SafeNet Luna Network HSM as HSM Admin, which requires you to first login at the command line as appliance "admin".

1. Connect to a command-line session, either via an SSH link or via a local serial terminal.
2. At the appliance "login as:" prompt, type "admin" and press **Enter**.
3. At the password prompt, type your admin password (for appliance admin, not HSM Admin) .
4. When the LunaSH (lunash:>) prompt appears, type the **hsm login** command:

   ```
   lunash:> hsm login
   ```

5. For a SafeNet Luna HSM with Trusted Path Authentication, there is no password to type. Instead, the Luna PED now prompts you to respond with the blue (HSM Admin) PED key.
6. Insert the appropriate blue PED key (the one that you imprinted when you first initialized this HSM, or one of your duplicates of it) and press **Enter** on the PED keypad. If a PED PIN (optional) was previously set, enter it at the prompt.
7. Login is complete. You may perform HSM administration/maintenance tasks.

Roles

SafeNet Luna HSM products offer multiple identities, some mandatory, some optional, that you can invoke in different ways to map to roles and functions in your organization.

The following topics offer some aspects that you might wish to consider before committing to an HSM configuration:

- "Named Administrative Users and Their Assigned Roles" on the next page

- "Custom User Roles" on the next page
- "Custom NTLS Registration Role" on page 44
- "Implications of Backup and Restore of User Profiles" on page 46
- "Security of Shell User Accounts" on page 46

Named Administrative Users and Their Assigned Roles

Default Users

By default, the appliance has:

- One 'admin' user, with role "admin", always enabled, default password "PASSWORD"
- One 'operator' user, with role "operator", disabled until you enable, default password "PASSWORD"
- One 'monitor' user, with role "monitor", disabled until you enable, default password "PASSWORD"
- One 'audit' user, with role "audit", disabled until you enable, default password "PASSWORD"

Those four built-in accounts can be neither created nor destroyed, but 'admin' can enable or disable the others as needed. For a list of commands accessible to the default user roles, see "LunaSH Command Summary" on page 1 in the *LunaSH Command Reference Guide*.

Additional Users

You can leave the default arrangement as-is, or you can create additional users with names of your own choice, and assign them any of the roles (and the powers that go with those roles). The default password of any created user is "PASSWORD" (all uppercase).

Thus, you could choose to have:

- Multiple admin-level users, each with a different name, that can perform most actions that the original admin can perform.
- Multiple operator-level users (or none, if you prefer), each with a different name, that have access to a reduced set of administrative commands.
- Multiple monitor-level users (or none, if you prefer), each with a different name, that are restricted to using commands that view, list or show.
- Multiple audit-level users (or none, if you prefer), each with a different name, that are restricted to HSM audit logging functions. See "Audit Logging " on page 1 for more information on this specialized role.

User Naming Guidelines

Administrative users' names can be 1-32 characters, chosen from letters a-z, or A-Z, numbers 0-9, the dash, the dot, or the underscore.

No spaces are allowed. User names cannot start with a dot, dash, or number.

As with any secure system, no two users (regardless of role) can have the same name.

Why Create Extra Administrative Users?

One reason for creating multiple named users would be for the purpose of distinguishing individual persons' activities in the logs.

For example, a user named 'john' running the LunaSH **syslog tail** command would show in the April 13 log as:

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

Command Result : 0 (Success)
```

Perhaps you have people performing similar functions at physically separate locations, or you might have staff assigned to teams or shifts for 24-hour coverage. It could be valuable (or required by your security auditors) to know and be able to show which specific person performed which actions on the system.

Custom User Roles

Named roles can be customized to have access to a specific subset of commands, allowing unique task delegation that suits organizational needs.

The custom role is defined by a list of the LunaSH commands that it can run. The role can be applied to and removed from any existing user to give them access to only the commands they require for a particular operation. This ensures that a given user does not obtain access beyond their security clearance. See "LunaSH Command Summary" on page 1 in the *LunaSH Command Reference Guide* for a list of commands.

To import, add, or remove a custom user role to your HSM and its users, see the following commands in the *LunaSH Command Reference Guide*:

- "user role import" on page 1
- "user role add" on page 1
- "user role delete" on page 1

Role Naming Guidelines

Role names can be 1-64 characters, chosen from letters a-z, or A-Z, numbers 0-9, the dash, the dot, or the underscore.

No spaces are allowed. User names cannot start with a dot or dash. 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.

To create a custom 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).

   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** (Windows) or **scp** (Linux/UNIX). You require the SafeNet Luna Network HSM appliance admin password to complete this step. The file is automatically placed in the appropriate directory on the appliance. Do not specify a target directory.

<table>
<tr><td><b>Windows</b></td><td><b>Syntax: pscp</b> [options] <source_filename> <user>@&lt;host&gt;<b>:</b>[&lt;target_filename>]
<b>Example:</b>To copy the role definitionfile (<b>myrole.txt</b>) to the myLuna appliance, keeping the same name:<pre>pscp myrole.txt admin@myLuna:
admin@myLuna's password: ********
myrole.txt | 1 kB | 1.1 kB/s | ETA: 00:00:00 | 100%</pre></td></tr>
<tr><td><b>Linux/UNIX</b></td><td><b>Syntax:scp</b> [options] <source_filename> <user>@&lt;host&gt;<b>:</b>[&lt;target_filename>]
<b>Example:</b> To copy the role definition file (<b>myrole.txt</b>) to the appliance with IP 192.168.0.123, keeping the same name:<pre>scp myrole.txt admin@192.168.0.123:
admin@192.168.0.123's password: ********
myrole.txt | 1 kB | 1.1 kB/s | ETA: 00:00:00 | 100%</pre></td></tr>
</table>

3. Log into the appliance as the **admin** user.

4. Import the role definition file to create the role able to access the commands it lists:

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

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 a user:

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

Example

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 backup commands and not including restore commands. Then you would import the file to your HSM:

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

"backuprolefile" was successfully imported.

Command Result : 0 (Success)
```

After your file has been successfully imported, you can assign the role it defines to the user "Alex":

```
lunash:>user role add -username Alex -role backup

User Alex was successfully modified.

Command Result : 0 (Success)
```

Custom NTLS Registration Role

Creating NTLS links between a client and partition using the one-step method (see "Create a Network Trust Link - One-step setup" on page 1 in the *Configuration Guide*) usually requires administrative access to the SafeNet Luna Network HSM 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 custom 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
```

> **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" on page 1 in the *LunaSH Command Reference Guide* for the complete set of **client** commands.

2. Transfer the role definition file (registerclient.txt in the example below) to the appliance using **pscp** (Windows) or **scp** (Linux/UNIX).

Windows	**pscp registerclient.txt admin@**<server_host/IP>**:**
	`pscp registerclient.txt admin@192.168.0.123:`
	`admin@192.168.0.123's password: ********`
	`registerclient.txt
		1 kB	1.1 kB/s	ETA: 00:00:00	100%`

Linux/UNIX	**scp registerclient.txt admin@**<server_host/IP>**:**
	`scp registerclient.txt admin@192.168.0.123:`
	`admin@192.168.0.123's password: ********`
	`registerclient.txt
		1 kB	1.1 kB/s	ETA: 00:00:00	100%`

3. Log into 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 login as "register" with the default password of 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.

8. 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**

   See "clientconfig deploy" on page 1 for full command syntax.

Implications of Backup and Restore of User Profiles

The commands **sysconf config backup** and **sysconf config restore** allow 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 before the backup was made. This includes the set of users that existed when the backup was made, the passwords that users had at the time of the backup, and the enabled/disabled status of users at the time of the backup. 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 (therefore unable to perform their tasks); disabled users might be enabled (therefore re-granted access that was suspended); 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 backup, be sure to 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.

Security of Shell User Accounts

Both the SafeNet Luna Network HSM appliance and any computers that make network connections for administrative purposes should reside inside your organization's secure premises, behind well-maintained firewalls. Site-to-site connections should be undertaken via VPN, and attacks on the shell account(s) is not normally an issue.

However, if your application requires placing the SafeNet appliance in an exposed position (e.g., the DMZ and beyond), your shell account(s) may be vulnerable to attackers. It is your responsibility to ensure that you protect your sensitive data.

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

Changing Appliance Passwords

From time to time, you might have reason to change the various passwords on the appliance and HSM. This might be because a password has possibly been compromised, or it might be because you have security procedures that mandate password-change intervals.

Appliance Passwords

The command used to change the appliance password for a user is different for admin users and operator or monitor users.

Admin-Level Users

Users with Admin privileges can use the following command to change their own password or the password of other appliance users, including other admin-level users. The current password is not required to change a password. As a result, never leave a session unattended.

lunash:> **user password** <userid>

If you issue the command without specifying a userid, the password for the currently logged-in user is changed.

Operator or Monitor-Level Users

Users with operator or monitor privileges can use the following command to change their own password:

lunash>: **my password set**

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

HSMs and Partition Passwords

The above affects the password(s) for the appliance only, and does not affect the HSM or HSM partitions. See "About Changing HSM and Partition Passwords" on page 1, "Resetting Passwords" on page 1 and "Failed Logins" on page 1 for more information.

Forgotten Passwords/Lost Authentication

Recover from a forgotten password as follows.

Appliance Admin Password Recovery

If you forget your appliance admin password, you can reset by logging in to the special account called 'recover'. See "Recover or Reset the Admin Account Password" on page 50.

HSM Admin/Security Officer Authentication - No Recovery

If you lose the HSM Admin authentication (a password for SafeNet Luna HSMs with Password Authentication; the blue PED key for SafeNet Luna HSMs with Trusted Path Authentication) , you must re-initialize the HSM, which also zeroizes the HSM (the contents of the HSM become permanently unavailable, and must be replaced/regenerated after you re-initialize -- allowing anyone to change or reset the appliance admin password without knowing the current password would not be considered good security, thus we force zeroization of all HSM contents in such a situation (either you have lost access/authentication to your own data/keys and therefore don't care that they are erased, or an attacker is attempting to gain access and you want your data/keys made unavailable, and you want to be made aware that the attack has occurred).

> **NOTE** You can restore from a Backup HSM if you use the token's PED keys (answer **Yes** to the PED's "Reuse..." question, and **No** New Domain) when initializing the HSM.)

Partition Roles Authentication Recovery

The Partition SO authentication is under the same restrictions as the HSM SO with the added provisons:

- For SafeNet Luna Network HSM, the HSM SO cannot "reset" the Partition SO's password or blue PED key secret. For the HSM SO, any initialized partition is a "black box" that the HSM SO can create or destroy, but cannot access.
- All authentication-management actions in a partition must take place via a registered client connection, normally using the **role** commands of the LunaCM utility:
  - The Partition SO can modify their own password or blue PED key secret using the LunaCM **role changepw** command.
  - The Crypto Officer and Crypto User can modify their own authentication (password or black PED key secret or gray PED key secret, or challenge secret for applications) using the LunaCM **role changepw** command.
  - The Partition SO can reset the Crypto Officer's or the Crypto User's authentication using the LunaCM **role resetpw** command only if HSM policy 15: Enable SO reset of partition PIN is enabled.

Lost PED Key or Forgotten Password

Passwords

Go to the secure lockup (a safe, an off-site secure deposit box, other) where you keep such important information, read and memorize the password. Return to the HSM and resume using it.

PED keys

Retrieve one of its copies from your on-site secure storage, or from your off-site disaster-recovery secure storage. Make any necessary replacement copies, using Luna PED, and resume using your HSM(s).

If you have lost a blue PED key, someone else might have found it. Consider using **lunacm:>changepw** or **lunash:>hsm changepw**, as appropriate to invalidate the current blue key secret, which might be compromised, and to safeguard your HSM with a new SO secret, going forward. HSM and partition contents are preserved.

Lost PED Key or Forgotten Password and No Backup

Blue PED key or SO password

If you truly have not kept a securely stored written backup of your HSM SO Password, or for PED-authenticated HSM, your blue SO PED key, then you are out of luck. If you have access to your partition(s), immediately make backups of all partitions that have important content. When you have done what you can to safeguard partition contents, perform **hsm factoryreset**, followed by **hsm init** - this is a "hard initialization" that wipes your HSM (destroying all partitions on it) and creates a new HSM SO password or blue PED key. You can then create new partitions and restore contents from backup. Any object that was in HSM SO space (rather than within a partition) is irretrievably lost.

Red PED key or HSM/Partition domain secret

If you have the red PED key or the HSM-or-Partition domain secret for another HSM or Partition that is capable of cloning (or backup/restore) with the current HSM or Partition, then you have the domain that you need - just make a copy. Cloning or backup/restore can take place only between entities that have identical domains, so that other domain must be the same as the one you "lost".

If you truly have not kept a secured written backup of your HSM or partition cloning domain, or for PED-authenticated HSM, your domain PED key(s), then you are out of luck. Any keys or objects that exist under that domain can still be used, but cannot be cloned or backed-up or restored. Begin immediately to phase in new/replacement keys/objects on another HSM, for which you have the relevant domain secret(s) or red PED key(s). Ensure that you have copies of the red PED keys, or that you have a written record of any text domain string, in secure on-site and off-site backup locations. Phase out the use of the old keys/objects, as you have no way to protect them against a damaged or lost HSM.

Orange Remote PED key

You will need to generate a new Remote PED Vector on one affected HSM with **lunacm:>ped vector init** or **lunash:>hsm ped vector init** to have that HSM and an orange key (plus backups) imprinted with the new RPV. Then you must physically go to all other HSMs that had the previous (lost) RPV and do the same, except you must say **Yes** to the PED's "Do you wish to reuse an existing keyset?" question, in order to bring the new RPV to all HSMs. If you forget and say **No** to the PED's "...reuse..." question, then you must start over.

White Audit PED key

You will need to initialize the audit role on any affected HSM. This creates a new Audit identity for that HSM, which orphans all records and files previously created under the old, lost audit role. The audit files that were previously created can still be viewed, but they can no longer be cryptographically verified. Remember, when performing **Audit init** on the first HSM, you can say **Yes** or **No** to Luna PED's "Do you wish to reuse an existing keyset?" question, as appropriate, but for any additional HSMs that share that audit role, you must answer **Yes**.

Forgotten PED PIN

Forgetting a PED PIN is the same as not having the correct PED key. See above for options in each situation.

Once a PED PIN is imposed, it is a required component of role authentication unless you arrange otherwise. You can remove the requirement for a PED PIN on a given HSM role only if you are currently able to authenticate (login) to that role. For black PED keys, you can have the SO reset your authentication. For other roles not.

For blue PED keys, forgetting a PED PIN is fatal.

For red PED keys, forgetting the PED PIN is eventually fatal, but you can work in the meantime while you phase out your orphaned keys and objects.

Forgetting PED PINs for other roles, like losing their PED keys is just more-or-less inconvenient, but not fatal.

Forgotten which PED key goes with which HSM/Partition

See your options, above. The most serious one is the blue PED key or the PED PIN for the SO role. You have only three tries to get it right. On the third wrong attempt, the HSM contents are lost. Wrong attempts are counted if you present the wrong blue PED key, or if you type the wrong PED PIN with the right PED key.

For black User PED keys, and their PED PINS (if applicable) you have ten tries to get the right key or the right combination, unless the SO has changed from the default number of retries. If you are getting close to that maximum number of bad attempts, stop, and ask the SO to reset your partition PW.

For other PED keys, there is no restriction on re-tries.

Recover or Reset the Admin Account Password

The **recover** account is a limited-purpose account that has the permanent (or fixed) password "PASSWORD". The **recover** account's only purposes are:

- to reset the password of the **admin** user, if the **admin** password is lost/forgotten, or
- to reset the entire SafeNet Luna Network HSM appliance to blank condition (all passwords are reset, any contents [including any certificates] are erased and any partitions are removed).

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.

The **recover** account does not have the following:

- Lockout
- Password expiry
- Public key authentication (you cannot access **recover** via SSH anyway)
- SSH access
- Changeable password

> **CAUTION!** The exception to the "physical access to the appliance" statement is where you have your appliances connected to a "terminal server" that aggregates serial links and makes them accessible via telnet or similar. We do that in a test lab, where access control is not critical, and it can be very convenient when we are constantly setting up and tearing down appliances and HSM hosts for various test and verification scenarios. However, connection of your SafeNet appliances to a remotely accessible terminal server could expose an additional avenue of attack, and therefore we suggest that you always avoid allowing such a potential security opening in a production environment.

What to do if you ever forget or lose the admin password

1. Have the blue SO PED key available, and the Luna PED connected, powered on, and in Local PED-USB mode (see "Changing Modes" on page 1), for PED authenticated HSMs, or have the HSM password available for password authenticated HSMs.
2. Connect a serial terminal to the **serial console connector** on the SafeNet Luna Network HSM rear panel.
3. Login as **recover**.

```
myLuna login: recover
Password:
Last login: Fri May  4 15:42:31 on ttyS0

WARNING !!  The recover function will stop the network interface, disable SSH
            service, reset the admin password to the default and then
            force you to change admin password from default before restarting the
            network interface and SSH service.  Network interface and SSH service
            will be re-enabled and restarted only if the recover process is successful.

If you are sure you wish to continue, type 'proceed', otherwise hit ENTER to abort.
```

```
proceed
Proceeding ...

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

'hsm login' successful.


Stopping sshd:                                             [  OK  ]

Changing password for user admin.

You can now choose the new password.

The password must be at least 8 characters long.
The password must contain characters from at least 3 of the following 4 categories:
    - Uppercase letters (A through Z)
    - Lowercase letters (a through z)
    - Numbers (0 through 9)
    - Non-alphanumeric characters (such as !, $, #, %)

New password:
Retype new password:
passwd: all authentication tokens updated successfully.

Starting sshd:                                             [  OK  ]

Successfully performed admin password recovery. Exiting...
```

> **NOTE** If you have already initialized the HSM, then you are prompted for the HSM Security Officer credential. If you have not initialized the HSM prior to resetting the admin password, then no credential is required.

4. Login as **admin**. You are prompted to change the **admin** password.
5. Change the **admin** password.

If you believe that your SafeNet Luna HSM server 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

See the "Warning" text at the beginning of the recover dialog, above. 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.

CHAPTER 4: Timestamping – NTP and Clock Drift

This chapter describes how to maintain accurate time on the appliance by performing the following tasks:

- "Setting the Time Zone" below
- "Correcting Clock Drift Manually" on the next page
- "NTP on SafeNet Luna Network HSM" on page 55

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**

To set the time zone to...	Command
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 "NTP on SafeNet Luna Network HSM" 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 SafeNet Luna Network HSM.

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

   > **NOTE** The SafeNet Luna Network HSM 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**

NTP on SafeNet Luna Network HSM

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. SafeNet Luna Network HSM 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" on the next page. 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 57.

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 the previous page.

For command syntax, see "sysconf ntp" on page 1 in the *LunaSH Command Reference Guide*.

Connecting to a Public NTP Server

Connections to public NTP servers are unauthenticated and therefore less secure. See "Securing Your NTP Connection" on the next page 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 may take a few minutes to synchronize the NTP server. Checking immediately may 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.

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 **scp**'d to the SafeNet Luna Network HSM 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**

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

CHAPTER 5: System Logging

SafeNet Luna Network HSM 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 Overview" on page 1.

About System Logging

Logs are managed with the **syslog** commands (see "syslog" on page 1), 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** Syslog format is in accordance with RFC 5424. See "Syslog Introduction" on page 1 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
critical	Critical condition

Severity Keyword	Severity Description
err/error	Error condition
warn/warn	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.

Configuring System Logging

Logs are managed in LunaSH with the **syslog** commands (see "syslog" on page 1). 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 in LunaSH with **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 61

> "Exporting System Logs" on page 62

> "Deleting System Logs" on page 63

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:

Use **syslog period** (see "syslog period" on page 1). 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:

Use **syslog rotations** (see "syslog rotations" on page 1). 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:

Use **syslog rotate** (see "syslog rotate" on page 1). 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 58 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 63).

> **NOTE** This feature has software and/or firmware dependencies. See "Version Dependencies by Feature" on page 1 for more information.

To customize severity levels:

1. Set the severity level for the desired log type (lunalogs,messages,cron,secure,boot). See "syslog severity set" on page 1.

   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 (see "syslog show" on page 1).

   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 Monitoring Guide" on page 1 in the *Syslog and SNMP Monitoring Guide*. Syslog format is in accordance with RFC 5424.

To search the current rotation of system logs:

Use **syslog tail** (see "syslog tail" on page 1). 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" (see "syslog tail" on page 1).

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 (see "syslog tarlogs" on page 1).

   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 **scp/pscp** (see "SCP and PSCP" on page 1).

   >**scp admin@**<applianceIP>**:logs.tgz .**

3. If you have configured NTP, transfer the **ntp.log** file from the appliance to a client.

   >**scp 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:

Use **syslog cleanup** (see "syslog cleanup" on page 1).

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 SafeNet Luna Network HSM to a central syslog server on the network.

You can use the LunaSH **syslog remotehost** commands to specify the central syslog server (see "syslog remotehost" on page 1).

- "Configuring a Remote Syslog Server" on the next page
- "Customizing Remote Logging Severity Levels" on page 65

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 (see "syslog remotehost add" on page 1).

   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 syslog daemon or service to allow it to receive logs from your SafeNet Luna Network HSM appliance(s).

3. Optionally, confirm the remote logging settings (see "syslog show" on page 1).

   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 58 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 has software and/or firmware dependencies. See "Version Dependencies by Feature" on page 1 for more information.

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 (see "syslog severity set" on page 1).

   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 (see "syslog show" on page 1).

   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).

CHAPTER 6: Backing Up the Appliance Configuration

This chapter describes how to back up and restore the appliance configuration. You can backup and restore the appliance configuration to a file, or to an HSM.

Backing Up and Restoring Your Appliance Service Configuration

You can backup the configuration settings for the various services running on the SafeNet Luna Network HSM so that you can restore your configuration if necessary. The ability to backup and restore your appliance configuration assures that your clients will be able to connect to a restored appliance, and all services will function correctly, should that be required.

Backing up your current configuration

You can use the **sysconf config backup** command at any time to create a backup file that contains the current state of all service parameters configured on the appliance. You can create multiple backup files, and provide a description for each file, allowing you to backup and restore multiple different configurations. The backup files are stored on the file system by default. You can export them to the internal HSM or an external backup HSM. The following configuration settings are saved:

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

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:

```
[Net_HSM]lunash:>sysconf config list


Configuration backup files in file system:

Size        |  File Name                                      |  Description
--------------------------------------------------------------------------------------------------
16641       |  Net_HSM_Config_20120222_0556.tar.gz            |  Clients OracleTDE and WebSphere
16588       |  Net_HSM_Config_20120222_0558.tar.gz            |  Automatic Backup Before Restoring

Command Result : 0 (Success)
```

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.

Managing your 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 files, if desired.

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**. See "Backing Up the Appliance Configuration to the HSM" on page 71 for details.

Restoring configuration settings from a backup file

Use the **sysconf config restore** command to restore the configuration settings for a specific service, or for all services, from a configuration backup file. You must stop any services you wish to restore before performing the restore operation, and reboot the appliance for the changes to take effect. A new configuration backup file of the current configuration is created automatically when you perform a restore operation, allowing you to easily revert to the previous configuration, if necessary.

NOTE Check the new configurations before rebooting or restarting the services.

Example of Backing Up and Restoring Your Appliance Configuration

If we factory reset the configuration parameters, a snapshot backup is created automatically, but for this example we will explicitly create a configuration backup file.

1. Create a backup of current appliance configuration parameters.

```
[Net_HSM] lunash:>sysconf config backup -description Example backup

Created configuration backup file: Net_HSM_Config_20120222_0556.tar.gz

Command Result : 0 (Success)
```

2. Check the current state of a configuration parameter (users).

```
[Net_HSM] lunash:>user list
Users           Roles           Status          RADIUS
admin           admin           enabled         no
bob             monitor         enabled         no
john            admin           enabled         no
monitor         monitor         enabled         no
operator        operator        enabled         no

Command Result : 0 (Success)
```

3. Perform the factory reset of the chosen configuration parameter (users).

```
[Net_HSM] lunash:>sysconf config factoryReset -service users

WARNING !! This command resets the configuration of the selected service(s) to factory
defaults.
 Resetting services to factory defaults can affect connectivity and the operation of the HSM.
 If you are sure that you wish to proceed, then type 'proceed', otherwise type 'quit'.

> proceed
 Proceeding...
 Resetting service(s) to factory defaults:
 -----------------------------------------
 users : succeeded

Command Result : 0 (Success)


[Net_HSM] lunash:>sysconf appliance reboot

WARNING !!  This command will reboot the appliance.
           All clients will be disconnected.
If you are sure that you wish to proceed, then type 'proceed', otherwise type 'quit'
> proceed
Proceeding...
'hsm supportInfo' successful.
Use 'scp' from a client machine to get file named:
supportInfo.txt
Broadcast message from root (pts/1) (Wed Feb 22 08:00:41 2012):
The system is going down for reboot NOW!
Reboot commencing

Command Result : 0 (Success)
```

4. After the appliance returns from reboot, restart the SSH session and log in.

```
[Net_HSM] lunash:>
login as: admin
```

```
admin@192.20.10.202's password:
Last login: Wed Feb 22 05:44:39 2012 from 192.20.10.143
SafeNet Luna Network HSM 7.0 Command Line Shell - Copyright (c) 2001-2017 Gemalto, Inc. All
rights reserved.
*****************************************************
**                                                  **
**   For security purposes, you must change your    **
**   admin password.                                **
**                                                  **
**   Please ensure you store your new admin         **
**   password in a secure location.                 **
**                                                  **
**               DO NOT LOSE IT!                    **
**                                                  **
*****************************************************
Changing password for user admin.
You can now choose the new password.
A valid password should be a mix of upper and lower case letters,
digits, and other characters.  You can use an 8 character long
password with characters from at least 3 of these 4 classes.
An upper case letter that begins the password and a digit that
ends it do not count towards the number of character classes used.
Enter new password:
Re-type new password:
passwd: all authentication tokens updated successfully.
Password change successful.
```

The reset to factory appliance settings for the **users** parameter seems to have worked. Our "admin" password was reset to the default password "PASSWORD", and we had to apply a non-default password.

5. With that done, we can verify if additional aspects of the **users** parameters were also reset to factory spec.

```
[Net_HSM] lunash:>user list

Users           Roles           Status          RADIUS
admin           admin           enabled         no
monitor         monitor         enabled         no
operator        operator        enabled         no

Command Result : 0 (Success)
```

Notice that created users "bob" and "john" are gone, but the system-standard users "admin", "operator", and "monitor" persist. Both "operator" and "monitor" will have had their passwords reset to the default, as well.

```
[Net_HSM] lunash:>sysconf config list

Configuration backup files in file system:

Size         |  File Name                                |  Description
--------------------------------------------------------------------------------------------
16641        |  Net_HSM_Config_20120222_0556.tar.gz      |  testing-this

16588        |  Net_HSM_Config_20120222_0558.tar.gz      |  Automatic Backup Before Restoring

Command Result : 0 (Success)
```

6. The list of configuration backup files is unchanged. We can choose one and restore it.

```
[Net_HSM] lunash:>sysconf config restore -service users -file Net_HSM_Config_20120222_
0556.tar.gz
```

```
WARNING !!  This command restores the configuration backup file: Net_HSM_Config_20120222_
0556.tar.gz.
It first creates a backup of the current configuration before restoring: Net_HSM_Config_
20120222_0556.tar.gz.
If you are sure that you wish to proceed, then type 'proceed', otherwise type 'quit'.
> proceed

Proceeding...
Created configuration backup file: Net_HSM_Config_20120222_0606.tar.gz
Restore the users configuration: Succeeded
You must reboot the appliance 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)


[Net_HSM] lunash:>sysconf appliance reboot
WARNING !!  This command will reboot the appliance.
            All clients will be disconnected.
If you are sure that you wish to proceed, then type 'proceed', otherwise type 'quit'
> proceed

Proceeding...
'hsm supportInfo' successful.
Use 'scp' from a client machine to get file named:
supportInfo.txt
Broadcast message from root (pts/1) (Wed Feb 22 08:00:41 2012):
The system is going down for reboot NOW!
Reboot commencing

Command Result : 0 (Success)
```

7. After rebooting again, we are able to log in with our original "admin" password.

   Once again we check the list of users.

```
[Net_HSM] lunash:>user list

Users           Roles           Status          RADIUS
admin           admin           enabled         no
bob             monitor         enabled         no
john            admin           enabled         no
monitor         monitor         enabled         no
operator        operator        enabled         no
```

   We see that users "bob" and "john" have returned. We could also log in as "operator" and "monitor" and find that their chosen passwords have been restored.

8. Finally, ask for the list of system configuration backup files one more time.

```
[Net_HSM] lunash:>sysconf config list

Configuration backup files in file system:

Size        | File Name                                    | Description
----------------------------------------------------------------------------------------------
16641       | Net_HSM_Config_20120222_0556.tar.gz          | testing-this

16588       | Net_HSM_Config_20120222_0558.tar.gz          | Automatic Backup Before Restoring

16248       | Net_HSM_Config_20120222_0606.tar.gz          | Automatic Backup Before Restoring
```

```
Command Result : 0 (Success)

[Net_HSM] lunash:>sysconf config restore
```

We see that a new file was created (Net_HSM_Config_20120222_0606.tar.gz) before the restore operation, and the other files are intact.

Backing Up the Appliance Configuration to the HSM

You can protect a configuration setup against the possibility of appliance failure by exporting a backup snapshot 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 SafeNet Luna Network HSM appliance. This could be useful if a component failed in the appliance, you sent the appliance back to SafeNet for rework under the RMA procedure, received it back repaired, and then retrieved the file from your HSM to restore your appliance settings.
- An external HSM, such as a Backup HSM or token. 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 SafeNet appliances with a standard set of parameters applicable to your enterprise.

If you are exporting a configuration backup to a SafeNet Luna Network HSM, 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.

CHAPTER 7: Troubleshooting

This section attends to appliance-level problems and their solutions.

Failed Logins and Lockout on Appliance

In addition to the bad login responses at the HSM and partition level, for all SafeNet Luna HSMs (see "Failed Logins" on page 1), SafeNet Luna Network HSM also has the appliance-level authentication layer for admin, operator, monitor, auditor, and for any named users you have created.

The response pattern for those is all the same, and is limited by default SSH settings:

> If you initiate an SSH session against the appliance, and fail to respond to the prompts, the system waits for the 120-second grace period to run out, and expires the session. 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 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.

You can configure SafeNet Luna Network HSM to accept administrative connections (SSH) on only one Ethernet channel, and client (NTLS) connections on the other.

Due to the pace at which the appliance SSH service evaluates submitted passwords and then prompts for retry, it generally takes more than 15 seconds to submit six bad attempts in a session to reach the maximum permitted, causing the session to drop. Then, there is the individual session tear-down and restart time to consider, before new attempts can resume. These factors help to limit the pace of brute-force attacks, while still allowing timely recovery from mistyping or forgetfulness by an administrative user.

Appliance Hardware Function Troubleshooting

This section provides additional information by answering questions that are frequently asked by our customers.

We were configuring rack power for several SafeNet Luna Network HSMs - planning peak load, etc. When we re-connected rack power, not all the appliances came on.

Did you verify that they were all on before you removed rack power?

SafeNet Luna Network HSM is configured to return to its previous state on application of AC power. If the appliance was running, and power was removed, then when power is re-applied the appliance re-boots. If the appliance was not running when power was removed, then the appliance does not restart when power becomes available again, and you must manually toggle the appliance power switch.

What actions must I take to move a SafeNet Luna Network HSM appliance from one datacenter to another?

Each installation will have its own issues and peculiarities. For this discussion we will assume that both the SafeNet Luna Network HSM appliance and the application server - PKI, web, other - that is the main client of the SafeNet Luna Network HSM are being moved. Here are some common steps to consider:

- Change the IP address of the SafeNet Luna Network HSM
- Change/update any other IP dependencies that are configured on the SafeNet Luna Network HSM, such as NTP servers, Syslog servers, NTLS binding by IP, etc.
- On the client computer (PKI server, web server, other) change the IP address of the SafeNet Luna Network HSM as found in the client computer's crystoki.ini/chrystoki.conf file
- Regenerate certificates on both the SafeNet Luna Network HSM and the client computer(s), if you used IP addresses rather than hostnames (no name resolution configured)
- Delete the client from the SafeNet Luna HSM server
- Exchange the new certificates
- Re-register the client on the SafeNet Luna HSM server
- Re-assign the appropriate HSM partition to the client
- If the application is Windows-based and identical client/server computers (or complete clones) are not used in the new datacenter, then there might be some Windows issues to complete, such as making/updating registry entries, running **certutil -repairstore**, and so on
- Before you transport the SafeNet Luna Network HSM, place the appliance in Secure Transport Mode

Client Connections Troubleshooting

This section contains information for troubleshooting.

Messages During an SSH Session

If during an SSH session you see a message similar to the following example, do not be alarmed. The message originates from the operating system within SafeNet Luna Network HSM and is benign.

```
Message from syslogd@172 at Jun 18 03:14:44 ... kernel:
 Disabling IRQ #225
```