SafeNet Network HSM

Appliance Administration Guide

gemalto
security to be free

Document Information

Product Version	6.2
Document Part Number	007-011136-007
Release Date	18 December 2015

Revision History

Revision	Date	Reason
A	18 December 2015	Initial release.

Trademarks

Acknowledgements

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

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

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

This product uses Brian Gladman’s AES implementation.

Refer to the End User License Agreement for more information.

Regulatory Compliance

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

USA, FCC

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

(1) This device may not cause harmful interference, and

(2) This device must accept any interference received, including interference that may cause undesired operation.

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

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

- Reorient or relocate the receiving antenna
- Increase the separation between the equipment and receiver
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected
- Consult the dealer or an experienced radio/TV technician for help

Changes or modifications not expressly approved by SafeNet could void the user's authority to operate the equipment.

Canada

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

Europe

This product is in conformity with the protection requirements of EC Council Directive 2004/108/EC. Conformity is declared to the following applicable standards for electro-magnetic compatibility immunity and susceptibility; CISPR22and IEC801. This product satisfies the CLASS B limits of EN 55022.

Disclaimer

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

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

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

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

CONTENTS

PREFACE
About the Appliance Administration Guide

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

As an HSM Server, SafeNet Network HSM provides increased operational flexibility over traditional HSMs. The SafeNet 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) that allows the K6 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:

- "Appliance Hardware Functions" on page 12
- "Client Connections" on page 35
- "Users and Passwords" on page 45
- "Timestamping – NTP and Time Drift" on page 55
- "System Logging" on page 73
- "Backing Up the Appliance Configuration" on page 75

This preface also includes the following information about this document:

- "Customer Release Notes" on the next page
- "Gemalto Rebranding" on the next page
- "Audience" on the next page
- "Document Conventions" on page 9
- "Support Contacts" on page 10

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

Customer Release Notes

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

- http://www.securedbysafenet.com/releasenotes/luna/crn_luna_hsm_6-2.pdf

Gemalto Rebranding

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

Old product name	New product name
Luna SA HSM	SafeNet Network HSM
Luna PCI-E HSM	SafeNet PCI-E HSM
Luna G5 HSM	SafeNet USB HSM
Luna PED	SafeNet PED
Luna Client	SafeNet HSM Client
Luna Dock	SafeNet Dock
Luna Backup HSM	SafeNet Backup HSM
Luna CSP	SafeNet CSP
Luna JSP	SafeNet JSP
Luna KSP	SafeNet KSP

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

Audience

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

All products manufactured and distributed by Gemalto NV 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.

Format	Convention
[**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

Contact method	Contact	
Address	Gemalto NV 4690 Millennium Drive Belcamp, Maryland 21017 USA	
Phone	Global	+1 410-931-7520
	Australia	1800.020.183
	China	(86) 10 8851 9191
	France	0825 341000
	Germany	01803 7246269
	India	000.800.100.4290
	Netherlands	0800.022.2996
	New Zealand	0800.440.359
	Portugal	800.1302.029
	Singapore	800.863.499
	Spain	900.938.717
	Sweden	020.791.028
	Switzerland	0800.564.849
	United Kingdom	0800.056.3158
	United States	(800) 545-6608

Contact method	Contact
Web	www.safenet-inc.com
Support and Downloads	www.safenet-inc.com/support Provides access to the Gemalto Knowledge Base and quick downloads for various products.
Technical Support Customer Portal	https://serviceportal.safenet-inc.com Existing customers with a Technical Support Customer Portal account can log in to manage incidents, get the latest software upgrades, and access the Gemalto Knowledge Base.

1

Appliance Hardware Functions

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

- "Front-panel Display" below
- "System Behavior with Hardware Tamper Events" on page 14
- "Shutdown or Reboot" on page 23
- "Power Supply and Fan Maintenance" on page 24
- "HSM Emergency Decommission Button" on page 31
- "Power Consumption " on page 32
- "Frequently Asked Questions" on page 33

Front-panel Display

The SafeNet Network HSM front-panel LCD provides system status summary information, for example:.

Ver:6.0.0-xx

ISO 60

The top line of the display cycles through the current software version, followed by the currently assigned network interface device addresses. The bottom line shows the current system status (see table below). If there are no faults detected, the display indicates that the appliance is in service, condition code 0 (ISO 0). If one or more fault conditions have been detected, the display shows the most severe, until that condition has been corrected, then it displays the next most severe condition, 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. Therefore, if you have fixed a condition that caused an error, the display should clear the error indication within seconds. If the display continues to show the error message, then the condition may have re-occurred and you should investigate. The display summarizes the information that you can retrieve using various "show" commands in the SafeNet Shell (lunash).

Condition Codes

The following codes are currently implemented:

Condition Type	Code	Meaning	LunaSH command equivalent
ISO	0	In service Okay, no trouble	n/a
	55	In Service Okay, eth0 is offline. Please run 'network show' and 'service status network' for more information	network show
	60	In Service Okay, eth1 is offline. Please run 'network show' and 'service status network' for more information.	network show
	100	In Service Okay, SNMP subsystem is not running. Please run "service status snmp" for more information.	service status snmp
OOS	20	Out of Service - Please run "service status ntls" for more information. **Note:** Both the NTLS and STC services must be running for the appliance to be in service.	service status ntls
	25	Out of Service - NTLS is not bound to an ethernet device. Please run "service status ntls" and "syslog tail" for more information	service status ntls
	30	Out of Service - HSM subsystem has experienced one or more critical events. Please run "hsm information show" and "syslog tail" for more information.	hsm information show hsm show
	80	Out of Service - Please run "service status stc" for more information. **Note:** Both the NTLS and STC services must be running for the appliance to be in service.	service status stc
OFL	50	Off Line - Neither ethernet interface is connected to the network. Please run "network show" command and "syslog tail" for more information.	network show
IST	70	In Service with Trouble - The syslog subsystem is not running. Please run "service status syslog" and "syslog tail" for more information.	
	90	In Service with Trouble - SSH (secure shell) subsystem is not running. Please run "service status ssh" and "syslog tail" for	service status ssh

Condition Type	Code	Meaning	LunaSH command equivalent
		more information.	
	110	In Service with Trouble - Hard disk utilization is too high. Please run "syslog tarlogs" and then scp to remove older log files	status disk

Display Conventions

The front-panel displays two lines of 16 characters. When no error conditions are detected (in service okay), the display cycles through the network interface devices, showing the hostname and IP address of each device. Because the display width is limited to sixteen characters, some information may span both lines, especially information text at appliance power up. For the service status information, the LCD scrolls the codes if there are more than can fit on a single line (e.g., OFL 50,20,100, →OFL 50,20,100,55, →OFL 20,100,55,60 →OFL 100,55,60).

System State	Expanded Description
ISO	In this service state the appliance is online and the necessary subsystems are operational. The appliance is providing encryption/signing services as expected.
IST	In this service state the appliance is online and the necessary subsystems are operational. The appliance is able to provide encryption/signing services but not necessarily to the fully expected level.
OFL	In this service state the appliance is not currently connected to the ethernet network and cannot provide service.
OOS	In this service state the appliance is online but the necessary subsystems are NOT operational. The appliance is NOT providing service.

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 24 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 31 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)	
hsm srk enable	Move one split of the MTK out of the HSM, and onto a purple PED Key, so the MTK cannot be reconstituted until/unless the external split (SRK) is presented.
hsm srk transportMode enter	Delete the MTK so HSM contents cannot be decoded or used.
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.

Action	Result/State
hsm login	No, can't do that either: LUNA_RET_MTK_ZEROIZED
hsm srk transportMode recover	Present the correct purple PED Key when prompted by the PED; the SRV is read into the HSM, allowing the MTK to be reconstituted, and making the HSM contents available/usable once more. 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 screw driver)	The HSM stops responding as the vkd (HSM driver) times out [the command-line prompt is still available until you issue a command (like hsm srk show) 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	(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
[Stop/ Start] switch on the back panel	

when the system is back up, run
hsm srk show
	`[myluna1] lunash:>hsm srk show`
	`Secure Recovery State flags: ================================`
	`External split enabled:...yes`
	`SRK resplit required:.... no`
	`Hardware tampered:........yes`
	`Transport mode:.......... no`
	
	`Command Result : 0 (Success) [myluna1] lunash:>`

view the logs	The **hsm.log** shows events like:
	ERR: RTC: external tamper latched
	and
	TVK was lost due to tamper
	and
	RTC: tamper 2 signal
	and
	ERR: MTK: security function was zeroized for unknown reason
	
	These are all indications from various modules that a tamper event has occurred. They are visible after the system is restarted - the tamper event itself occurs too quickly to be recorded at the time, so it is noted when the HSM goes through its start-up sequence after system reboot.
	Many lines of logging occur when the HSM restarts, so it is necessary to specify more than the default 20 lines at the end of the log when you issue:
	syslog tail - logname hsm
	Try searching the last couple of hundred entries with:
	syslog tail -logname hsm -search tamper -e 200
	
	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)`

Action	Result/State

	`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)`
	
	`lunash:>`

hsm srk show	External Split Enabled .... yes SRK resplit required ....no Hardware Tampered ....yes Transport Mode ....no
hsm login	not permitted: LUNA_RET_MTK_ZEROIZED
hsm srk transportMode recover	Present the correct purple PED Key when prompted by the PED. The SRV is read into the HSM, allowing the MTK to be reconstituted, and making the HSM contents available/usable once more. Because this was a physical tamper, and not a deliberate setting of Transport Mode, the PED does NOT present the Transport Mode verification string. THIS (above) IS HOW YOU RECOVER FROM A PHYSICAL TAMPER EVENT.
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

hsm srk transportMode enter	Delete the MTK so HSM contents cannot be decoded or used.
hsm srk show	External Split Enabled .... Yes SRK resplit required ....No Hardware Tampered ....No

Action	Result/State
	Transport Mode ....Yes
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.

What if you have disabled external storage of one of the MTK splits (the SRK), and a tamper occurs?

hsm srk disable	If you already had the SRK split out to a purple PED Key, this command brings it back in, so that both splits of the MTK reside inside the HSM.
hsm srk show	Confirm that SRK is no longer in use. hsm srk show Secure Recovery State flags: ================================ External split enabled: ....no SRK resplit required: ....no Hardware tampered: ....no Transport mode: .... no Command Result : 0 (Success)
open	Nothing obvious happens, until the front-panel LCD text gets to

Action	Result/State
the fan bay to induce a tamper event	the part of the sequence where it can display "HSM Error".
run an HSM command	[myluna1] lunash:>hsm show Appliance Details: ================== Software Version: 5.1.0-25 Error: Unable to communicate with HSM. Please run 'hsm supportInfo' and contact customer support. Command Result : 65535 (Luna Shell execution) [myluna1] lunash:> The HSM is no longer responsive.
reboot by pressing the Stop/Start switch or by "sysconf appliance reboot"	Appliance stops. Appliance starts.

when appliance is back in operation, look at the hsm.log	`[myluna1] lunash:>syslog tail -logname hsm -search tamper -e 200`
	`2010 Nov 9 14:50:34 myluna1 local6 err oamp[2239]:`
	`  ERR: RTC: external tamper latched`
	`2010 Nov 9 14:50:34 myluna1 local6 info oamp[2239]:`
	`  INFO: RTC: tamper timestamp = 230143 min`
	`  (YYYY:MM:DD:hh:mm:ss = 0000:06:08:19:43:28.00)`
	`2012 Nov 9 14:50:34 myluna1 local6 info oamp[2239]:`
	`  INFO: RTC: tamper circuits re-armed 2012 Nov 9 14:50:34`
	`  myluna1 local6 err oamp[2239]: ERR: TVK was lost due to tamper`
	`Command Result : 0 (Success)`
	`[myluna1] lunash:>hsm srk show`
	`Secure Recovery State flags:`
	`=================================`
	` External split enabled: .. no`
	` SRK resplit required: .... no`

Action	Result/State

	`Hardware tampered: ........no`
	`Transport mode: .......... no`
	`Command Result : 0 (Success)`
	`[myluna1] lunash:>`
	The tamper event appears in the log, after the system reboots.

run "hsm show" and "syslog tail " to search the hsm log for recent tamper events	`lunash:>hsm show`
	`Appliance Details:`
	`==================`
	`Software Version: 5.1.0-25`
	`HSM Details:`
	`============`
	`HSM Label: myhsm`
	`Serial #: 700027`
	`Firmware: 6.2.1`
	`Hardware Model: Luna K6`
	`Authentication Method: PED keys`
	`HSM Admin login status: Not Logged In`
	`HSM Admin login attempts left: 3 before HSM zeroization!`
	`RPV Initialized: No`
	`Manually Zeroized: No`
	`Partitions created on HSM:`
	`==========================`
	`Partition: 700027008, Name: mypar1`
	`FIPS 140-2 Operation:`
	`=====================`
	`The HSM is NOT in FIPS 140-2 approved operation mode.`
	`HSM Storage Information:`
	`========================`
	`Maximum HSM Storage Space (Bytes): 2097152`
	`Space In Use (Bytes): 104857`
	`Free Space Left (Bytes): 1992295`
	`Command Result : 0 (Success)`
	`[myluna1] lunash:>`
	The HSM is back in operation, as it was before the tamper event.
	Both splits of the MTK were present on the HSM, so recombining them to reconstitute the MTK was automatic when the HSM was reset.
	No action is required to re-instate the HSM from the tamper.
	You are alerted that an event has happened by the HSM becoming unresponsive, forcing you to restart.
	You can confirm that the reason for the HSM problem was, in fact, a tamper event, by looking at the log.
	`[myluna1] lunash:>syslog tail -logname hsm -search tamper -e 200`
	`2012 Nov 9 14:50:34 myluna1 local6 err oamp[2239]: ERR: RTC: external`

Action	Result/State

	`tamper latched`
	`2010 Nov 9 14:50:34 myluna1 local6 info oamp[2239]: INFO: RTC: tamper timestamp = 230143 min (YYYY:MM:DD:hh:mm:ss = 0000:06:08:19:43:28.00)`
	
	`2012 Nov 9 14:50:34 myluna1 local6 info oamp[2239]: INFO: RTC: tamper circuits re-armed 2012 Nov 9 14:50:34 myluna1 local6 err oamp[2239]: ERR: TVK was lost due to tamper`
	`Command Result : 0 (Success)`
	`[myluna1] lunash:>hsm srk show`
	`Secure Recovery State flags:`
	`=================================`
	` External split enabled: .. no`
	`SRK resplit required: .... no`
	`Hardware tampered: ........no`
	`Transport mode: .......... no`
	`Command Result : 0 (Success)`
	`[myluna1] lunash:>`
	The tamper event appears in the log after the system reboots.

Carry on using the HSM and its partitions.	

Here is an example of hsm.log file entries following a tamper event. We performed several tampers over the space of a few minutes.

```
[myluna1] lunash:>syslog tail -logname hsm -search tamper -e 200
2012 Nov  4 14:21:18 GA1  local6 err  oamp[2240]: ERR:    RTC: external tamper latched
2012 Nov  4 14:21:18 GA1  local6 info  oamp[2240]: INFO:    RTC: tamper timestamp = 222861 min
(YYYY:MM:DD:hh:mm:ss = 0000:06:03:18:21:18.00)
2012 Nov  4 14:21:18 GA1  local6 info  oamp[2240]: INFO:    RTC: tamper circuits re-armed
2012 Nov  4 14:21:18 GA1  local6 err  oamp[2240]: ERR:    TVK was lost due to tamper
2012 Nov  4 14:21:18 GA1  local6 err  oamp[2240]: ERR:    MTK: security function was zeroized on
previous tamper event and has not been restored yet
2012 Nov  4 14:36:28 GA1  local6 err  oamp[2239]: ERR:    RTC: tamper 2 signal
2012 Nov  4 14:36:28 GA1  local6 info  oamp[2239]: INFO:    RTC: tamper timestamp = 222881 min
(YYYY:MM:DD:hh:mm:ss = 0000:06:03:18:41:00.00)
2012 Nov  4 14:36:28 GA1  local6 info  oamp[2239]: INFO:    RTC: tamper circuits re-armed
2012 Nov  4 14:36:28 GA1  local6 err  oamp[2239]: ERR:    TVK was lost due to tamper
2012 Nov  4 14:44:35 GA1  local6 err  oamp[2245]: ERR:    RTC: tamper 2 signal
2012 Nov  4 14:44:35 GA1  local6 info  oamp[2245]: INFO:    RTC: tamper timestamp = 222888 min
(YYYY:MM:DD:hh:mm:ss = 0000:06:03:18:48:44.00)
2012 Nov  4 14:44:35 GA1  local6 info  oamp[2245]: INFO:    RTC: tamper circuits re-armed
2012 Nov  4 14:44:35 GA1  local6 err  oamp[2245]: ERR:    TVK was lost due to tamper
```

```
Command Result : 0 (Success)
[myluna1] lunash:>
```

As you can see, the search returns with several lines containing the keyword "tamper".

Note: if you run just 'syslog tail - logname hsm' without specifying a greater number of entries, the default is to show merely the last 20 lines of the file, which is usually insufficient to see if a tamper event has been recorded. Similarly, if you run 'syslog tail - logname hsm -search tamper', the search is run only on the default 'tail' sample. Not enough entries.

The Audit user is not able to view the hsm.log file.The audit user can view the audit logs which will contain similar event records, with different formatting.

To view a table that compares and contrasts various "deny access" events or actions that are sometimes confused, see "Comparison of Destruction/Denial Actions" on page 1in the *Administration Guide*.

Summary of Your Responses to Tamper Events

With No SRK

If you have a password-authenticated HSM, or if you have a PED-authenticated HSM that does not have the SRK stored externally, 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.

You can verify that the problem was actually a tamper by viewing the hsm.log.

With SRK on Purple PED Key

If you have a PED-authenticated HSM that **does** have the SRK stored externally, then only one split of the MTK resides 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 looks for both splits and must prompt you to supply the missing one from the purple PED Key, in order to reconstitute the MTK and go on operating normally. That is the additional intervention needed from you.

You can verify that the problem was actually a tamper by viewing the hsm.log.

Shutdown or 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 back panel of the system, or issue the `sysconf appliance reboot` command.

To switch off the system, you can issue the `sysconf appliance poweroff` command, or use the START/STOP switch on the SafeNet Network HSM back 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 back-panel START/STOP switch, which forces an immediate shutdown. This should **not** normally be required, and should never be done unless it is required, since it bypasses the normal, graceful file-system closing and shutdown procedure.

No Physical Access to SafeNet Network HSM Appliance

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 Network HSM, any risk is minimal, but not zero.
- The advantage of using the hardreboot 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 poweroff command, then it should remain 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 should restart 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 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 the situation and the condition of each PS.

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.

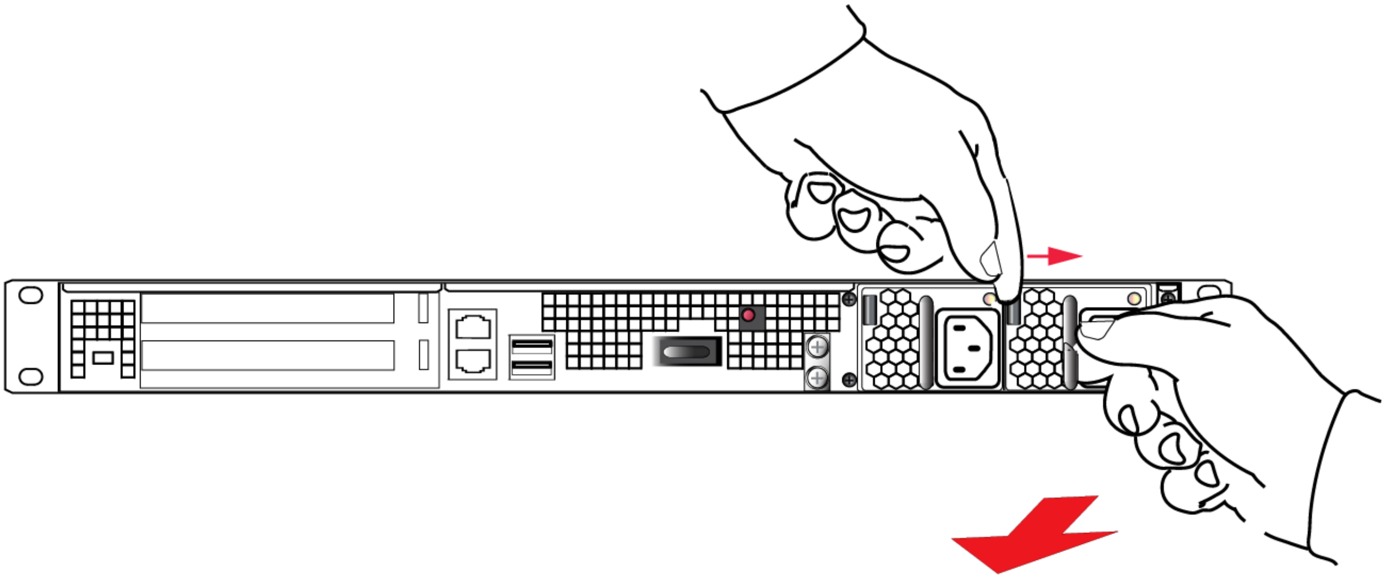
If only one power supply is present, the audible alarm is silent. If you wish to operate your SafeNet Network HSM appliance with only one power supply, we recommend that you remove the second supply to silence the audible alarm.

Replacing a Power Supply

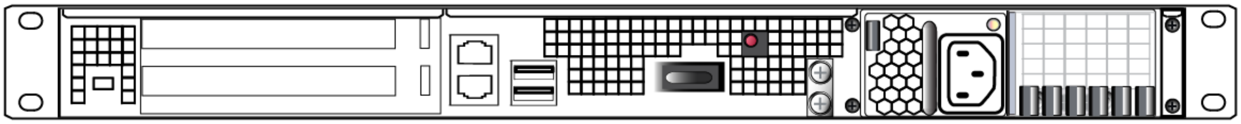
You may need to replace a power supply in the event of a failure.

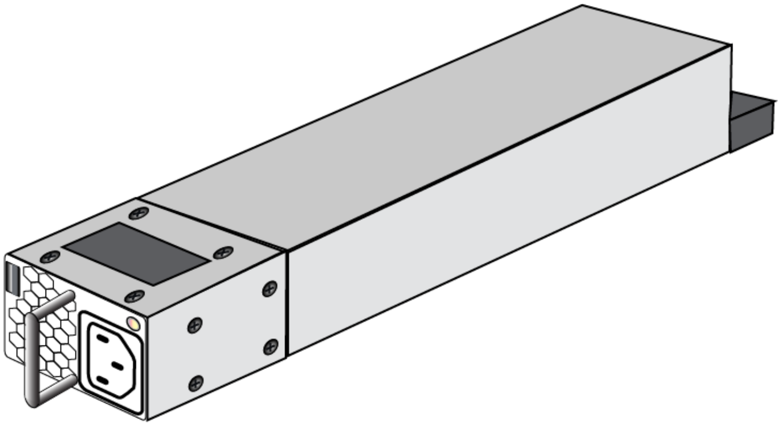
To remove a power supply

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)

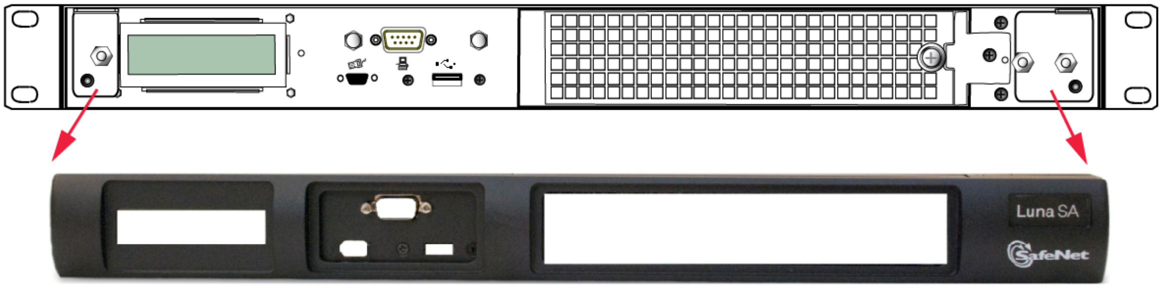
Here is a normal front-view of the SafeNet Network HSM appliance .

Removing the Front Bezel

The decorative front bezel is attached to the appliance by spring clips. It is not needed for appliance operation, meaning that you can remove the bezel while the appliance is operating, with no ill effect. However, if the appliance can be switched off (not currently in production/service), then the filter can be removed and cleaned more easily - less chance of knocking dirt into the airflow while handling the filter.

To remove the front bezel

1. First disconnect any cables that are connected to front-panel connectors (serial terminal, SafeNet PED, USB devices), then grasp the bezel near each end, and tug sharply toward you, while tipping it slightly downward. The bezel should come loose in your hands. Put it aside.



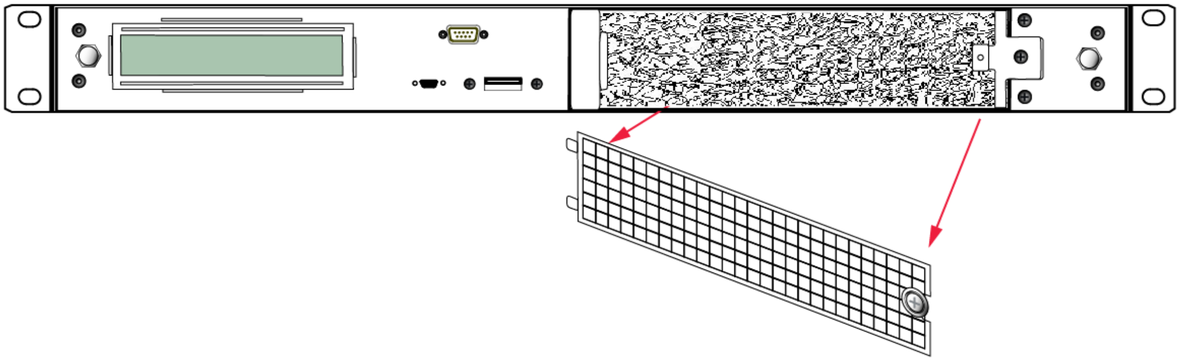
2. The ventilation grille, located to the right, on the appliance front panel, is secured in two parts, by two screws - a knurled, captive thumb-screw, and a Torx T8 screw. The knurled screw can be fastened or released without tools. It secures the lattice screen that in turn retains the mesh air filter.

Cleaning the 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.

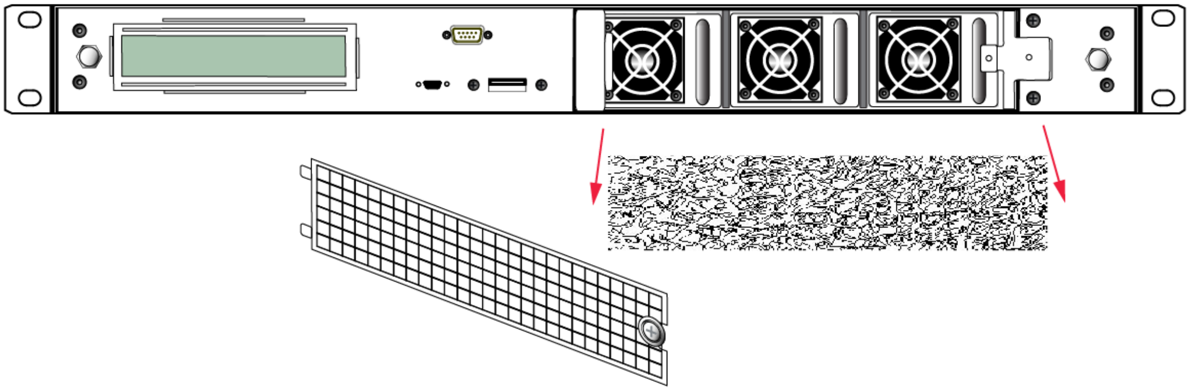
To clean the filter

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 Inr 0 RPM Unplugged or Failed

FAN1B Inr 0 RPM Unplugged or Failed

FAN2A OK 3000 RPM

FAN2B OK 2900 RPM

FAN3A OK 2900 RPM

FAN3B OK 3000 RPM
```

⚠ **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.

When the system returns from restarting, one of two scenarios applies, depending on your authentication method:

Password authenticated

If your HSM is password authenticated, or if your HSM is PED authenticated but it does not have "Store MTK Split Externally" set to **True**, then 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 "`partition activate -partition <name-of-partition>`" each of your HSM partitions before your clients can resume accessing them. That is, partition activation does not survive a tamper event.

PED authenticated

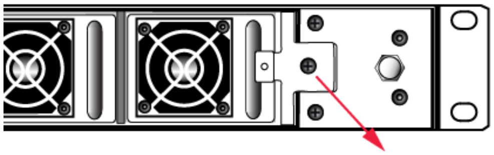
If your HSM is PED authenticated, and it does have "Store MTK Split Externally" set to **True**, then the HSM returns to find only one of the splits of the MTK available and it uses the PED to demand the other MTK split (the SRK) from your purple PED Key. When that is presented, the HSM reconstitutes the MTK, allowing you to resume operations.

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

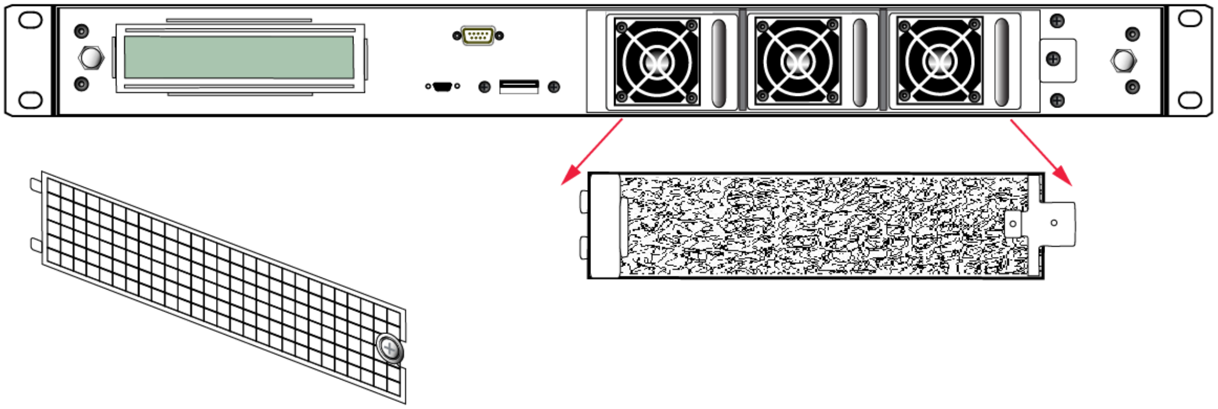
Note: Accessing the air filter mesh in front of the fans (using the thumbscrew to open the retaining grille) does not cause a tamper.

To replace a fan

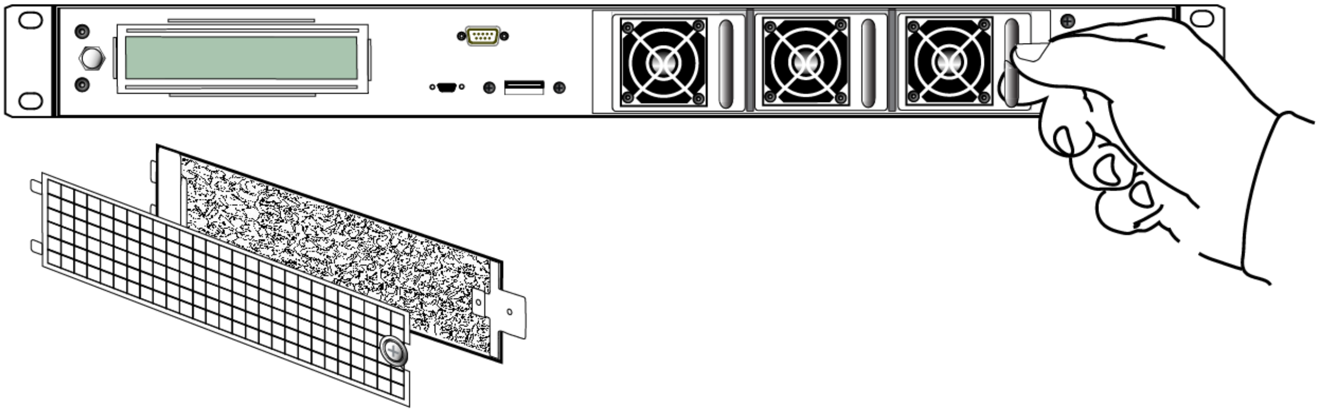
1. To open the fan bay, use a Torx number 8 screwdriver to remove the screw that secures the right-side tab of the fan retainer.



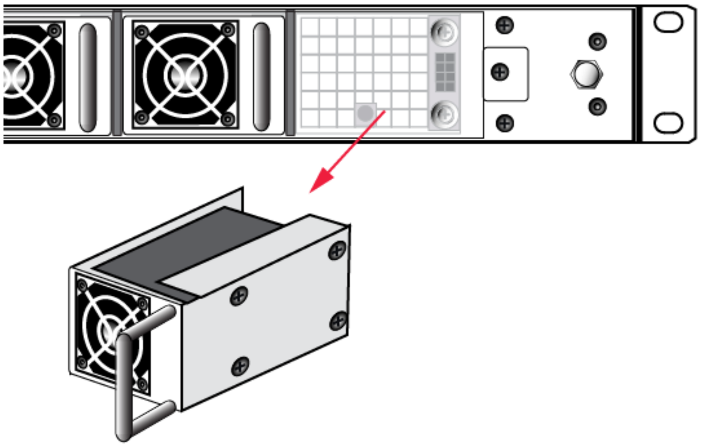
2. The fan retainer is anchored at its left by two tabs - swing the retainer out like a door, and remove it. There is no need to separate the filter mesh and its retainer from the larger fan retainer; the assembly can come out as one piece. The illustration below happens to show them separated.



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.

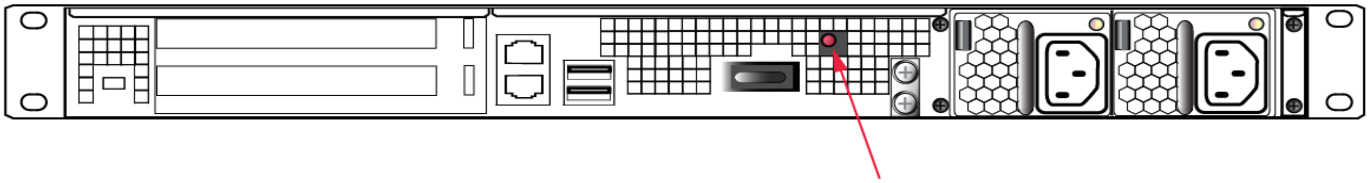
If you prefer these instructions illustrated by photographs, "Hardware Maintenance".

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, recessed behind the grille on the back 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 the button is pressed, the HSM is immediately decommissioned as the KEK is deleted from NVRAM. Without going into excessive detail about the HSM's internal workings, all security objects and user objects (your keys certificates, etc.) and general storage objects (cloning domain, etc.) are encrypted with their own subset storage keys (USK, GSK...), and those, in turn are encrypted with the Key Encryption Key (KEK - unique to each HSM). When the KEK is destroyed all objects on the HSM become permanently inaccessible and useless. They can still be seen, but they can never again be decoded - they are unrecoverable. Any cached data (such as partition activation data) are destroyed as well, gone, no trace.

After that happens, the HSM must be re-initialized before you (or your clients) can begin using it again. All contents of the HSM are lost.

To resume using your previous keys and certificates, you must restore them from a backup HSM - see SafeNet Remote Backup HSM.

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 hsm.log.
- The luna shell 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. "Destroy" action/event scenarios (Right-click the link if you prefer that it not open in a new window.)

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 SafeNet, 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 Network HSM is being returned to SafeNet

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

Power Consumption

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

Activity	Draw
Standby (connected to AC electrical mains but not powered on)	36W
Power-on Input Surge	15A
Idle (powered on but no demand)	100W
Active (under load from clients)	105W

All numbers are typical.

The SafeNet appliance has two power supplies, each rated at 450W, either of which is capable of running the system alone.

Frequently Asked Questions

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

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

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

SafeNet Network HSM is configured to return to 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 [re]start when power becomes available again, and you must manually toggle the appliance power switch.

What actions must I take to move a SafeNet 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 HSM server and the application server - PKI, web, other - that is the main client of the SafeNet HSM server are being moved. Here are some common steps to consider:

- change the IP address of the SafeNet HSM server
- change/update any other IP dependencies that are configured on the SafeNet HSM server, 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 HSM server as found in the client computer's crystoki.ini/chrystoki.conf file
- regenerate certificates on both the SafeNet HSM server and the client computer(s), if you used IP addresses rather than hostnames (no name resolution configured)
- delete the client from the SafeNet HSM server
- exchange the new certificates
- re-register the client on the SafeNet 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.

Failed Logins and Lockout on SafeNet Appliance

In addition to the bad login responses at the HSM and partition level, for all SafeNet HSMs (see "Failed Logins" on page 1), SafeNet 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 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.

2
Client Connections

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

Connections to the Appliance - Limits

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

What is the maximum number of clients I can register against one SafeNet Network HSM appliance?

No hard limit is set.

What is the maximum number of clients that can connect to one SafeNet Network HSM appliance, at the same time?

No hard limit is set, but see below.

What is the maximum number of connections per registered client?

No hard limit is set, but see below.

What is the maximum number of connections, in total, to a single SafeNet Network HSM appliance?

Previously, a hard limit of 800 connections was set for SafeNet Network HSM 4.x, SafeNet Network HSM 5.0, and SafeNet Network HSM 5.1.

For SafeNet Network HSM 5.2 and newer, no hard limit is set. SafeNet 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 Network HSM Port Usage

Here is how ports are used on the SafeNet Network HSM appliance, by default.

Standard Ports

Port Type	Port	Usage	Direction
TCP	22	SSH (Secure Shell) Network Access to appliance from client and/or remote workstations for administration	Bi-directional
TCP	1792	NTLS (Network Trust Link Service) Application traffic SafeNet Client Utilities cmu, vtl, your application(s), etc. [*]	Bi-directional
TCP	1503	RemotePED Only port that is configurable Establishing secure connection for a Remote PED Not applicable in a PWD based HSM	HSM to Remote Workstation/Client
TCP	5656	Secure Trusted Channel (STC) Application traffic SafeNet Client Utilities cmu, vtl, your application(s), etc. [*]. See "Secure Trusted Channel (STC)" on page 1 in the *Administration Guide* for more information.	Bi-directional

[* SafeNet Network HSM communicates with the SafeNet Client. Applications use the client connection to obtain service from the HSM. Service is available only to client systems that are registered with SafeNet Network HSM partitions.]

Additional Ports

Port Type	Port	Usage	Direction
UDP	514	Syslog Service Used to offload syslog to a remote syslog server	HSM to Syslog Server
UDP	123	NTP Service (Network Time Protocol)	HSM to NTP Server
UDP	161/162	SNMP Service (Simple Network Management Protocol)	HSM to SNMP Server

SafeNet Network HSM Appliance Port Bonding

SafeNet Network HSM has two physical interfaces: eth0 and eth1. They can be configured into a single virtual interface, bond0, for a round robin load balancing service on the two physical interfaces. 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.
- Use bonding only with static addressing. If you set bonding where dynamically allocated addressing is in use, then any future change in a DHCP lease would break interface bonding.
- Avoid executing bonding commands while clients are running applications against the SafeNet Network HSM. Where a bonding interface has the same IP as the IP of eth0, 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.

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

Once bonding is configured, client connections as well as SSH connections continue uninterrupted if either eth0 or eth1 fails.

Technical Details

SafeNet Network HSM uses the Linux Ethernet Channel Bonding Driver (v3.4.0-2) configured for link aggregation control protocol (LACP). Specifically:

- mode is active-backup
- primary is eth0
- primary_reselect is failure
- updelay is 2000
- miimon is 100

Additional details and descriptions of the above parameters can be reviewed in the document "Linux Ethernet Bonding Driver HOWTO" at https://www.kernel.org/doc/Documentation/networking/bonding.txt

(If your browser blocks pop-ups and new windows, copy and paste the link to the address field.)

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 virtual interface

1. Use the command "network interface bonding config" on page 1 to specify an IP address, subnet mask, and gateway for the bond0 interface.

Note: To avoid breaking the NTLS connection to the appliance, ensure that the IP address you specify for the bond0 interface is the IP address used for the current NTLS connection (either eth0 or eth1).

2. Use the command "network interface bonding enable" on page 1 to enable the bond0 interface.

Client Startup Delay Across Mixed Subnets

Where a client computer and SafeNet Network HSM are on different networks, any application (for example, our multitoken utility, or your client application program, etc) 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 Network HSM, an error is logged.

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

Using 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 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 pubic 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 Network HSM 6.0.0-42 Command Line Shell - Copyright (c) 2001-2015 SafeNet, 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 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 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 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@lunasa6's password:
id_rsa.pub                                     100%  392     0.4KB/s   00:00
operator@mypc:~$ ssh op-number1@lunasa6
op-number1@lunasa6's password:
Last login: Wed Mar  11 08:51:46 2015 from 192.168.10.18
```

```
SafeNet Network HSM 6.0.0-41 Command Line Shell - Copyright (c) 2001-2015 SafeNet, Inc. All
rights reserved.
[lunasa5] lunash:>my publickey add id_rsa.pub

Command Result : 0 (Success)
```

NTLS Keys in Hardware or in Software

In this context, "in hardware" means inside the HSM, while "in software" means on the appliance's hard disk, within the file system.

The default for SafeNet HSM appliances prior to SafeNet Network HSM 5 has been to have the securing keys for the NTLS link generated by the lunash command **sysconf regenCert**, and stored in the file system on the appliance's hard disk.

Moving into 'Hardware' (the HSM)

In SafeNet Network HSM 5.x and newer, it is also possible to create the ssl keys directly in the HSM and store them there, using the lunash command **sysconf hwRegenCert**.

A third option is to preserve software-created-and-stored keys and transfer them onto the HSM, using the lunash command **sysconf secureKeys**.

Either of the latter two options requires the creation of a special HSM partition named "Cryptoki User" to store those NTLS keys. This partition must be manually created with lunash command **partition create**.

Following creation or migration onto the HSM, the partition containing the NTLS keys must be activated with the lunash command **ntls activateKeys**.

You can verify if the system is using keys in hardware with the lunash command **ntls show**.

The keys in hardware feature creates a special container "Cryptoki User" to keep the RSA key pair for NTLS. Even though it shows in the partition list, this container is not meant to be managed by customers directly. Once it is created you should never to need touch this partition at all.

If sets of NTLS keys exist in both software (on the appliance's file system) and hardware (inside the HSM), only one set is valid and registered with clients.

Going Back to 'Software'

If you were using hardware secured (stored on the HSM) keys for your NTLS links between clients and appliance, and you decide to go back to using software-stored NTLS keys, you will need to generate new keys and certificates for NTLS, as you cannot move the existing NTLS keys from the "Cryptoki User" partition back to the appliance hard disk.

First, deactivate the "Cryptoki User" partition with the lunash command **ntls deactivateKeys**.

Then, remove the "Cryptoki User" partition with the lunash command **partition delete**.

Then, regenerate the NTLS keys and certificates in software with the lunash command **sysconf regenCert**.

Finally, restart NTLS with the lunash command **service restart ntls**.

Additional Notes

Most customers are expected to choose one option or the other (NTLS keys in HSM or NTLS keys on file system) and remain with that. Probably the only situation where you might encounter the above scenarios is in a lab, while trying the options before operational deployment.

If you deploy using one scheme, then wish to change at a later date by regenerating certificates (whether in hardware or in software), you must re-register all your clients with the new certificates.

If you migrate an existing set of keys from software (the file system) to hardware (the HSM), using **sysconf secureKeys**, you can carry on with your current registrations, because the NTLS keys have not changed. However, you do have to activate the NTLS partition and restart the service NTLS after any restart or power failure. [This is a limitation of having the NTLS private key in hardware. NTLS needs to open a session with a known appid that is already created and logged in by admin using **ntls activatekey** command. Every time the appliance reboots, the admin must issue the ntls command and restart NTLS before any NTL connections can be established between Clients and their working partitions.]

Item	**Keys in...**	
	Hardware (HSM)	**Software (hard disk)**
Security of NTLS keys	More	Less
Speed of link setup	Slower (more overhead - but little effect for client applications that set up a link, then perform many operations before link tear-down)	Faster (advantage to client applications that set up a fresh link for each operation, then tear down after the individual operation concludes - no advantage for long-duration links)
Speed ongoing	No advantage or disadvantage	No advantage or disadvantage
Convenience	Must swap keys with each client (registration) first time only. Afterward, you must activate the Cryptoki User partition and restart the service called NTLS following any system restart. Partition AutoActivation does not include the special Cryptoki User partition.	Must swap keys with each client (registration) first time only. Once the keys exist, the only task is to swap certificates with each client (registering), then no further link maintenance while the registrations are valid.

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.

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.

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-attach 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.

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 Network HSM and is benign.

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

Timeouts

As a general rule, do not adjust timeout settings (either via the interface or in config files) unless instructed to do so by SafeNet Customer 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.

If adjusting the configuration files for any reason:

⚠ **CAUTION:** Never insert TAB characters into the chrystoki.ini (Windows) or crystoki.conf (UNIX) file.

However, with the above said...

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 Network HSM client will wait for a response from the SafeNet 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 Network HSM deployments (such as SafeNet Enterprise HSMs in an HA configuration) where a quicker determination of the health of the SafeNet Network HSM system is required. This value can be set in the SafeNet 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>;
:
}
```

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 [Trusted Path]

Before you can create HSM Partitions, perform an HSM backup, or perform other administrative functions on the HSM, you must login to the SafeNet 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 HSM with Trusted Path Authentication, there is no password to type. Instead, the SafeNet 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 (duplicates are usually made for backup purposes, often for off-site secure storage, and may also be needed for operational reasons)] 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 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

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"

Those three "built-in" accounts can be neither created nor destroyed, but 'admin' can enable or disable the other two as needed.

You can leave that 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" (yes, all uppercase).

Thus, you could choose to have:

- multiple admin-level users, each with a different name,
- multiple operator-level users (or none, if you prefer), again each with a different name, and
- multiple monitor-level users (or none, if you prefer), each with a different name.

Administrative users' names can be a single character or as many as 128 characters, chosen from letters a-z, or A-Z, numbers 0-9, the dash, the dot, or the underscore. No spaces.

abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789-._

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

Abilities or Privileges of Created Users

Named users empowered with the "admin" role can perform most actions that the original admin can perform.

User accounts granted the "operator" role have access to a reduced set of administrative commands.

User accounts granted the "monitor" role can take no actions on the appliance or HSM, and are restricted to commands that view, list or show.

The commands available to the roles are listed in "User Accounts and Their Privileges".

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 : 172.20.10.133/3107
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.

You might find other uses. Please let us know.

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
- the enabled/disabled status of users, at the time of the backup.

This means that:
- 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 (therefor unable to perform their tasks)
- disabled users might be enabled (therefore re-granted access that was suspended) and
- any user accounts removed since that backup will be restored.

The first three could be administrative inconveniences. The fourth and fifth outcomes could be serious security issues.

Your records should indicate when user-profile changes were made, and what those changes were, so any time that 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

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

However, if your application requires placing the SafeNet appliance in an exposed position (the DMZ and beyond), then please see "About Connection Security" in the Overview document for some additional thoughts.

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

To change the password of a user, use the following command:

```
lunash:> user password [userid]
Changing password for user "admin"
New UNIX password
Retype new UNIX password
All authentication tokens updated successfully
Command result : (0) success
lunash:>
```

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

You are assumed to already know the current password (because you must be logged in as that user if you are issuing the command), so you are not prompted for the current password before being asked for the new one. Therefore, as an elementary security measure, never leave a logged-in session unattended.

Any user with the "admin" role can change that user's own password or another user's password, without knowing the other user's current password.

HSMs and Partitions

The above affects the password(s) for the appliance only, and does not affect the HSM or HSM partitions.

For those, see "About Changing HSM and Partition Passwords" and see "Resetting Passwords" .

Also, see "Failed Logins".

Forgotten Passwords

Recover from a forgotten password as follows:

Appliance admin

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 52.

HSM Admin / Security Officer

If you lose the HSM Admin authentication (a password for SafeNet HSMs with Password Authentication; the blue PED Key for SafeNet 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 [choose YES to the PED's "Reuse..." question, and NO New Domain] when initializing the HSM... yo do have all your important material backed up, don't you?)

Partition Owner /Partition User / Crypto Officer

If you lose the Partition Owner/User authentication, the HSM Admin or Security Officer can reset the password with command 'partition -resetPw'.

The HSM Policy "21: Force user PIN change after set/reset" determines whether the Partition User can access the Partition with the password that is set by "partition -resetPw", or if the User must explicitly set a new password with "partition changePw" before being allowed to access the Partition. That policy can be used to enforce role separation between SO and User.

Help! I have lost my blue/black/red/orange/purple/white PED Key or I have forgotten the password!

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

ANSWER-general (PED Keys): Retrieve one of the copies that we (and your security advisor/consultant) always advise you to make, from your on-site secure storage, or from your off-site [disaster-recovery] secure storage, make any necessary replacement copies, using SafeNet PED, and resume using your HSM(s).

If you have lost a blue PED Key, someone else might have found it. Consider `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.

But I don't have keys or secrets in secure on-site or off-site storage! What do I do?

ANSWER - 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 **do** have access to your partition(s), then immediately make backups of all partitions that have important content. When you have done what you can to safeguard partition contents, then 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.

ANSWER - black PED Key or Partition User password : If you truly have not kept a secured written backup of your partition User Password, or for PED-authenticated HSM, your black partition User PED Key, then log into your HSM as SO, and perform `partition resetPw`. The `partition changePw` action is done by a partition owner who has the current credential and wishes to change it, so that one is not available to you now. The `partition **reset**Pw` is done by the HSM SO when the current partition secret has been lost, or is compromised (perhaps by the unplanned departure of personnel). Select option 4 when you run the command.

lunash:> partition resetpw -partition mypar

Which part of the partition password do you wish to change?

1. change User or Partition Owner (black) PED key data
2. generate new random password for partition owner
3. generate new random password for crypto-user
4. both options 1 and 2

0. abort command

Please select one of the above options: 4

```
Luna PED operation required to reset partition PED key data - use User or Partition Owner (black) PED key.
****
'partition resetPw' successful.

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

**** Follow the PED prompts:

a. press [No] when asked “Would you like to reuse an existing keyset? (y/n)”

b. provide the M and N values of your choice ([1] and [1] if you don't want MofN)

c. press [Yes] to overwrite the user key

d. provide your choice of PED key PIN when prompted (or just press [Enter] if you do not wish to impose a PED PIN)

e. press [Yes] when asked “Do you want to duplicate the keyset? (y/n)”

f. write down the new random challenge from the PED screen (for best legibility, type it)

Now that you have the new partition authentication, you can change the PED-generated text challenge to something more to your liking via the `partition` **`changePw`** command, choosing option 3.

```
lunash:> partition changePw -partition mypar1

Which part of the partition password do you wish to change?

1. change partition owner (black) PED key data
2. generate new random password for partition owner
3. specify a new password for the partition owner
4. both options 1 and 2

0. abort command

Please select one of the above options: 3
> ****************

Please enter the password for the partition:
>********

Please enter a new password for the partition:
>********


'partition -changePw' successful.

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

ANSWER - red PED Key or HSM-or-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. You have no fall-back, in case of accident. Begin immediately to phase in new/replacement keys/objects on another HSM, for which you DO 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.

ANSWER - orange 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 that are intended to use Remote PED with the new orange PED Key(s). If you forget and say "No" to the PED's "...reuse..." question, then you are starting over.

ANSWER - 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. Only records and files that are created under the new audit role can be verified, in future. Remember, when performing Audit init on the first HSM, you can say "Yes" or "No" to SafeNet PED's "Do you wish to reuse an existing keyset?..." question, as appropriate, but for any additional HSMs that must share that audit role, you must answer "Yes" to "Do you wish to reuse an existing keyset?..."

ANSWER - purple PED Key : If SRK was not enabled, this is not a problem - any purple PED Keys you had for that HSM are invalid anyway. If SRK was enabled, then your options depend on whether the HSM is currently in a tamper condition or Secure Transport mode... or not. There is no way to recover from a tamper or from Secure Transport Mode if the external split of the Master Tamper Key (the SRK) is not available. If you haven't got a backup purple key, your HSM is locked the moment it experiences a tamper event, or if it was placed in Secure Transport Mode. The same applies if you do have the key, but have forgotten/lost a numeric PED PIN that you [optionally] applied when the purple key was imprinted with the Secure Recovery Vector (the external split of the MTK). Either way, you must obtain an RMA and return the HSM to SafeNet for remanufacture. All HSM contents are lost.

If the purple key is lost, BUT the HSM is still in working mode - that is, it has not experienced a tamper event, and you have not placed it in Secure Transport Mode - then you should immediately rescue any important HSM or partition contents by backing them up, and restoring onto another HSM (that does NOT have SRK enabled, or for which SRK is enabled, but you DO still have the purple key). Once that is accomplished, decommission the original HSM, obtain an RMA, and ship it back to SafeNet for re-manufacture. It is not safe to continue using an HSM that has SRK enabled, but for which you have lost the purple PED Key. Any tamper event would render contents irretrievable. Avoid putting yourself in such a situation.

I have my PED Key, but I forgot my PED PIN! What can I do?

Forgetting a PED PIN is the same as not having the correct PED Key. See above, for your options in each situation. A PED PIN is an [OPTION] that you decide, at the time a role is created. If your security regime/protocol demands that your HSM access must enforce multi-factor authentication, then a PED PIN is a useful/necessary option for you. If your security protocol does NOT demand such measures, then you should seriously consider whether it is justified.

Once a PED PIN is imposed, it is a required component of role authentication, until/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 (log in) to that role. For black PED Keys, you can have the SO reset your authentication. For other roles... not.

Thus, for blue or purple PED Keys, forgetting a PED PIN, like losing the PED Key (with no backups) 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 normally not fatal.

I have my PED Keys and my PED PINS, but I can't remember which one goes with which HSM (or 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. Good luck. Try to be better organized in future.

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 HSM server 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 login **only via the local serial connection**. The 'admin' user's account password can be changed remotely by anyone who already knows it, but the 'admin' user's password cannot be arbitrarily reset unless the person doing so has physical access to the appliance, to make the serial connection.

CAUTION: The exception to 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 SafeNet PED connected, powered on, and "Awaiting command..", for PED authenticated (FIPS 140-3) HSMs, or have the HSM password available for password authenticated HSMs.
2. Connect a serial terminal to the **serial console connector** on the SafeNet HSM server front panel.
3. Login as "recover".

```
 myluna login: recover
Password:
Last login: Wed Apr 13 10:21:37 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 ...
HSM is zeroized. Will proceed to recover admin password.
Stopping sshd:[ OK ]
Shutting down interface eth0: [ OK ]
Shutting down loopback interface: [ OK ]
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.
Bringing up lookback interface: [ OK ]
Bringing up interface eth0:
Determining IP information for eth0… failed.
[FAILED]
Bringing up interface eth1:
Determining IP information for eth1.. failed; no link present. Check cable?
[FAILED]
Starting sshd:WARNING: initlog is deprecated and will be removed in a future
release
[ OK ]
Successfully performed admin password recovery. Exiting …
```

Note: If you have already initialized the HSM, then you are prompted for the appropriate blue PED Key. If you have not initialized the HSM prior to resetting the admin password, then the default HSM SO authentication is used, from the SafeNet PED, and no PED Key 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 HSM server has not been compromised, you can resume using it as before (taking care to both remember and secure the 'admin' password).

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.

Note: 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.

Note: 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

4
Timestamping – NTP and Time Drift

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

Correct for time drift (non-NTP)

- "Correcting Time Drift" below

Configure NTP (network time protocol) or Secure NTP

- "NTP and Secure NTP on SafeNet Network HSM" on page 58
- "Example Using Simple NTP" on page 59
- "Using Secure NTP" on page 62
- "Example Using Secure NTP" on page 63

Timezone codes

- "Timezones and Timezone Codes" on page 65

Correcting Time Drift

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 to do so is to implement Network Time Protocol 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 the NTP topics of this Administration section, and in the Concepts section of this Help.

Some situations might not permit maintaining a constant connection to an external time-data source (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.

First, establish the drift that exists for your appliance

Begin drift measurement. This also sets the time.

Note: the SafeNet Network HSM appliance must run uninterrupted for several days to allow a time 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.

Issue the drift start command:

```
[myluna] lunash:>sysconf drift startmeasure -c 15:12:15
```

```
Setting the time to 15:12:15 and recording data for drift correction mechanism.
Current date and time set to: Tue Dec 9 13:47:45 EST 2008
Command Result : 0 (Success)
[myluna] lunash:>
```

At any time, you can check the status of the drift measurement to ensure it has not been interrupted:

```
[myluna] lunash:>sysconf drift status
Drift measurement started on: Tue Dec 9 13:47:45 EST 2008
Measurement has yet to be stopped.
Command Result : 0 (Success)
```

After issuing the start command, allow the system to run for several days before issuing the stop command. The appliance's drift system enforces a 3 day minimum - here's what it says if you attempt a shorter period:

```
[myluna] lunash:>sysconf drift stopmeasure -c 08:53:30
Measuring drift correction data on this appliance.
Drift measurement is not complete. This command must be run at least 3 days
after the 'sysconf drift start' command, in order to ensure accuracy of the
measurement.
```

It is up to you how you acquire an accurate time, in order to establish the drift and its correction. One method would be to use NTP on a different computer that has no connection to the SafeNet Network HSM. In this example we used a 4 day span. Issue the “stopmeasure” command with the current and accurate time:

```
[myluna] lunash:>sysconf drift stopmeasure -c 14:53:00
Measuring drift correction data on this appliance.
Storing measured drift of 8 seconds/day in internal configuration files.
Use the command 'sysconf drift init' to initialize drift correction.
Command Result : 0 (Success)
[myluna] lunash:>
```

The sysconf drift stopmeasure command stops the count and then compares the <currentprecisetime> that you typed in, against the calculated time (since you ran the sysconf drift startmeasure command). The difference in seconds, the total drift, is then divided by the interval over which the measurement was running, in order to calculate a drift-per-day value.

In order for the drift to be properly corrected for operation, it is best to initialize drift correction immediately after stopping the measurement cycle, otherwise it might be necessary to redo the measurement. Note that the drift time stored is the time reported when measurement was stopped.

```
[myluna] lunash:>sysconf drift init -c 14:58:15
Measuring drift correction data on this appliance.
Setting the time to 14:58:15 and initializing drift correction of 8 seconds per day on this
appliance. The time will be adjusted daily to compensate for this drift.
Use the command 'sysconf drift reset' to disable drift correction.
Date and time set to: Fri Dec 12 14:58:15 EST 2008
Command Result : 0 (Success)
[myluna] lunash:>
```

For this example, we allow the system to run for a few more days and check the time to ensure the correction is maintained. To ensure that drift correction is still in effect, use the sysconf drift status command in addition to status time.

```
[myluna] lunash:>sysconf drift status
Drift measurement started on: Tue Dec 9 13:47:45 EST 2008
Measurement stopped on: Tue Dec 9 13:47:45 EST 2008
Current drift correction is: 8 seconds per day
(Note that drift correction may be manually set.)
Command Result : 0 (Success)
```

For purposes of example, set the drift rate manually to ensure that it is also effective:

```
[myluna] lunash:>sysconf drift set
Enter the value to be used for drift (in seconds per day): 8
This value will overwrite the previous value of the drift that may have
been measured. If you are sure that you wish to overwrite it, then type
'proceed', otherwise type 'quit'
> proceed
Proceeding...
NOTE: The new value will not take effect until 'sysconf drift init' is run.
Command Result : 0 (Success)
[kuso] lunash:>sysconf drift init -c 09:11:45
Measuring drift correction data on this appliance.
Setting the time to 09:11:45 and initializing drift correction of
8 seconds per day on this appliance. The time will be adjusted daily
to compensate for this drift.
```

Use the command 'sysconf drift reset' to disable drift correction.

Date and time set to: Mon Dec 15 09:11:45 EST 2008

Command Result : 0 (Success)

[myluna] lunash:>

In a lab situation, this should sit for at least 3 days to ensure that the drift correction is effective.

NTP and Secure NTP on SafeNet Network HSM

Left to their own devices, all computer/hardware clocks are subject to some drift. These changes occur slowly and are usually small, but can be nevertheless significant in many applications. Thus it is desirable to be able to synchronize the appliance's internal clock with a known-to-be-accurate source of time information. Network Time Protocol (NTP) provides a means whereby your appliance (or any other network-connected digital device) can receive time signals from extremely accurate servers of time data.

Network Time Protocol (NTP) by default does not authenticate NTP servers. NTP version 3 provides an authentication option using symmetric keys shared between NTP clients and servers.

NTP version 4, in addition to supporting NTP v3 symmetric key authentication provides a public key authentication mechanism called ‘Autokey’. These authentication mechanisms enable NTP clients (SafeNet Network HSM) to authenticate trusted NTP servers. NTP servers do not authenticate clients.

SafeNet Network HSM can be configured as an NTP client, not sever or peer. Also Multicast and Manycast are not supported in SafeNet Network HSM at this time. A page of the Administration & Maintenance section of this Help explains configuring NTP authentication ("Example Using Secure NTP" on page 63) in SafeNet Network HSM using LunaSH (lunash:>) commands. The available configuration commands are described in the Reference section of this Help, under "Lunash Appliance Commands > sysconf Commands > sysconf ntp Commands" ( ).
For more information about NTP authentication please refer to the NTP v4 documentation [1][2].

SafeNet Network HSM uses NTP v4 (4.2.6p2) and supports both symmetric and public key authentication as described below. Compared with legacy SafeNet Network HSM implementation, new LunaSH(lunash:>) commands have been added and some of the previously-used commands (pre-2009) have been modified.

Using NTP authentication in SafeNet Network HSM requires NTP servers which have been properly configured to support authentication. Configuring NTP servers is beyond the scope of this document. For information about configuring NTP servers please refer to the standard NTP documentation [1][3].

Standard, non-secure NTP is available from a variety of public sites. For greater security and control, your organization might have established its own secure NTP server(s) or might have entered into agreement with a trusted supplier of secure NTP service. Contact your local IT manager or security officer for the particulars.

The short description is that you

- make note of the parameters of the certificate that the server provides, then
- configure your SafeNet Network HSM to use that NTP server and to accept the server's authentication certificate as identified by the parameters that you previously recorded (key ID, size, fingerprint, etc. as appropriate), and
- have your SafeNet Network HSM begin using the time signal supplied by that secure NTP server.

What If I Can't Use NTP?

NTP is the most reliable and straightforward way to correct the time-drift inherent in computer systems, but your situation might preclude that solution. An alternate method of establishing and correcting the drift on your HSM appliance is to use the on-board drift-correction commands ("Correcting Time Drift" on page 55).

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

Example Using Simple NTP

The following is an example of using simple or standard (non-secured) NTP on SafeNet Network HSM. We recommend that you use secure NTP, instead. This example is provided for comparison.

Enable NTP

```
[kuso] lunash:>sysc ntp enable

NTP is enabled

Shutting down ntpd: [FAILED]

Starting ntpd: [ OK ]

Please wait to see the result ......

NTP is running

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

NTP Associations Status:

ind assID status conf reach auth condition last_event cnt

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

1 186 9014 yes yes none reject reachable 1

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

Please look at the ntp log to see any potential problem.

Command Result : 0 (Success)
```

Add an NTP server

```
[kuso] lunash:>sysc ntp addserver ntp.cpsc.ucalgary.ca

NTP server 'server ntp.cpsc.ucalgary.ca' added.

WARNING !! Server 'ntp.cpsc.ucalgary.ca' added without authentication.

NTP is enabled

Shutting down ntpd: [ OK ]

Starting ntpd: [ OK ]
```

```
Please wait to see the result ......
NTP is running
===============================================================
NTP Associations Status:
ind assID status conf reach auth condition last_event cnt
===============================================================
1 64241 9014 yes yes none reject reachable 1
2 64242 9014 yes yes none reject reachable 1
===============================================================
Please look at the ntp log to see any potential problem.
Command Result : 0 (Success)
[kuso] lunash:>
```

It might take a few minutes to synchronize. If it is checked immediately you will, most likely, get an error:

```
[kuso] lunash:>sysc ntp status
NTP is running
NTP is enabled
Peers:
=================================================================================
remote refid st t when poll reach delay offset jitter
=================================================================================
LOCAL(0) .LOCL. 10 l 34 64 3 0.000 0.000 0.001
time4.cpsc.ucal 10.10.0.22 2 u 35 64 3 47.625 -37958. 6.158
=================================================================================
Associations:
=================================================================================
ind assID status conf reach auth condition last_event cnt
===============================================================
1 64241 9014 yes yes none reject reachable 1
2 64242 9014 yes yes none reject reachable 1
=================================================================================
NTP Time:
=================================================================================
ntp_gettime() returns code 5 (ERROR)
time ccceb621.3118b000 Wed, Nov 19 2008 10:58:25.191, (.191783),
maximum error 51216 us, estimated error 16 us
ntp_adjtime() returns code 5 (ERROR)
modes 0x0 (),
offset 0.000 us, frequency 0.000 ppm, interval 4 s,
maximum error 51216 us, estimated error 16 us,
status 0x40 (UNSYNC),
time constant 0, precision 1.000 us, tolerance 512 ppm,
pps frequency 0.000 ppm, stability 512.000 ppm, jitter 200.000 us,
intervals 0, jitter exceeded 0, stability exceeded 0, errors 0.
===============================================================================
Command Result : 0 (Success)
```

It takes a few minutes to synchronize - note below that the estimated errors are now zero:

```
[kuso] lunash:>sysc ntp status
NTP is running
NTP is enabled
Peers:
===============================================================================
remote refid st t when poll reach delay offset jitter
===============================================================================
LOCAL(0) .LOCL. 10 l 46 64 377 0.000 0.000 0.001
*time4.cpsc.ucal 10.10.0.22 2 u 44 64 377 47.936 -37995. 27.368
===============================================================================
Associations:
===============================================================================
ind assID status conf reach auth condition last_event cnt
===========================================================
1 64241 9014 yes yes none reject reachable 1
2 64242 9614 yes yes none sys.peer reachable 1
===============================================================================
NTP Time:
===============================================================================
ntp_gettime() returns code 0 (OK)
time ccceb7ae.5f9ff000 Wed, Nov 19 2008 11:05:02.373, (.373534),
maximum error 1072493 us, estimated error 0 us
```

```
ntp_adjtime() returns code 0 (OK)
modes 0x0 (),
offset 0.000 us, frequency 0.000 ppm, interval 4 s,
maximum error 1072493 us, estimated error 0 us,
status 0x1 (PLL),
time constant 2, precision 1.000 us, tolerance 512 ppm,
pps frequency 0.000 ppm, stability 512.000 ppm, jitter 200.000 us,
intervals 0, jitter exceeded 0, stability exceeded 0, errors 0.
===============================================================================
Command Result : 0 (Success)
[kuso] lunash:>
```

Using Secure NTP

The SafeNet Network HSM appliance supports simple, non-secure NTP (Network Time Protocol), as well as two types of secure or trusted NTP :

- Symmetric Key - used to prove authenticity of data received, when a shared secret is held by both the NTP server and its client - choose this option by using the sysconf ntp symmetricAuth commands
- Public Key (Autokey) - uses asymmetric key pairs to achieve the authentication when a shared secret is not readily established - choose this option by using the sysconf ntp autokeyAuth and selecting the desired Identity Scheme to employ

Identity Schemes are methods for proving the identity of remote systems, in this case NTP servers.

If you have previously been using ordinary, simple (not secured) NTP we recommend that you begin using the secure version. If you have older keys or certificates from secure/trusted NTP servers, we recommend that you renew with more current authentication that does not use MD5.

NTP in general is described in the Concepts section of this Help at About NTP.

The available configuration commands are described in the Reference section of this Help, under "Lunash Appliance Commands > sysconf Commands > sysconf ntp Commands".

Using Autokey Authentication

1. Generate Autokey Keys:
   ```
   lunash:>sysconf ntp autokeyAuth generate -password mypa$$word
   ```
2. Add the server using “-autokey” option:
   ```
   lunash:>sysconf ntp addserver myTrustedNTPServer –autokey
   ```
3. Run the command
   ```
   lunash:>sysconf ntp status
   ```
   to check the status

Using Symmetric Key Authentication

1. Obtain the symmetric keys from your trusted server and add them using the command:
   ```
   lunash:>sysconf ntp symmetricAuth key add
   ```

2. Add the key id from step 1 to the list of trusted keys using the command:
   lunash:>sysconf ntp symmetricAuth trustedKeys add
3. Add the server using "-key keyID" option:
   lunash:>sysconf ntp addserver –key keyID
4. Run the command
   lunash:>sysconf ntp status
   to check the status

Example Using Secure NTP

We suggest that you use secure NTP (as opposed to the non-secure standard variety) for your SafeNet Network HSM. Secure NTP can be mixed with regular/simple NTP. For this example, any simple NTP will be removed for now:

```
[kuso] lunash:>sysc ntp list
=================================================================
NTP Servers:
server 127.127.1.0
server ntp.cpsc.ucalgary.ca
=================================================================
Command Result : 0 (Success)
[kuso] lunash:>sysc ntp delete ntp.cpsc.ucalgary.ca
NTP server ntp.cpsc.ucalgary.ca deleted
NTP is enabled
Shutting down ntpd:                                         [  OK  ]
Starting ntpd:                                              [  OK  ]
Please wait to see the result ......
NTP is running
===========================================================
NTP Associations Status:
ind assID status  conf reach auth condition  last_event cnt
===========================================================
1  7095  9014   yes   yes  none    reject   reachable  1
===========================================================
Please look at the ntp log to see any potential problem.
Command Result : 0 (Success)
[kuso] lunash:>
```

Obtain an identity scheme from the secure NTP server (IFF, GQ or MV key). Check with the site of the server for the particulars. For this example, an IFF key is used. It must be scp'd to the SafeNet Network HSM server and installed:

```
[kuso] lunash:>sysconf ntp  autokeyAuth install -idscheme IFF -keyfile ntpkey_IFFkey_tor1-
jprobe.upn.local.3436099994
------- Installing Imported Identity Scheme File -------
Configured Autokey IFF Identity Scheme.
You must restart NTP for the changes to take effect.
Check NTP status after restarting it to make sure that the client is able to start and sync with
the server.
Command Result : 0 (Success)
[kuso] lunash:>
```

As instructed, restart NTP:

```
[kuso] lunash:>service restart ntp
Shutting down ntp:                                          [  OK  ]
Starting ntp:                                               [  OK  ]
Command Result : 0 (Success)
```

```
[kuso] lunash:>
```

The Secure NTP used for this example uses the default parameters, so only the password is specified:

```
[kuso] lunash:>sysconf ntp autokeyAuth generate -p myPas$w0rd!
Generate new keys and certificates using ntp-keygen
Using OpenSSL version 9070df
Random seed file /root/.rnd 1024 bytes
Generating RSA keys (512 bits)...
RSA 0 1 5       1 11 24                         3 1 2
Generating new host file and link
ntpkey_host_kuso->ntpkey_RSAkey_kuso.3437830225
Using host key as sign key
Generating certificate RSA-MD5
X509v3 Basic Constraints: critical,CA:TRUE
X509v3 Key Usage: digitalSignature,keyCertSign
Generating new cert file and link
ntpkey_cert_kuso->ntpkey_RSA-MD5cert_kuso.3437830225
ntp-keygen Result: 0
You must restart NTP for the changes to take effect.
Check NTP status after restarting it to make sure that the client is able to start and sync with
the server.
Command Result : 0 (Success)
[kuso] lunash:>
```

As instructed, restart NTP at this time:

```
kuso] lunash:>service restart ntp
Shutting down ntp:                                         [  OK  ]
Starting ntp:                                              [  OK  ]
Command Result : 0 (Success)
[kuso] lunash:>
```

Check the status of NTP. Like standard NTP, this may take a few minutes for a proper synchronization to occur:

```
[kuso] lunash:>sysconf ntp status
NTP is running
NTP is enabled
Peers:
==============================================================================
remote           refid      st t when poll reach   delay   offset  jitter
==============================================================================
LOCAL(0)        .LOCL.          10 l    6   64   77    0.000    0.000   0.001
*tor1-jprobe.upn 206.248.171.198  2 u   59   64    3    0.341  -554.47   3.309
==============================================================================
Associations:
==============================================================================
ind assID status  conf reach auth condition  last_event cnt
===========================================================
1 56812  9614   yes    yes  ok  sys.peer   sys_peer  1
2  5725  f63a   yes    yes   ok   sys.peer    sys_peer  3
==============================================================================
NTP Time:
==============================================================================
ntp_gettime() returns code 0 (OK)
time cce922c5.76cdb000  Tue, Dec  9 2008 12:00:53.464, (.464076),
maximum error 452335 us, estimated error 0 us
ntp_adjtime() returns code 0 (OK)
modes 0x0 (),
offset 0.000 us, frequency 0.000 ppm, interval 4 s,
maximum error 452335 us, estimated error 0 us,
status 0x1 (PLL),
time constant 2, precision 1.000 us, tolerance 512 ppm,
==============================================================================
Command Result : 0 (Success)
[kuso] lunash:>
```

Timezones and Timezone Codes

How to Set a Timezone with the Timezone Equivalent List

In lunash, the `sysconf timezone` command allows you to change the current system timezone setting to a value appropriate to your locality and your situation. You may prefer to use only GMT, or you may wish to match your local timezone.

Note that the time zone code reported by `sysconf timezone show` is a localized abbreviation. For example, the following two commands set the time zone code to “EST” (during periods when daylight savings time is not in effect).

```
sysconf timezone set America/Kentucky/Louisville
```

```
sysconf timezone set Australia/Brisbane
```

For more information on time zone abbreviations, please visit: http://www.worldtimezone.com/

The time system accepts local settings as either an offset from Greenwich Mean Time (GMT +3 hours, GMT -5 hours, etc.) or as city/state names.

If you choose a named timezone, the system attempts to implement the Daylight Saving Time regime – setting the system time forward one hour on the appropriate date, and back one hour to standard time on the date appropriate for your locality.

If you choose GMT plus-or-minus a numeric offset, then that value is fixed, and the system does not attempt to implement Daylight Saving Time. If you require an adjustment, then you must make it yourself, by manually issuing the appropriate time-change.

Timezone Codes

If a heading is subdivided, then click it to expand that portion of the list.

Use the heading plus the subdivision(s), separated by “/” characters.

If a heading has no subdivisions, use the heading alone as the timezone code.

For example, to set the timezone to Abidjan, the command would be:

```
 sysconf timezone set Africa/Abidjan
```

To set the timezone to Hongkong, the command would be:

```
 sysconf time zone set Hongkong
```

To set the timezone to Knox, Indiana, the command would be:

```
 sysconf timezone set America/Indiana/Knox
```

Note: (Please be patient. Some of these links can take a long time to open.)

Africa

Abidjan, Accra, Addis_Ababa, Algiers, Asmera

Bamako, Bangui, Banjul, Bissau, Blantyre, Brazzaville, Bujumbura

Cairo, Casablanca, Ceuta, Conakry

Dakar, Dar_es_Salaam, Djibouti, Douala

El_Aaiun

Freetown

Gaborone

Harare

Johannesburg

Kampala, Khartoum, Kigali, Kinshasa

Lagos, Libreville, Lome, Luanda, Lubumbashi, Lusaka

Malabo, Maputo, Maseru, Mbabane, Mogadishu, Monrovia

Nairobi, Ndjamena, Niamey, Nouakchott

Ouagadougou

Porto-Novo

Sao_Tome

Timbuktu, Tripoli, Tunis

Windhoek

America

Adak, Anchorage, Anguilla, Antigua, Araguaina, Aruba, Asuncion, Atka

Barbados, Belem, Belize, Boa_Vista, Bogota, Boise, Buenos_Aires

Cambridge_Bay, Cancun, Caracas, Catamarca, Cayenne, Cayman, Chicago, Chihuahua, Cordobam, Costa_Rica, Cuiaba, Curacao

Dawson, Dawson_Creek, Denver, Detroit, Dominica

Edmonton, Eirunepe, El_Salvador, Ensenada

Fortaleza, Fort_Wayne

Glace_Bay, Godthab, Goose_Bay, Grand_Turk, Grenada, Guadeloupe, Guatemala, Guayaquil, Guyana

Halifax, Havana, Hermosillo

Indiana, Indianapolis, Inuvik, Iqaluit

Jamaica, Jujuy, Juneau

Knox, Kentucky, Knox_IN

La_Paz, Lima, Los_Angeles, Louisville

Marengo, Monticello, Maceio, Managua, Manaus, Martinique, Mazatlan, Mendoza, Menominee, Merida, Mexico_City, Miquelon, Monterrey, Montevideo, Montreal, Montserrat

Nassau, New_York, Nipigon, Nome, Noronha

Panama, Pangnirtung, Paramaribo, Phoenix, Port-au-Prince, Porto_Acre, Port_of_Spain, Porto_Velho, Puerto_Rico

Rainy_River, Rankin_Inlet, Recife, Regina, Rio_Branco, Rosario

Santiago, Santo_Domingo, Sao_Paulo, Scoresbysund, Shiprock, St_Johns, St_Kitts, St_Lucia, St_Thomas, St_Vincent, Swift_Current

Tegucigalpa, Thule, Thunder_Bay, Tijuana, Tortola

Vancouver, Vevay, Virgin

Whitehorse, Winnipeg

Yakutat, Yellowknife

Antarctica

Casey

Davis, Dumont, DUrville

Mawson, McMurdo

Palmer

South_Pole, Syowa

Vostok

Arctic

Longyearbyen

Asia

Aden, Almaty, Amman, Anadyr, Aqtau, Aqtobe, Ashgabat, Ashkhabad

Baghdad, Bahrain, Baku, Bangkok, Beirut, Bishkek, Brunei

Calcutta, Chungking, Colombo

Dacca, Damascus, Dhaka, Dili, Dubai, Dushanbe

Gaza

Harbin, Hong_Kong, Hovd

Irkutsk, Istanbul

Jakarta, Jayapura, Jerusalem

Kabul, Kamchatka, Karachi, Kashgar, Katmandu, Krasnoyarsk, Kuala_Lumpur, Kuching, Kuwait

Macao, Magadan, Manila, Muscat

Nicosia, Novosibirsk

Omsk

Phnom_Penh, Pontianak, Pyongyang

Qatar

Rangoon, Riyadh

Saigon, Samarkand, Seoul, Shanghai, Singapore

Taipei, Tashkent, Tbilisi, Tehran, Tel_Aviv, Thimbu, Thimphu, Tokyo

Ujung_Pandang, Ulaanbaatar, Ulan_Bator, Urumqi

Vientiane, Vladivostok

Yakutsk, Yekaterinburg, Yerevan

Atlantic

Azores

Bermuda

Canary, Cape_Verde

Faeroe

Jan_Mayen

Madeira

Reykjavik

South_Georgia, Stanley, St_Helena

Australia

ACT, Adelaide

Brisbane, Broken_Hill

Canberra

Darwin

Hobart

LHI, Lindeman, Lord_Howe

Melbourne

North, NSW

Perth

Queensland

South, Sydney

Tasmania

Victoria

West

Yancowinna

Brazil

Acre

DeNoronha

East

West

Canada

Atlantic

Central

Eastern, East-Saskatchewan

Mountain

Newfoundland

Pacific

Saskatchewan

Yukon

Chile

(Continental and EasterIsland are part of CET zone, but they are not set individually; to set this timezone use `sysconf timezone set CET`)

Europe

Amsterdam, Andorra, Athens

Belfast, Belgrade, Berlin, Bratislava, Brussels, Bucharest, Budapest

Chisinau, Copenhagen

Dublin

Gibraltar

Helsinki

Istanbul

Kaliningrad, Kiev

Lisbon, Ljubljana, London, Luxembourg

Madrid, Malta, Minsk, Monaco, Moscow

Nicosia

Oslo

Paris, Prague

Riga, Rome

Samara, San_Marino, Sarajevo, Simferopol, Skopje, Sofia, Stockholm

Tallinn, Tirane, Tiraspol

Uzhgorod

Vaduz, Vatican, Vienna, Vilnius

Warsaw

Zagreb, Zaporozhye, Zurich

Indian (Indian Ocean Timezone Locales)

Antananarivo

Chagos, Christmas, Cocos, Comoro

Kerguelen

Mahe, Maldives, Mauritius, Mayotte

Reunion

CST6CDT

Cuba

EET

Egypt

Eire

EST

EST5EDT

Etc

GMT, GMT0, GMT-0, GMT+0, GMT-1, GMT+1, GMT-10, GMT+10, GMT-11, GMT+11, GMT-12, GMT+12, GMT-13, GMT-14, GMT-2, GMT+2, GMT-3, GMT+3, GMT-4, GMT+4, GMT-5, GMT+5, GMT-6, GMT+6, GMT-7, GMT+7, GMT-8, GMT+8, GMT-9, GMT+9

Greenwich

UCT, Universal, UTC

Zulu

GB

GB-Eire

GMT

GMT0

GMT-0

GMT+0

Greenwich

Hongkong

HST

Iceland

Iran

Israel

Jamaica

Japan

Kwajalein

Libya

MET

Mexico

BajaNorte, BajaSur

General

Mideast

Riyadh87, Riyadh88, Riyadh89

MST

MST7MDT

Navajo

NZ

NZ-CHAT

Pacific

Apia, Auckland

Chatham

Easter, Efate, Enderbury

Fakaofo, Fiji, Funafuti

Galapagos, Gambier, Guadalcanal, Guam

Honolulu

Johnston

Kiritimati, Kosrae, Kwajalein

Majuro, Marquesas, Midway

Nauru, Niue, Norfolk, Noumea

Pago_Pago, Palau, Pitcairn, Ponape, Port_Moresby

Rarotonga

Saipan, Samoa

Tahiti, Tarawa, Tongatapu, Truk

Wake, Wallis

Yap

Poland
Portugal
PRC
PST8PDT
ROC
ROK
Singapore
Turkey

UCT
Universal

US

Alaska, Aleutian, Arizona

Central

Eastern, East-Indiana

Hawaii

Indiana-Starke

Michigan, Mountain

Pacific

Samoa

UTC

WET

W-SU

Zulu

5
System Logging

This chapter describes logging of SafeNet appliance events, outside the HSM. It contains the following sections:

- "Notes About Logging" below
- "Remote System Logging" below

For logging of HSM events, see "Overview - Security Audit Logging and the Audit Role".

Notes About Logging

Most of the relevant logs are managed with the syslog commands, where you set rotation and other parameters to suit your own monitoring and management schedule.

The NTP logs are not included in the periodic rotations in SafeNet Network HSM. Our experience is that most customers want to accumulate NTP logs in one continuous file over a long period of time. Events are sufficiently infrequent that the NTP log file won't grow very fast, and so would never fill up the whole log directory.

Similarly, HSM logs are excluded from periodic rotation. A security auditor would likely want to see the complete HSM log (hsm.log).

Customers can delete NTP logs and other log files, except hsm.log, using this command:

lunash:>syslog cleanup

For NTP tracking and administration, only the ntp.log file is important. Ensure that you have retrieved a copy of that file before you run 'syslog cleanup'.

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.

Remote System Logging

To take advantage of remote system logging on any UNIX/Linux system that supports the standard syslog service, refer to the SafeNet Network HSM syslog commands under "syslog remotehost"(subcommands "add", "delete" and "list")The remote host must have UDP port 514 open to receive the logging - refer to your host's OS and firewall documentation.

1. On the SafeNet Network HSM appliance, run the command
lunash:>syslog remotehost add <target-collector's-ip-or-hostname>

2. On the receiving or target system, start syslog with the "-r" option to allow it to receive the logs from your SafeNet Network HSM appliance(s).

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, as described in the following section:

- "Backup and Restore Your Appliance Service Configuration " below

Backup and Restore Your Appliance Service Configuration

SafeNet Network HSM stores details of your appliance's configuration settings for various services. Use the `sysconf config` commands to access and manage those settings. A file named "factoryInit_local_host_Config.tar.gz" preserves the original factory settings for all the configurable appliance services [network, SSH, NTLS, syslog, NTP, SNMP, users, and system services].

You can create a backup summary of the state of all those service parameters at any time with `sysconf config backup -description <some_words_of comment>`, and you can list all such files, complete with the description you provided for each one with `sysconf config list`.

At any time, you can reset all the configurable appliance parameters back to factory state with `sysconf config factoryReset`, which applies the settings from "factoryInit_local_host_Config.tar.gz". When you run that command, the system first takes a snapshot of your current settings, in case you later wish to revert back from original factory settings to the settings you had just before`sysconf config factoryReset` was issued.

Note: If you upgrade your appliance, the original factory configuration no longer applies. Do **not** attempt to restore the original configuration: the configuration settings might not apply for the new appliance version.

Note: Immediately after you upgrade your appliance, create a new configuration with the "sysconf config backup" command 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.

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, similar to this example for a SafeNet Network HSM appliance named "sa5":

```
[sa5] lunash:>sysconf config list
Configuration backup files in file system:
Size            File Name                               Description.
16641       |  sa5_Config_20120222_0556.tar.gz         |  testing-this

.7028       |  factoryInit_local_host_Config.tar.gz    |  Initial Factory Settings
16588       |  sa5_Config_20120222_0558.tar.gz         |  Automatic Backup Before Restoring
Command Result : 0 (Success)
[sa5] lunash:>sysconf config restore
```

If you wish, you can keep only the backup files that you find useful, and individually delete any others with `sysconf config delete -file <filename>`.

Optionally, you clear away all the files with `sysconf config clear`.

Either way, the file "factoryInit_local_host_Config.tar.gz" is not touched.

Note that the configuration backup file area is a special-purpose location. You will not see those files listed if you run the command `my file list`.

Example of Backing Up and Restoring

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

Create a backup of current appliance configuration parameters.

```
[sa5] lunash:>sysconf config backup -description testing-this backup feature
Created configuration backup file: sa5_Config_20120222_0556.tar.gz
Command Result : 0 (Success)
[sa5] lunash:>
```

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

```
[sa5] 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)
[sa5] lunash:>
```

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

```
[sa5] lunash:>sysconf config factoryReset -service users
This command restores the initial factory configuration of service: users.
The HSM and Partition configurations are NOT included.
WARNING !!  This command restores the configuration backup file: factoryInit_local_host_Con-
fig.tar.gz.
It first creates a backup of the current configuration before restoring: factoryInit_local_host_
Config.tar.gz.
If you are sure that you wish to proceed, then type 'proceed', otherwise type 'quit'.
> proceed
Proceeding...
Created configuration backup file: sa5_Config_20120222_0800.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)
[sa5] 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)
[sa5] lunash:>
```

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

```
[sa5] lunash:>
login as: admin
admin@172.20.10.202's password:
Access denied
admin@172.20.10.202's password:
Last login: Wed Feb 22 05:44:39 2012 from 172.20.10.143
SafeNet Network HSM 5.1.0-25 Command Line Shell - Copyright (c) 2001-2011 SafeNet, 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.
[sa5] lunash:>
```

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.

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

```
[sa5] lunash:>user list
Users           Roles           Status          RADIUS
admin           admin           enabled         no
monitor         monitor         enabled         no
operator        operator        enabled         no
Command Result : 0 (Success)
[sa5] lunash:>
```

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.

```
sa5] lunash:>sysconf config list
Configuration backup files in file system:
Size            File Name                               Description.
16641       |  sa5_Config_20120222_0556.tar.gz         |  testing-this

.7028       |  factoryInit_local_host_Config.tar.gz    |  Initial Factory Settings
16588       |  sa5_Config_20120222_0558.tar.gz         |  Automatic Backup Before Restoring
Command Result : 0 (Success)
[sa5] lunash:>sysconf config restore
```

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

```
[sa5] lunash:>sysconf config restore -service users -file sa5_Config_20120222_0556.tar.gz
WARNING !!  This command restores the configuration backup file: sa5_Config_20120222_
0556.tar.gz.
It first creates a backup of the current configuration before restoring: sa5_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: sa5_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)
[sa5] lunash:>
[sa5] 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)
[sa5] lunash:>
```

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

Once again we check the list of users.

```
[sa5] 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.

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

```
sa5] lunash:>sysconf config list
Configuration backup files in file system:
Size File Name Description.
16641       | sa5_Config_20120222_0556.tar.gz         | testing-this
.7028       | factoryInit_local_host_Config.tar.gz  |  Initial Factory Settings
16588       | sa5_Config_20120222_0558.tar.gz         | Automatic Backup Before Restoring
16248       | sa5_Config_20120222_0606.tar.gz         | Automatic Backup Before Restoring
Command Result : 0 (Success)
[sa5] lunash:>sysconf config restore
```

We see that a new file was created (...0606.tar.gz...) before the restore operation, and the other files are intact.

Backup to HSM

You can protect a configuration setup against the possibility of appliance failure by moving a backup snapshot file into your 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 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.

6
PKI Bundle

This chapter describes Public Key Infrastructure for SafeNet Network HSM, by means of attached SafeNet USB HSM. It contains the following sections:

- "Set Up and Use PKI-bundle Option" on the next page

Set Up and Use PKI-bundle Option

What is PKI Bundle?

The PKI Bundle option is the use of a SafeNet USB HSM, connected externally to a SafeNet Network HSM appliance, allowing the SafeNet USB HSM to share the networked capabilities of the SafeNet Network HSM.

It works like this:

- General online cryptographic operations are carried out via the SafeNet Network HSM and its on-board application partitions for constant, rapid access.
- The SafeNet USB HSM (a single-slot or single-partition HSM) is pre-deployed (initialized) and then deployed as a slot/partition of the appliance, used for operations where high performance is not a requirement.

Note: The PKI Bundle feature is supported with PED-authenticated SafeNet Network HSM, and the connected SafeNet USB HSM must also be PED-authenticated. PKI bundling with password-authenticated SafeNet Network HSM or SafeNet USB HSM is not supported.

Note: The SafeNet Network HSM PKI Bundle option does not support Per-Partition Security Officer (PPSO). That is, a SafeNet USB HSM that is USB-connected to a SafeNet Network HSM appliance can be configured with any compatible firmware, including firmware version 6.22.0 (or newer), but cannot have the PPSO capability applied.

Note: SafeNet Network HSM PKI Bundle option **does not support** the use of SafeNet DOCK2 and removable PCMCIA token HSMs (SafeNet CA4).

Prepare to use the PKI Bundle feature

1. If you have not already done so, set up Remote PED between the SafeNet Network HSM appliance and an instance of PEDserver on a suitable host computer; see "Configuring Remote PED" on page 1
2. Have the SafeNet USB HSM USB-connected to the SafeNet Network HSM appliance, and ensure that the SafeNet USB HSM is imprinted with the desired orange PED Key, in order to perform the following actions using Remote PED.
3. Use the **token pki predeploy** command to initialize the SafeNet USB HSM for use as a PKI device with SafeNet Network HSM. Type:

```
lunash:> token pki predeploy -label myPKI -serial 777199

Please type "proceed" to continue, anything else to abort: proceed
********************************************
*                                          *
*     About to factory Reset the HSM       *
*                                          *
********************************************
```

```
********************************************
*                                          *
*   About to initialize the HSM            *
*   Please pay attention to the PED        *
*                                          *
********************************************
Do you want to use FIPS-approved algorithms and key strengths only (yes or no)? yes
********************************************
*                                          *
*   About to change the HSM FIPS policy    *
*   Please pay attention to the PED        *
*                                          *
********************************************
********************************************
*                                          *
*   About to create a partition on the HSM *
*   Please pay attention to the PED        *
*                                          *
********************************************
********************************************
*                                          *
*   About to set the partition policies    *
*   Please pay attention to the PED        *
*                                          *
********************************************
********************************************
*                                          *
*   About to create a partition challenge  *
*   and activate the partition.            *
*   Please pay attention to the PED        *
*   Please write down the PED secret!      *
*                                          *
********************************************

Please enter the partition challenge:

        Please attend to the PED.
Success predeploying the token!!

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

4. Use the **token pki deploy** command to make the pre-deployed SafeNet USB HSM available to the SafeNet Network HSM as a (removable) partition or PKCS#11 slot, for use by your applications. Type:

```
lunash:> token pki deploy -label myPKI -serial 777199
**********************************************
*                                            *
*   About to activate the token for testing. *
*   Please pay attention to the PED          *
*                                            *
**********************************************

Please enter the current user challenge:

Success deploying token myPKI with serial num 777199 !
```

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

5. Use the **client assignpartition** command to assign the deployed HSM to the remote client, much as you assigned application partitions with the SafeNet Network HSM to their client(s). Type

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

'client assignPartition' successful.

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