

SafeNet Network HSM 6.2.2

Appliance Administration Guide

Document Information

Product Version	6.2.2
Document Part Number	007-011136-012
Release Date	01 December 2016

Revision History

Revision	Date	Reason
A	01 December 2016	Initial release.

Trademarks, Copyrights, and Third-Party Software

Copyright 2001-2016 Gemalto. All rights reserved. Gemalto and the Gemalto logo are trademarks and service marks of Gemalto and/or its subsidiaries and are registered in certain countries. All other trademarks and service marks, whether registered or not in specific countries, are the property of their respective owners.

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 (ey@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.

Disclaimer

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

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

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

- The copyright notice, the confidentiality and proprietary legend and this full warning notice appear in all copies.
- This document shall not be posted on any publicly accessible network computer or broadcast in any media, and no modification of any part of this document shall be made.

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

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

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

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

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

Regulatory Compliance

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

USA, FCC

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

- This device may not cause harmful interference.
- This device must accept any interference received, including interference that may cause undesired operation.



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

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

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

Changes or modifications not expressly approved by Gemalto 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; CISPR22 and IEC801. This product satisfies the CLASS B limits of EN 55022.

CONTENTS

PREFACE	About the Appliance Administration Guide	11
Customer Release Notes		12
Gemalto Rebranding		12
Audience		12
Document Conventions		13
Notes		13
Cautions		13
Warnings		13
Command Syntax and Typeface Conventions		13
Support Contacts		14
1	Appliance Hardware Functions	16
Front-panel Display		16
Condition Codes		16
Display Conventions		18
System Behavior with Hardware Tamper Events		18
Tampering with the Appliance		18
Decommission		19
What Happens When You Tamper - Including Opening the Fan Bay		19
Summary of Your Responses to Tamper Events		27
Shutdown or Reboot		27
No Physical Access to SafeNet Network HSM Appliance		28
Automatic Restart Following a Power Interruption		28
Power Supply and Fan Maintenance		28
Replacing a Power Supply		29
The Fans		30
Summary		35
HSM Emergency Decommission Button		35
What the Emergency Decommission Button Does		35
When to Use the Emergency Decommission Button		36
Power Consumption		36
Frequently Asked Questions		37
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.		37
What actions must I take to move a SafeNet HSM appliance from one datacenter to another?		37
Failed Logins and Lockout on SafeNet Appliance		37
2	Client Connections	39
Connections to the Appliance - Limits		39
SafeNet Network HSM Port Usage		40
Standard Ports		40
Additional Ports		40
SafeNet Network HSM Appliance Port Bonding		41

Technical Details	41
Using Port Bonding	41
Client Startup Delay Across Mixed Subnets	42
Using Public-Key Authentication	43
Public Key Authentication to a SafeNet Appliance Using UNIX SSH Clients	43
Set up Public-Key SSH access for other SafeNet Network HSM users	45
NTLS Keys in Hardware or in Software	45
Moving into 'Hardware' (the HSM)	46
Going Back to 'Software'	46
Additional Notes	46
When to Restart NTLS	47
SSH Disabled Upon Reboot	47
NTLS (SSL) Performance Issue	48
Impact of the service restart ntlS Command	48
Messages During an SSH Session	48
Timeouts	49
Network Receive Timeout	49
3 Users and Passwords	50
HSM Login [Trusted Path]	50
Roles	50
Named Administrative Users and Their Assigned Roles	51
Abilities or Privileges of Created Users	52
Why Create Extra Administrative Users?	52
Implications of Backup and Restore of User Profiles	52
Security of Shell User Accounts	53
Changing Appliance Passwords	53
Appliance	53
HSMs and Partitions	53
Forgotten Passwords / Lost Authentication	54
Appliance admin password recovery	54
HSM Admin / Security Officer Authentication - No Recovery	54
Legacy Partition Owner / Partition User / Crypto Officer Authentication Recovery	54
PSO Partition Roles Authentication Recovery	54
Help! I have lost my blue/black/red/orange/purple/white PED Key or I have forgotten the password!	55
But I don't have keys or secrets in secure on-site or off-site storage! What do I do?	55
I have my PED Key, but I forgot my PED PIN! What can I do?	57
I have my PED Keys and my PED PINS, but I can't remember which one goes with which HSM (or partition)!	57
Recover or Reset the Admin Account Password	58
4 Timestamping – NTP and Time Drift	61
Correcting Time Drift	61
First, establish the drift that exists for your appliance	61
NTP and Secure NTP on SafeNet Network HSM	64
What If I Can't Use NTP?	64
References	65
Example Using Simple NTP	65
Using Secure NTP	68
Example Using Secure NTP	69

Time Zones and Timezone Codes	71
How to Set a Time Zone with the Time Zone Equivalent List	71
5 System Logging	72
Notes About Logging	72
Hardware monitoring and logging	72
Remote System Logging	72
Configuring a Linux Syslog Server	73
Configuring the Appliance to Send Logs to the Remote Syslog Server	73
6 Backing Up the Appliance Configuration	74
Backup and Restore Your Appliance Service Configuration	74
Example of Backing Up and Restoring	75
Backup to HSM	78
6 PKI Bundle	79
Set Up and Use PKI-bundle Option	80
What is PKI Bundle?	80
Prepare to use the PKI Bundle feature	80
PREFACE Appendix A: Configuration Long-form	83
1 [Step 1] Planning Your Configuration	84
Appliance Roles	84
Named Administrative Users and Their Assigned Roles	85
Implications of Backup and Restore of User Profiles	86
Security of Shell User Accounts	86
HSM Roles and Secrets	87
Crypto Officer & Crypto User	87
How the Roles are Invoked	90
Bad Login Attempts	90
Domain Planning	90
Characteristics of Cloning Domains	91
PED-authenticated HSM Planning	93
SafeNet PED Planning	93
What each PED prompt means	94
HSM Initialization and the Blue SO PED Key	95
HSM Cloning Domain and the Red Domain PED Key	96
Partition Owner/User and the black PED Key	96
Remote PED Orange PED Key (RPK)	97
Auditor	97
Secure Recovery Purple PED Key (SRK)	97
Other Considerations	98
Password-authenticated HSM Planning	98
HSM Initialization	99
HSM Cloning Domain	99
Application Partition Owner or Crypto-Officer/Crypto-User	99

Application Partition Cloning Domain	99
Auditor	99
Effect of PPSO on SafeNet Network HSM	100
2 [Step 2] Configure Your Network Settings	102
Gather appliance network setting information	102
Client Requirements	102
Recommended Network Characteristics	103
Bandwidth and Latency Recommendation	103
About Latency and Testing	103
Power-up the HSM Appliance	103
Power On Instructions for the SafeNet Network HSM Appliance	104
Power Off	105
Resuming appliance power	106
Open a Connection	106
First Login and Changing Password	107
Set the System Date and Time and SSH Certificate	109
Timezone Codes	110
Create a new SSH Certificate	111
Configure the IP Address and Network Parameters	112
Make Your Network Connection	114
Generate a New HSM Server Certificate	116
3 [Step 3] Initialize the HSM	119
Password-Authenticated versus PED-Authenticated HSMs	119
Which kind do I have?	119
What if I make a mistake about the type of authentication I present?	119
High-Level Configuration Steps	120
About Initializing a Password-Authenticated HSM	121
Initializing a Password Authenticated HSM	121
About Initializing a PED-Authenticated HSM	123
Recover the SRK	123
Re-split the SRK	125
Other Uses of the SRK	125
Initializing a PED-Authenticated HSM	126
Preparing to Initialize a SafeNet Network HSM [PED-version]	126
Why Initialize?	128
Start a Serial Terminal or SSH session	128
Initialize the HSM	128
Initialization - some additional options and description	135
4 [Step 4] Set the HSM Policies	141
Set HSM Policies (Password Authentication)	141
Set HSM Policies - PED (Trusted Path) Authentication	143
5 [Step 5] Create Application Partitions	147
Choose Partition Type	147
Legacy-style Partitions	147

Per-Partition SO (PPSO) Partitions	147
About Configuring Legacy Partitions	147
Prepare to Create a Legacy Partition (Password Authenticated)	149
About HSM Partitions on the Initialized HSM	149
Create (Initialize) a Password Authenticated Legacy-style Application Partition	150
Partition creation audit log entry	152
Next steps	152
Prepare to Create a Partition (PED Authenticated)	152
About HSM Partitions on the Initialized HSM	152
Create a PED Authenticated Legacy-style Application Partition (f/w pre-6.22.0)	155
About Application Partitions on the Initialized HSM	155
Partition creation audit log entry	161
Create a PED Authenticated Legacy-style Application Partition (f/w 6.22.0 or newer)	162
Partition creation audit log entry	167
Record the Partition Client Password (PED-Auth HSMs)	168
About Configuring an Application Partition with Its Own SO	168
Next step	170
HSM SO Configures PED-authenticated SafeNet Network HSM Partition with SO	171
Preliminary	171
Create the PPSO Partition	173
HSM SO Configures SafeNet Network HSM Password-authenticated Partition with SO	175
Create the PPSO Partition	175
6 [Step 6] Set the Partition Policies for Legacy Partitions	179
Displaying the Current Partition Policy Settings	179
Changing the Partition Policy Settings	181
Policy setting example, SafeNet HSM with Password Authentication	181
Policy setting example, SafeNet HSM with PED Authentication	182
RSA Blinding Mode	182
7 [Step 7] Create a Network Trust Link Between the Client and the Appliance	183
About Network Trust Links	183
The Host Trust Link (HTL) Option for VM Clients	183
Creating a Network Trust Link	184
De-registering and Re-registering Clients	190
8 [Step 8] Enable the Client to Access a Partition	191
Creating an NTL Link Between a Client and a Partition	191
Assigning a Client to a Partition	191
Verifying Your Setup	192
Client Connection Limits	193
Applications and Integrations	193
Creating an STC Link Between a Client and a Partition	193
Creating an STC Link to a Legacy Partition	194
Creating an STC Link to a Partition With SO	199
9 [Step 9] Configure PPSO Application Partitions	205
Initialize the Partition SO and Crypto Officer Roles on a PW-Auth PPSO Partition	205

Initialize the Crypto User Role on a PW-Auth PPSO Partition	207
Initialize the Partition SO and Crypto Officer Roles on a PED-Auth PPSO Partition	208
Initialize the Crypto User Role on a PED-Auth PPSO Partition	210
Crypto Officer or Crypto User Must Log In and Remain Logged In	211
Activate a PED-Auth PPSO Partition for the Crypto Officer Role	211
Activate a PED-Auth PPSO Partition for the Crypto User Role	213
 10 [Step 10] Set the Partition Policies for PPSO Partitions	217
Displaying the Current Partition Policy Settings	217
Changing the Partition Policy Settings	218
RSA Blinding Mode	219
 11 Optional Configuration Tasks	220
[Optional] Configure for RADIUS Authentication	220
RADIUS Configuration Summary	220
Configuring RADIUS with Your SafeNet Appliance	221

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 16](#)
- ["Client Connections" on page 39](#)
- ["Users and Passwords" on page 50](#)
- ["Timestamping – NTP and Time Drift" on page 61](#)
- ["System Logging" on page 72](#)
- ["Backing Up the Appliance Configuration" on page 74](#)

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 13](#)
- ["Support Contacts" on page 14](#)

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_6-2-2.pdf

Gemalto Rebranding

In early 2015, Gemalto 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 PCIe 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 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	<p>The bold attribute is used to indicate the following:</p> <ul style="list-style-type: none"> • Command-line commands and options (Type <code>dir /p</code>.) • 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.)
<i>italics</i>	<p>In type, the italic attribute is used for emphasis or to indicate a related document. (See the <i>Installation Guide</i> for more information.)</p>
<variable>	<p>In command descriptions, angle brackets represent variables. You must substitute a value for command line arguments that are enclosed in angle brackets.</p>

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> <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> <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 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.

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 18
- "Shutdown or Reboot" on page 27
- "Power Supply and Fan Maintenance" on page 28
- "HSM Emergency Decommission Button" on page 35
- "Power Consumption " on page 36
- "Frequently Asked Questions" on page 37

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 ntlis" for more information. Note: Both the NTLS and STC services must be running for the appliance to be in service.	service status ntlis
	25	Out of Service - NTLS is not bound to an ethernet device. Please run "service status ntlis" and "syslog tail" for more information	service status ntlis
	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 28](#) 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 35](#) 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 factory Reset	Starting point
hsm initializ e	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 transp ortMod e enter	Delete the MTK so HSM contents cannot be decoded or used.
hsm show	Basic HSM info remains undisturbed.
partitio n list	None have been created since initialization, above.
partitio n 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 transp ortMod e recove r	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.
partitio n create	Partition is created.
partitio n 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
(syste m resum es) run "sysco nf applia nce 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	<pre>[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:></pre>
view the logs	<p>The hsm.log shows events like:</p> <pre>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</pre> <p>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.</p> <p>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:</p> <pre>syslog tail -logname hsm</pre> <p>Try searching the last couple of hundred entries with:</p> <pre>syslog tail -logname hsm -search tamper -e 200</pre> <p>The audit log shows events like:</p> <pre>lunash:>audit log tail -f hsm_150073_00000001.log</pre> <pre>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)</pre>

Action	Result/State
	<pre>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:></pre>
hsm srk show	<pre>External Split Enabled yes SRK resplit requiredno Hardware Tamperedyes Transport Modeno</pre>
hsm login	<pre>not permitted: LUNA_RET_MTK_ZEROIZED</pre>
hsm srk transportMode recover	<pre>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.</pre>
hsm login	<pre>This time, it works.</pre>
partition list	<pre>Confirm that the pre-existing partition is present.</pre>
partition show Contents	<pre>Confirm that any pre-existing partition contents are there.</pre>

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

hsm srk transportMode enter	<pre>Delete the MTK so HSM contents cannot be decoded or used.</pre>
hsm srk show	<pre>External Split Enabled Yes SRK resplit requiredNo Hardware TamperedNo</pre>

Action	Result/State
	Transport ModeYes
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 comm and	<pre>[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.</pre>
reboot by pressing the Stop/Start switch or by "sysconf appliance reboot"	<p>Appliance stops.</p> <p>Appliance starts.</p>
when appliance is back in operation, look at the hsm.log	<pre>[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</pre>

Action	Result/State
	<pre>Hardware tampered:no Transport mode: no Command Result : 0 (Success) [myluna1] lunash:></pre> <p>The tamper event appears in the log, after the system reboots.</p>
<pre>run "hsm show" and "syslo g tail " to search the hsm log for recent tamper events</pre>	<pre>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:></pre> <p>The HSM is back in operation, as it was before the tamper event.</p> <p>Both splits of the MTK were present on the HSM, so recombining them to reconstitute the MTK was automatic when the HSM was reset.</p> <p>No action is required to re-instate the HSM from the tamper.</p> <p>You are alerted that an event has happened by the HSM becoming unresponsive, forcing you to restart.</p> <p>You can confirm that the reason for the HSM problem was, in fact, a tamper event, by looking at the log.</p> <pre>[myluna1] lunash:>syslog tail -logname hsm -search tamper -e 200 2012 Nov 9 14:50:34 myluna1 local6 err oamp[2239]: ERR: RTC: external</pre>

Action	Result/State
	<p>tamper latched</p> <p>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)</p> <p>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</p> <p>Command Result : 0 (Success)</p> <p>[myluna1] lunash:>hsm srk show</p> <p>Secure Recovery State flags:</p> <p>=====</p> <p>External split enabled: .. no</p> <p>SRK resplit required: no</p> <p>Hardware tampered:no</p> <p>Transport mode: no</p> <p>Command Result : 0 (Success)</p> <p>[myluna1] lunash:></p> <p>The tamper event appears in the log after the system reboots.</p>
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 1 in 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.

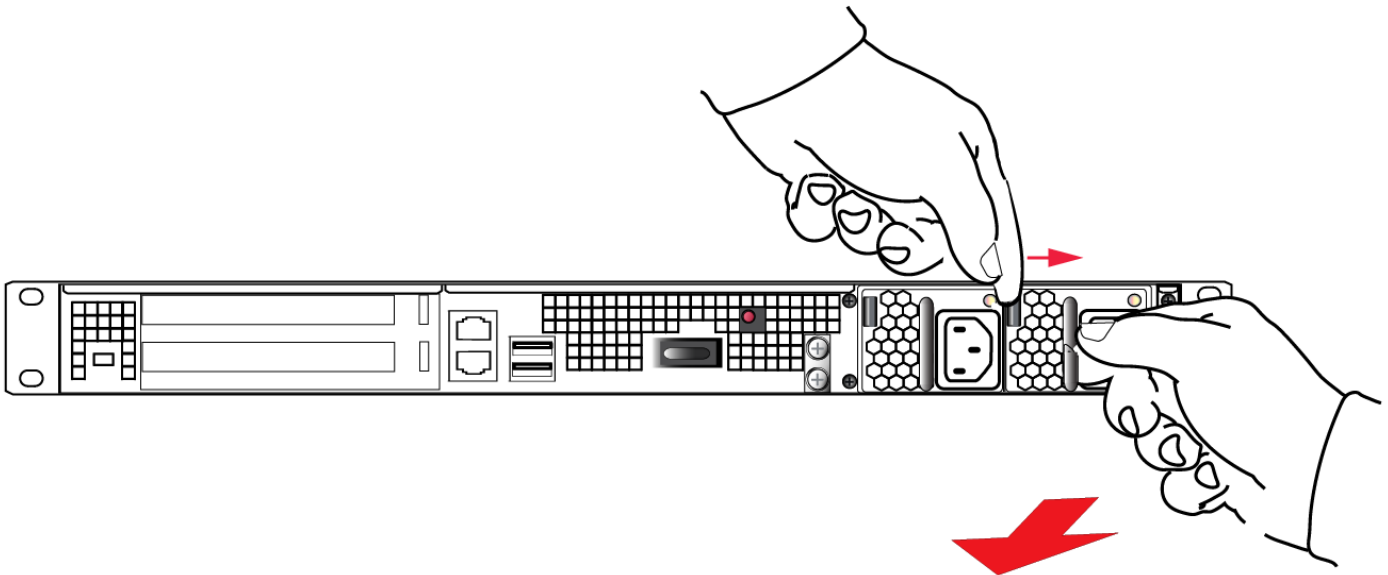
If only one power supply is present, the audible alarm is silent. If you wish to operate your SafeNet Network HSM appliance with only one power supply, we recommend that you remove the second supply to silence the audible alarm.

Replacing a Power Supply

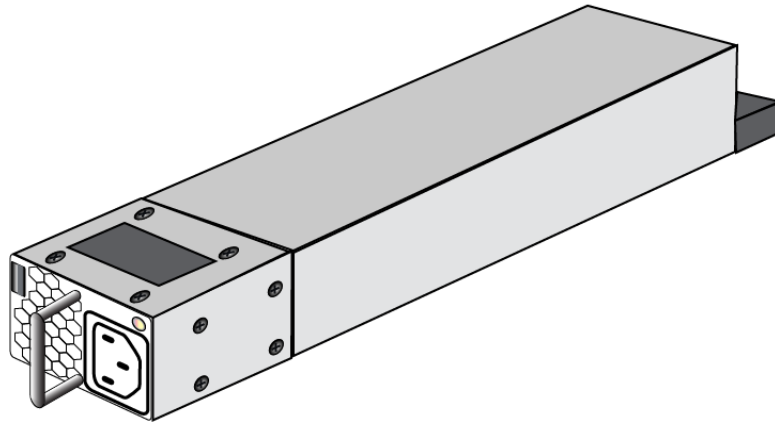
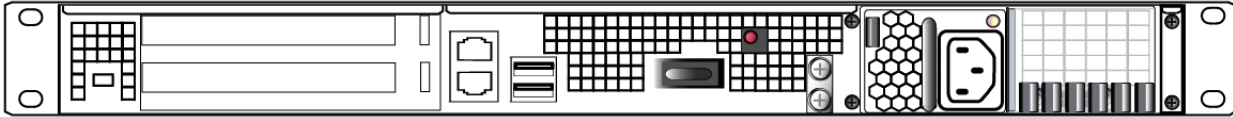
You may need to replace a power supply in the event of a failure.

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 .

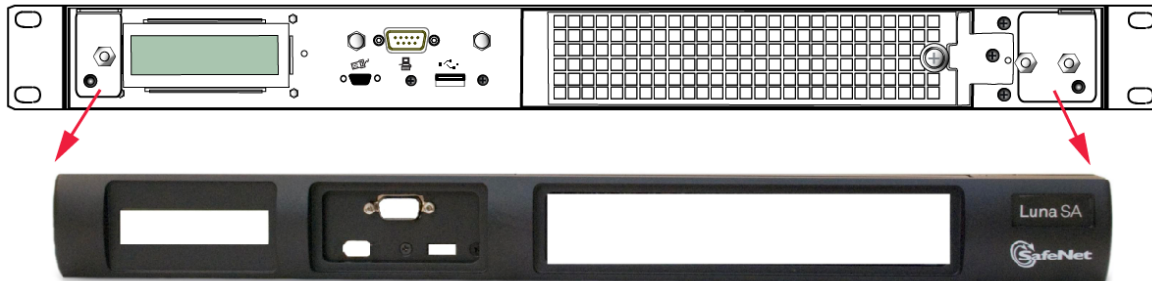


Removing the Front Bezel

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.



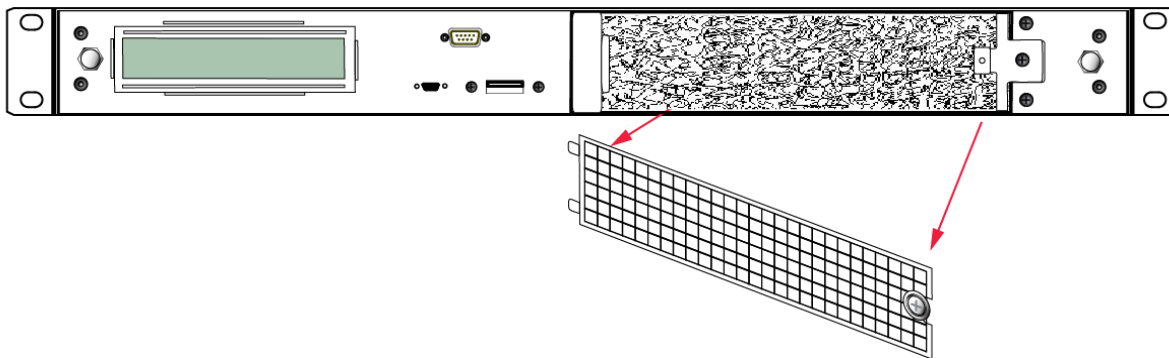
2. The ventilation grille, located to the right, on the appliance front panel, is secured in two parts, by two screws - a knurled, captive thumb-screw, and a Torx T8 screw. The knurled screw can be fastened or released without tools. It secures the lattice screen that in turn retains the mesh air filter.

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.

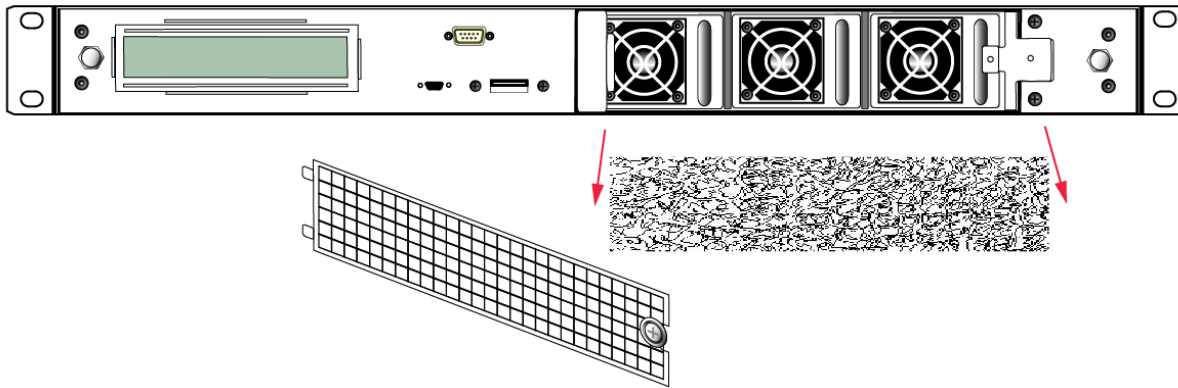
To clean the filter

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.



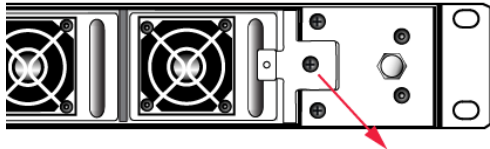
Note: Partition authentication data is de-cached by the tamper - you must "`partition activate -partition <name-of-partition>`" each of your HSM partitions before your clients can resume accessing them. That is, partition activation does not survive a tamper event. In either case, you can examine the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



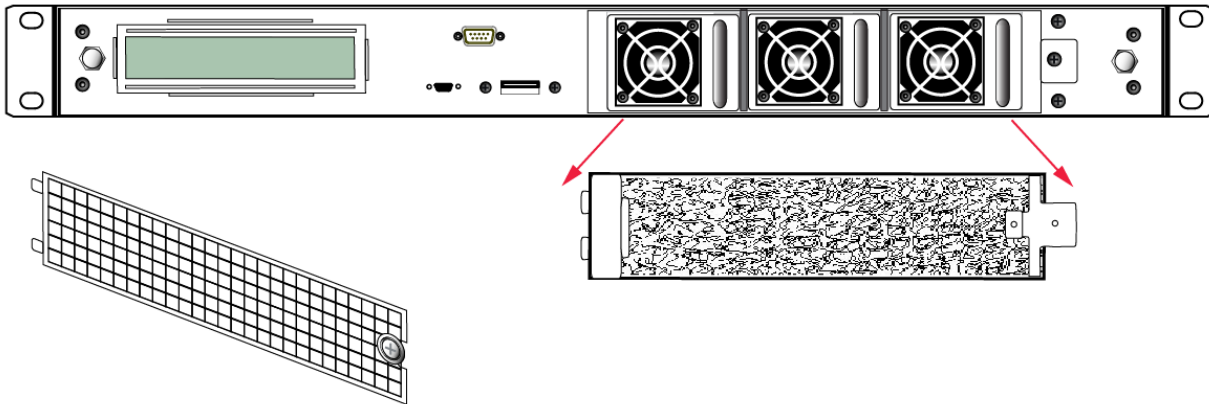
Note: Accessing the air filter mesh in front of the fans (using the thumbscrew to open the retaining grille) does not cause a tamper.

To replace a fan

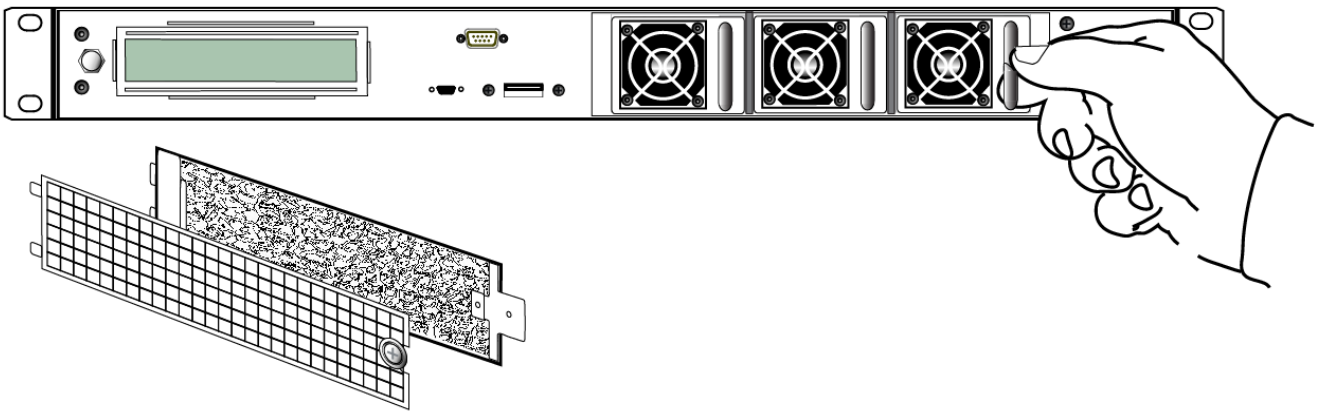
1. To open the fan bay, use a Torx number 8 screwdriver to remove the screw that secures the right-side tab of the fan retainer.



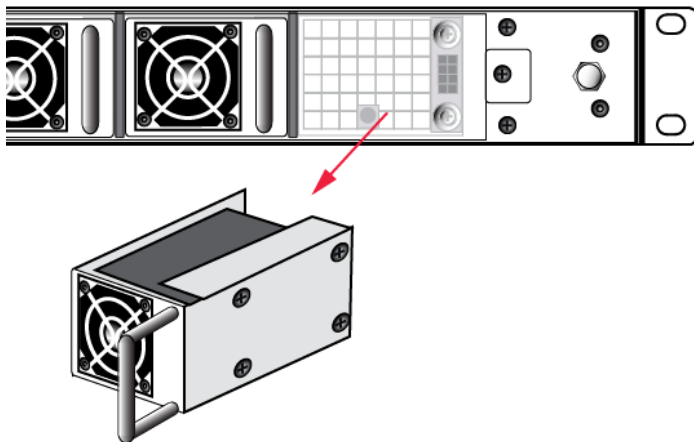
2. The fan retainer is anchored at its left by two tabs - swing the retainer out like a door, and remove it. There is no need to separate the filter mesh and its retainer from the larger fan retainer; the assembly can come out as one piece. The illustration below happens to show them separated.



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.

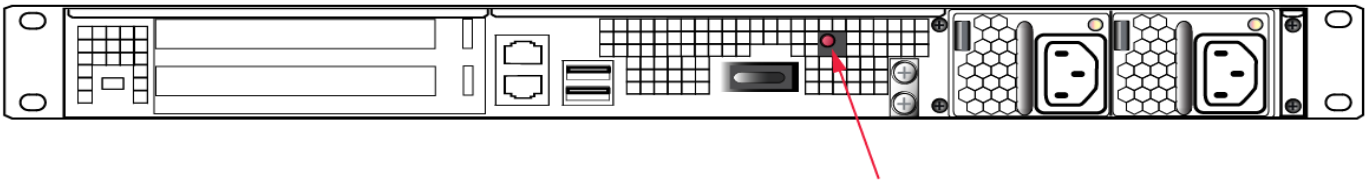
If you prefer these instructions illustrated by photographs, ["Hardware Maintenance"](#).

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/chrstoki.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.

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 "](#) below
- ["SafeNet Network HSM Port Usage"](#) on the next page
- ["SafeNet Network HSM Appliance Port Bonding"](#) on page 41
- ["Client Startup Delay Across Mixed Subnets"](#) on page 42
- ["Using Public-Key Authentication"](#) on page 43
- ["NTLS Keys in Hardware or in Software"](#) on page 45
- ["When to Restart NTLS"](#) on page 47
- ["SSH Disabled Upon Reboot"](#) on page 47
- ["NTLS \(SSL\) Performance Issue"](#) on page 48
- ["Impact of the service restart ntlm Command"](#) on page 48
- ["Messages During an SSH Session"](#) on page 48
- ["Timeouts"](#) on page 49

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 <i>Administration Guide</i> 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).



Note: Beginning with SafeNet Network HSM version 6.2.1, all of the standard Linux port bonding modes are supported, and specified with the `-mode` option of the **network interface bonding config** command:

mode=0 (Balance Round Robin)

mode=1 (Active backup)

mode=2 (Balance XOR)

mode=3 (Broadcast)

mode=4 (802.3ad)

mode=5 (Balance TLB)

mode=6 (Balance ALB)

2. Use the command ["network interface bonding enable" on page 1](#) to enable the bond0 interface.

Optional Considerations

You can configure NTLS to "all" if you wish, and that will work fine with port bonding.

Alternatively, if you intend to use port bonding, you can,

- physically connect eth0 to a network and set eth0 to an IP address,
- configure NTLS for eth0,
- physically connect eth1 to another network but don't bother establishing a separate eth1 IP address (because it will disappear with bonding), and then
- enable bonding.

This ensures that the bonding address is the address already established for NTLS. This has the desired effect of having NTLS work with either port (due to the bonding), but you later disable bonding for any reason, you don't have to remember to assign NTLS to eth0. That is, it was already assigned to eth0 from the start, it picks up the dual physical interface redundancy advantages when bonding is established, and it reverts cleanly to eth0-only in the event that bonding is disabled.

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:el: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 public key that you sent over earlier (from server mypc in our example)

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

Command Result : 0 (Success)

7. Check the list again:

```
[myLuna] lunash:>my public-key list
```

SSH Public Keys for user 'admin':

Name	Type	Bits	Fingerprint
id_rsa.pub	ssh-rsa	1024	6e:7a:7e:e1:2a:54:8f:99:3e:6a:56:f8:38:22:fb:a6

Command Result : 0 (Success)

Notice that the fingerprint reported is the same as was generated back on mypc.

8. From mypc, ssh into myLuna; you should NOT be password prompted:

```
[root@mypc /]# ssh admin@myluna
```

SafeNet 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 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 ntl**.

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.

SSH Disabled Upon Reboot

It is possible to encounter a situation where the SSH service gets disabled upon a reboot of the SafeNet Network HSM appliance, such that you must manually connect using a serial cable and then start the SSH service on the HSM after every reboot.

This situation occurs when an administrator uses the recover account to reset the admin password but cancels out of the session before changing the password from the default PASSWORD. To fix the appliance, complete the recover procedure to the point of setting a new admin password.

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 ntlis Command

If you perform a **service restart ntlis** 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>;
:
}
```

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 \[Trusted Path\]" below](#)
- ["Roles" below](#)
- ["Changing Appliance Passwords" on page 53](#)
- ["Forgotten Passwords / Lost Authentication" on page 54](#)
- ["Recover or Reset the Admin Account Password" on page 58](#)

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

- to map to roles and functions specified in your applications.

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

Two kinds of roles exist on a Network HSM appliance:

- appliance administrative roles that
 - give access to monitor or administer the host system
 - enable a user with further authentication to access the HSM
- HSM administrative roles

Appliance roles alone perform system monitoring and administration functions for networking, logging, update-package handling, file handling, system status, system services, REST API management, and any other host-related features, as well as access to HSM functions that do not require HSM login (generally HSM commands that observe, but do not change the HSM).

Appliance roles along with HSM roles allow authenticated command access to HSM functions that require explicit authentication to the HSM in order to make changes within the HSM or perform other sensitive management operations.

In other words, the HSM is its own entity, residing inside the Network HSM appliance, and command-line access to the HSM requires two levels of authentication, the SSH login that also serves to administer the appliance outside the HSM, and then HSM authentication for sensitive operations inside the HSM.

The SafeNet Network HSM can also be accessed via our REST API, that you can acquire separately. A REST API documentation set (not part of the doc-set that you are reading right now) is included in the downloadable REST API software archive. Contact Gemalto Support.

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 / Lost Authentication

Recover from a forgotten password as follows:

Appliance admin password recovery

If you forget your appliance admin password, you can reset by logging in to the special account called 'recover'. See ["Recover or Reset the Admin Account Password" on page 58](#).

HSM Admin / Security Officer Authentication - No Recovery

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... you do have all your important material backed up, don't you?)

Legacy Partition Owner / Partition User / Crypto Officer Authentication Recovery

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.

PSO Partition Roles Authentication Recovery

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

- For SafeNet Network Appliance HSM, the HSM SO cannot "reset" the Partition SO's password or blue PED Key secret - for the HSM SO, any PSO is a "black box" that s/he can create or destroy, but cannot see or touch inside.
- All authentication-management actions in a PSO partition must take place via a registered client connection, normally using the **role** commands of the lunacm utility:
 - The PSO can modify her/his own password or blue PED Key secret using the lunacm **role changePw** command.
 - The Crypto Officer and Crypto User can modify their own authentication (password or black PED Key secret or gray PED Key secret, or challenge secret for applications) using the lunacm **role changePw** command.

- The PSO can reset the Crypto Officer's or the Crypto User's authentication using the lunacm **role resetPw** command.

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 - legacy partitions: 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 resetPw` 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 loopback 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 for the appliance.
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. We do this to prevent the appliance 'admin' account from being accessible over the network with a known password.

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
-

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 64](#)
- ["Example Using Simple NTP" on page 65](#)
- ["Using Secure NTP" on page 68](#)
- ["Example Using Secure NTP" on page 69](#)

Timezone codes

- ["Time Zones and Timezone Codes" on page 71](#)

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 69](#)) 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 61](#)).

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.cpssc.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:>

```

Time Zones and Timezone Codes

How to Set a Time Zone with the Time Zone Equivalent List

In lunash, the `sysconf timezone` command ("[sysconf timezone](#)" on page 1) allows you to change the current system time zone setting to a value appropriate to your locality and your situation. You might prefer to use only GMT, or you might 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” (Eastern Standard Time) during periods when daylight saving time is not in effect.

```

sysconf timezone set America/Kentucky/Louisville
sysconf timezone set /Etc/GMT+5

```



Note: SafeNet Network HSM uses POSIX-compliant time zone reference.

In normal conversation, you might refer to EST as GMT-5, but in POSIX notation it is GMT+5 which is UTC-05:00.

For more information on time zone abbreviations, please visit: https://en.wikipedia.org/wiki/List_of_tz_database_time_zones

The time system accepts local settings either as an offset from Greenwich Mean Time (/Etc/GMT+3 hours is the same as UTC-03:00, or /Etc/GMT-5 hours is the same as UTC+05:00, etc.) or as region/city/state names.

If you choose a named city time zone, 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. |

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.



Note: Syslog format is in accordance with RFC 5424.

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

Remote system logging allows you to send logs from your SafeNet Network HSM to a central syslog server configured on the network. Y

You can use the LunaSH **syslog remotehost {add | delete | list}** commands to specify which central syslog server you want to send the SafeNet Network HSM appliance logs to.

Configuring a Linux Syslog Server

Most Linux distributions include rsyslog as the standard syslog daemon.

Refer to your Linux server documentation for instructions that detail how to configure rsyslog on Linux.



Note: The remote host must have UDP port 514 open to receive the logging. Refer to the operating system and firewall documentation for your host for more information.

Configuring the Appliance to Send Logs to the Remote Syslog Server

To configure your appliance to send logs to the remote syslog server

1. On the SafeNet Network HSM appliance, run the following command:

```
lunash:>syslog remotehost add <target_collector_IP_or_hostname>
```
2. On the receiving or target system, start the syslog daemon or service to allow it to receive the logs from your SafeNet Network HSM appliance(s).

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:>
```

PREFACE

Appendix A: Configuration Long-form

This section documents the long-form, detailed, step-by-step instructions for configuring your SafeNet HSM hardware, before you begin using it with your application(s). These instructions do not make use of the One-step NTLS Setup that was introduced in release 6.2.1.

To ensure a trouble-free configuration, perform the following steps in the order indicated:

1. ["\[Step 1\] Planning Your Configuration" on page 1](#)
2. ["\[Step 2\] Configure Your Network Settings" on page 1](#)
3. ["\[Step 3\] Initialize the HSM " on page 1](#)
4. ["\[Step 4\] Set the HSM Policies" on page 1](#)
5. ["\[Step 5\] Create Application Partitions" on page 1](#)
6. ["\[Step 6\] Set the Partition Policies for Legacy Partitions" on page 179](#)
7. ["\[Step 7\] Create a Network Trust Link Between the Client and the Appliance" on page 183](#)
8. ["\[Step 8\] Enable the Client to Access a Partition" on page 191](#)
9. ["\[Step 9\] Configure PPSO Application Partitions" on page 205](#)
10. ["\[Step 10\] Set the Partition Policies for PPSO Partitions" on page 217](#)

Also review ["Optional Configuration Tasks" on page 220](#) for more configuration options.

[Step 1] Planning Your Configuration

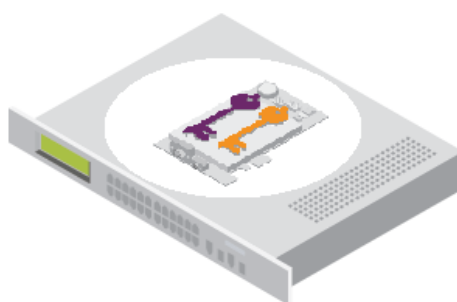
Before initializing your HSM, we suggest taking a moment to consider the following available features and options. Some would be inconvenient to change after your HSM is in service:

- ["Appliance Roles" below](#)
- ["Crypto Officer & Crypto User" on page 87](#)
- ["Domain Planning" on page 90](#)
- ["SafeNet PED Considerations" on page 1](#)
- ["PED-authenticated HSM Planning" on page 93](#)
- ["Password-authenticated HSM Planning" on page 98](#)

Appliance Roles

SafeNet Network HSM offers administrative roles external to the contained HSM, to oversee the management of the appliance that hosts the HSM, including network setup, system monitoring, and other tasks.

Appliance Role Summary



For the SafeNet Network HSM networked-appliance HSM, the roles fall under two main hierarchies:

- roles to access the appliance that contains the HSM and that provides the network connectivity; these are accessed through SSH or local serial connection, via the LunaSH or "lunash" command line, and include
 - the highest-level, full-access administrative role, called 'admin'
 - the medium-level operational administrative role, called 'operator', and

- the lowest-level observation-only administrative role, called 'monitor'
- roles that access the HSM, described in ["HSM Roles and Secrets" on page 87](#)

Within the SafeNet appliance, those appliance-level and HSM-level roles interact, where the access level of the role that is currently logged into the appliance, and using LunaSH (lunash), sees either the full set or a subset of HSM-using commands.

Thus, someone logged into the appliance as 'monitor' can see only reporting-type commands for the appliance (commands that show lists and status of subsystems), and can see only reporting-type commands for the HSM within the appliance.

Someone logged into the appliance as 'operator' can see and use most of the commands that the 'admin' user can access, at both the appliance and the HSM levels.

Someone logged into the appliance as 'admin' can see and use all possible commands affecting both the appliance and the contained HSM, including all commands that create and modify other roles, and that initialize the HSM.

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.

HSM Roles and Secrets

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 elements that you might wish to consider before committing to an HSM configuration.

Roles that access the HSM, the cryptographic engine within, or connected to, the host, include

- the 'HSM Administrator' or 'Security Officer' (SO) [Mandatory], responsible for initialization of the HSM, setting and changing of global Policies (based on the HSM's Capabilities), creation and deletion of application partitions
- the 'Auditor' [Optional], responsible for managing HSM audit logging, at "arm's length" (independently) from other roles on the HSM
- the 'application partition Security Officer' (SO) [Optional], responsible for creating other roles in the partition, resetting passwords, setting and changing partition-level Policies (based on the HSM's and the partition's Capabilities)
- the 'application partition Crypto Officer' [Mandatory], responsible for creating the Crypto User role, and for creating and modifying cryptographic objects in the HSM partition (see ["Crypto Officer & Crypto User"](#) below)
- the 'application partition Crypto User', responsible for using cryptographic objects (encrypt/decrypt, sign/verify...) in the HSM partition

In addition to the HSM roles listed above, certain other HSM-wide secrets exist for special purposes. Those include:

- the cloning domain, which determines whether the "cloning" (secure copy of cryptographic objects) operation is possible between two HSMs (which must share identical domain secrets) - applies to password-authenticated HSMs and to PED-authenticated HSMs; cloning is used in some forms of backup, as well as in HA
- the Remote PED vector (PED-authenticated HSMs only), which permits establishing a secure path for the HSM to access remotely-located SafeNet PED and PED Keys
- the Secure Recovery vector (PED-authenticated HSMs only), which permits controlled recovery from a real tamper incident, and also allows the HSM to be placed in, and securely recovered from, an induced 'tamper' state (Secure Transport Mode), for the most secure possible transport and storage of a SafeNet HSM and its contents.

Crypto Officer & Crypto User

An available security layer is required in some security and authentication schemes, as follows:

For those who need the additional distinction, the Partition Owner role (black PED Key) can optionally be subdivided into two further roles:

- Crypto Officer
- Crypto User

In the past, and continuing, the separation of roles on the SafeNet HSM follows the standard Cryptoki model:

- **appliance admin**

This is the basic administrative access to the a SafeNet HSM appliance. When you connect via ssh (putty.exe or other ssh utility), the SafeNet HSM presents the "login as:" prompt. The only ID that is accepted is "admin".

You must be logged in as the appliance "admin" before you can access further authentication layers such as HSM Admin, Partition Owner, Crypto Officer.

The appliance "admin" performs network administration and some other functions that do not require the additional authentication. Therefore, by controlling access to passwords (for a SafeNet HSM with Password Authentication) or to PED Keys (for a SafeNet HSM with Trusted Path Authentication), you can compartmentalize the various administrative and security roles.

- **HSM Admin**

HSM Admin has control of the HSM within the a SafeNet HSM appliance. To access HSM Admin functions, you must first be logged in as appliance admin.

In addition to all the other appliance functions, a user who has authenticated with the HSM Admin password (for a SafeNet HSM with Password Authentication) or the HSM Admin (blue) PED Key (for a SafeNet HSM with Trusted Path Authentication) can:

- create and delete Partitions,
- create and delete Partition Owners (black PED Key holders on a SafeNet HSM with Trusted Path Authentication only),
- backup and restore the HSM,
- change HSM Policies, etc.

- **HSM Partition Owner (or User)**

HSM Partition Owner has control of one or more Partitions (virtual HSMs) within the SafeNet HSM appliance. To access HSM Partition Owner functions, you must first be logged in as appliance admin.

In addition to all the other appliance functions, a user who has authenticated with the HSM Partition Owner (black) PED Key (for a SafeNet HSM with Trusted Path Authentication) can:

- modify partition policies
- activate a partition for use by Clients
- backup and restore Partition contents



Note: Both a SafeNet HSM with Password Authentication and a SafeNet HSM with Trusted Path Authentication have at least two layers of access control for an HSM Partition:

- the appliance admin login
- the Partition authentication



Note: SafeNetHSM with PED (Trusted Path) Authentication, splits the Partition access into two layers. The HSM Partition Owner (a concept that exists only for a SafeNet HSM with PED Authentication) first authenticates to the Partition with the appropriate black PED Key, then activates the Partition for Clients. Thereafter, each Client must further authenticate with the Partition Password (generated by SafeNet PED when the Partition is created).



Note: For SafeNet HSM with Password Authentication, the Partition Password is the only layer of authentication to a Partition. Therefore, any Client with that password has access to the Partition. What prevents a Client from manipulating objects on the Partition and performing Partition administration activities is the need to access the lunash command shell.



Note: Therefore, in both access-control models, a Client with the Password can connect and perform object generation and deletion, and can use objects (sign, verify, encrypt, decrypt), but they cannot perform Partition management operations unless they can also login to LunaSH (lunash) as admin.

- **Client**

A Client is a "working" or "production" user of one or more SafeNet Network HSM Partitions, that connects from a client computer (one that has set up a network trust link (NTL) by exchanging certificates and registering with the SafeNet Network HSM). If a Client can provide the Partition Password, it can generate, delete, and use cryptographic objects (keys and certificates) on the Partition, as long as the Partition is prepared to accept the connection.

In the case of SafeNet Network HSM with Password Authentication (assuming the HSM Partition has been previously created with the Password), the appliance simply needs to be powered on.

In the case of SafeNet Network HSM with Trusted Path Authentication (assuming the HSM Partition has been previously created and the Client given the Partition Password), the Partition must also be activated by the Partition Owner. That is, a Client, even with the proper Password cannot access a SafeNet Network HSM Partition unless that Partition has been placed in "activated" state by the HSM Partition Owner (using the black PED Key).

That authentication model continues unaffected, for those who prefer it. However an optional, enhanced Cryptoki model is also available, to separate the Partition Owner or Partition User role into a read-write entity and a separate read-only entity:

- **appliance admin**

(Same as appliance admin description above. No change.)

- **HSM Admin**

(Same as HSM Admin description above. No change.)

- **Crypto Officer** (full Read-Write access)

(same capabilities as HSM Partition Owner and Client in the default model)

As above for HSM Partition Owner, except that two separate Passwords can now (optionally) be associated with the black PED Key. In both cases, the black PED Key must be presented, and the administrator at the lunash command-line can:

- modify partition policies
- activate a partition for use by Clients
- backup and restore Partition contents

The Partition Password is presented when a Client application needs to use the Partition. In this model, there are two Passwords. The Crypto Officer Partition Password allows the Client to perform any crypto-graphic operation, both manipulation (generation, deletion, wrap/unwrap), and use (encrypt/decrypt, sign/verify).

The other password is used (along with the black PED Key) for the Crypto User. This is set by the HSM Admin when the Partition is created.

In operation, the Crypto Officer would log in at the management interface prompt for Partition maintenance tasks, and/or

a Client application could connect to a registered Partition (authenticating with the Crypto Officer Password) in order to generate and manipulate cryptographic objects in the Partition.

- **Crypto User** (or restricted Client user - Read-only)

If the Partition has been readied for access by the black PED Key, a Client can connect with a Client application, authenticating with the Crypto User Password (a challenge secret, generated on command by the SafeNet PED, similar to the Crypto Officer or Partition Owner Password that is generated on the SafeNet PED when a Partition is created).

The Crypto User Client can then make use of cryptographic materials already in the Partition (signing, verifying, encrypting, decrypting), but cannot manipulate those objects (no generating or deleting or wrapping/unwrapping).

This distinction differs from the old model, with just the one Partition Password, where Client users could not be restricted from generating and deleting keys and certificates.

Either model can be used. If you work in an environment that mandates the Crypto Officer / Crypto User distinction, it is available. If you have no need of the additional password, or if you have legacy applications that use the standard Cryptoki roles, then simply do not activate the Crypto Officer / Crypto User roles.

How the Roles are Invoked

By default, the Crypto User role does not exist, and so the black PED Key owner is HSM Partition Owner. You create a Crypto User (the restricted Client user) with the "partition createUser" command.

Bad Login Attempts

By default, both the Crypto Officer and the Crypto user can make 10 consecutive failed login attempts before invoking consequences. That is, the two bad-authentication counters are independent of each other.

Submissions of incorrect Partition Passwords (or Crypto Officer and Crypto User Passwords) are not counted as incorrect black PED Key attempts.



Note: The SafeNet HSM must actually receive some information before it logs a failed attempt, so if you merely forget to insert a PED Key, or provide a wrong-color key, then that is not logged as a failed attempt. When you successfully login, the bad-attempt counter is reset to zero.

Domain Planning

The cloning domain is a special-purpose secret that is attached to a partition on an HSM. It determines to which, and from which, other partitions (on the same HSM or on other HSMs) the current partition can clone objects. Partitions that send or receive partition objects by means of the cloning protocol must share identical cloning domain secrets. This is important for:

- cloning in backup and restore operations and
- synchronization in HA groups.

There is no provision to clone between an application partition and an HSM administrative partition, but you can apply the same domain secret for ease of administration. Password authenticated application partitions can clone partition contents one to the other, and PED authenticated application partitions can clone partition contents one to the other, but password authenticated HSMs (and their partitions) cannot perform cloning with PED-authenticated HSMs (and their partitions).

Cloning source	Cloning target					
	HSM Administrator partition A, cloning domain A	HSM Administrator partition B, cloning domain B	application partition 1, cloning domain A	application partition 1, cloning domain B	application partition 2, cloning domain A	application partition 2, cloning domain B
HSM Administrator partition A, cloning domain A	management objects	cannot clone domains not matched	N/A	N/A	N/A	N/A
HSM Administrator partition B, cloning domain B	cannot clone domains not matched	management objects	N/A	N/A	N/A	N/A
application partition 1, cloning domain A	N/A	N/A	yes (usually backup and restore)			
application partition 1, cloning domain B	N/A	N/A	cannot clone domains not matched	yes (usually backup and restore)		
application partition 2, cloning domain A	N/A	N/A			yes (usually backup and restore)	
application partition 2, cloning domain B	N/A	N/A				yes (usually backup and restore)

Characteristics of Cloning Domains

Password authenticated HSMs have text-string cloning domains for the HSM SO space and for any partitions that are created on the HSM. HSM and Partition domains are typed at the command line of the host computer, when required. Password authentication cloning domains are created by you.

PED authenticated cloning domains are created by a SafeNet HSM, which could be the current HSM, or it could be a previously initialized HSM that you wish to be in a cloning group with the current HSM.

PED authenticated HSMs have cloning domains in the form of encrypted secrets on red PED Keys, for the HSM SO space and for any partitions that are created on the HSM. The following characteristics are common to domains on all SafeNet HSMs.

- The HSM SO-space domain can be created at the HSM (therefore unique) at HSM initialization time, or it can be imported, meaning that it is shared with one-or-more other HSMs.
- The application partition domain can be created by the current HSM at partition creation time for legacy-style partitions or Partition SO role-creation time for PPSO partitions (therefore making it unique), or it can be imported, meaning that it is shared with one-or-more other HSM partitions.
- The application partition domain can be the same as the HSM SO domain or can differ.
 - For legacy-style partitions, where the HSM Administrator or Security Officer is also the SO of the application partition, it is appropriate to have the same domain for the HSM and for the partition(s).
 - For PPSO partitions, where the role of Security Officer for the application partition is deliberately separate from the role of HSM SO, it is appropriate that the HSM cloning domain and the application partition cloning domain would be different, and controlled by different people.
- The application partition domain can be the same as the domain of another partition on the same HSM (for HSMs that support multiple partitions) or can differ.

For PED authenticated HSMs, the domain secret for the SO space or for an application partition can be a single red PED Key, or it can be split (by the MofN feature) over several red keys, which are then distributed among trusted personnel such that no single person is able to provide the cloning domain without oversight from other trusted personnel.

In scenarios where multiple HSM partitions are in use, it can be useful to segregate those partitions according to department or business unit, or according to function groups within your organization. This ensures that personnel in a given group are able to clone or backup/restore only the contents of partitions sharing the domain for which they are responsible. Other functional groups, even with access to the same SafeNet HSM hardware have cloning or backup/restore access to their own domain partitions, but not to those of the first group... and vice-versa.

For Password authenticated HSMs, that sort of segregation is maintained entirely by procedure and by trust, as you rely on personnel not to share the domain text strings, just as you rely on them not to share other passwords.

For PED authenticated HSMs, the segregation is maintained by physical and procedural control of the relevant PED Keys that each group is allowed to handle.

It can pay to pre-plan how you will divide and assign access to HSM SO space and Partitions. Cloning Domain is one aspect of such access. There is rarely much call to store objects on the SO space, so the SO function is normally purely administrative oversight, and the decisions are straightforward. Each SO takes care of just her/his own HSM, or each SO can have oversight of multiple HSMs.

Partition access can also be straightforward, if you have no particular need to segregate access by groups or by functions or by geography or other descriptors. But, because partitions contain the working keys, certificates, and objects that are used in your business, it is more likely that some scheme must be devised and maintained to control who can do what with each HSM partition. Also, as mentioned previously, you might wish to spread out and reinforce responsibility by using MofN to ensure that administrative partition access can never be achieved by a single person operating alone. These considerations require that you plan how access controls are to be implemented and tracked, because the decisions must be made before you create the partitions.

Have your naming conventions and allotments planned out ahead of HSM initialization and partition creation, including a well-thought-out map of who should control cloning domain access for HSM SO spaces and for application partitions.

PED-authenticated HSM Planning

Planning for configuration of a PED-authenticated SafeNet HSM involves a number of layered, interlocking considerations that should be carefully thought through, in advance.

- Determine whether the HSM authentication secrets should fall under your organization's rules for password change cycles. For example, it could be a major undertaking to change 'passwords' for all PED Keys and their backup copies every couple of months.
- Determine your backup policy for PED Keys
 - how many copies should exist of each PED Key,
 - how they should be stored (on-site and off-site),
 - who has control/oversight of the backup copies of your HSM authentication.
- Decide whether application partitions should be owned and administered by the HSM SO (pre-firmware 6.22.0 legacy) or by a partition SO (with firmware 6.22.0 or newer, and the Per-partition SO CUF installed)
- Determine HSM and partition text labels, in keeping with your organization's requirements.
- Determine whether it is necessary or desirable to have split-secret, multi-person access control for any or all of the roles and secrets of the HSM, that is, whether MofN should be invoked.
- Determine whether it is necessary or desirable to invoke "something you know" secrets in addition to the "something you have" PED Key for any or all of the roles and secrets of the HSM, that is, whether PED PINs should be invoked.
- If PED PINs are used, determine, in advance how your organization's security policy deals with the departure or replacement of personnel who know the PED PINs.
- Determine which person or role within your organization will hold the PED Key(s) and passwords for each role
 - the SO of the HSM,
 - the SO of each application partition (optional),
 - the Crypto Officer and Crypto User, and
 - the Auditor (optional), as well as
 - the Cloning Domain(s),
 - the RPK (for optional Remote PED operation),
 - the SRK for optional tamper response or Secure Transport.
- Determine how PED Keys should be physically identified (which one is which copy), especially if you have invoked MofN.

SafeNet PED Planning

Plan your PED Key options and choices before you begin the actions that will invoke PED Keys.

The various PED Keys contain secrets that are created by an HSM, and are imprinted on the PED Key at the time that a triggering action is called - for example, both the HSM and a blue SO PED Key are imprinted with the HSM SO secret at the time the HSM is initialized. With the exception of the purple SRK PED Key, all of the other PED Key types can take a newly-created secret that is unique in the world at the time the HSM creates it.

Optionally, the PED dialog allows you to present a key with an existing secret (of the appropriate type for the current action) that was previously created by this HSM or by some other HSM. In that second case, the secret from the key is

imprinted on the HSM, and that key can now unlock its function (example: allow the SO to log in) on both the previous HSM and the current HSM. This can be repeated for any number of HSMs that you wish accessible by the one secret.

What each PED prompt means

Some questions/prompts from the PED when any key/access secret is first invoked are:

Reuse - do you wish to have the current HSM generate this secret, and imprint it on the PED Key (the "No" or do not reuse option), or do you wish to accept a secret (of the correct type) from the currently inserted PED Key, and imprint that secret onto the current HSM, making that secret common for this HSM and any others that recognize the same PED Key (the "Yes" or do reuse option)?

The decision is: do you wish this HSM to be accessed by the same secret that accesses this function/role on one or more other HSMs? Or do you wish this HSM to have a new, unique secret that is recognized by no previous HSM. Sometimes, it is advantageous to have a single secret for a group of HSMs managed by a single person. Sometimes, security or operational rules require that each HSM must have a different secret (for the role being configured).

The option to reuse an existing secret applies only within the same type of secret, so for example you cannot tell a partition to accept a secret from a blue SO PED Key. At partition creation, a partition must be imprinted either with a unique new key that also goes on a PED Key, or with a secret from an already-imprinted black PED Key.

The only exception, among the various PED Keys is the purple SRK PED Key, each of which is unique to its own HSM. No HSM can accept an SRV (the secret on the SRK) from outside. Each HSM creates its own.

MofN - do you wish to split the current secret over quantity N same-color PED Keys, such that quantity M of them will always be needed to assemble the full secret and authenticate that role? You invoke MofN by providing the M value and the N value using the PED Keypad, when prompted. You refuse MofN by setting the M value and the N value both to "1". MofN is the more secure choice, when you require multiple persons to be present (with their splits of the role secret) in order to access that role and perform its functions. No MofN is the more convenient choice, as only one secret-carrying key must be carried and tracked, per role.

Overwrite - during create/initialize/imprint events, when the PED has received answers to its preliminary questions, it prompts you to insert a key and press [Enter] on the keypad. This is the first point at which it actually looks at the inserted key. The PED then tells you what is on the inserted key (could be blank, could be any of several authentication secrets) and asks if you wish to overwrite. This is an opportunity to reconsider the key that you have inserted, before something irreversible happens. You can say "No" (don't overwrite what was found), remove the key, and go back to being prompted to insert a key. If you say "Yes" to overwrite what the PED just told you is on this inserted key, the PED gives you *another* chance to reconsider: "WARNING*** Are you sure...". The PED is very thorough about making sure that you do not accidentally overwrite a useful authentication secret.

PED PIN - At the point where it has been decided that you are not reusing key content, and you are or are not splitting the new secret across multiple keys, and that you are absolutely certain that you wish to write a new secret on the inserted key, the PED prompts you to type a PED PIN. The PED is about to write onto the key a secret that was just generated by the HSM. If you simply press [Enter] on the PED keypad, without typing any digits, you are providing no PED PIN, and the secret that goes onto the key is the secret as provided by the HSM. If you type any digits, before pressing [Enter] (minimum of 4 digits), then the typed digits (the new PED PIN) are XOR'd with the secret from the HSM, before the combined secret goes onto the PED Key. This means that the secret on the PED Key is not identical to the secret from the HSM, so in future you must always type those PED PIN digits to reverse the XOR and present the HSM with the secret it is expecting. With a PED PIN applied, the secret for that role is now two-factor - something you have (the version of the secret that is imprinted on the key) and something you know (the secret that you type in, to be XOR'd with the contained secret), to make the final secret that unlocks the HSM.

At this point, the key is imprinted. Now the PED inquires if you wish to duplicate the key you just made.

Duplicate - in general, you should always have duplicate keys for each role (or duplicate MofN sets, per role, if you chose to invoke the MofN split), so that you can have at least one off-site backup, and probably an on-site standby or backup set as well. Your security and operational policies will dictate how many sets you need. When the PED prompts to inquire if you wish to duplicate the current PED Key, you should be ready with the knowledge if you already have enough copies of that secret or if you need to make more. The more you make, the more you must track. But you must have enough to satisfy your organization's operational and security protocols.

The above paragraphs explain the meanings of each of the prompts that you would see from SafeNet PED while performing an action (like initialization) that imprints PED Keys with secrets. The following sections discuss some implications of the above choices for specific roles (PED Key colors).

HSM Initialization and the Blue SO PED Key

The first action that invokes SafeNet PED (which must be connected, as described in the SafeNet PED option section of the hardware setup chapter) is HSM initialization.

When you initialize, you are creating an SO (security officer) identity and space on the HSM. In most cases, this is an administrative position and the only keys or objects that are ever stored there are system keys, not user keys. The SO sets policy for the overall HSM, and creates partitions.

When creating an access secret for the SO, you are creating a secret for an administrator who sets up the HSM and then rarely is needed thereafter. You might have a single person who has the job of overseeing several HSMs, in which case, only the first HSM creates a secret to imprint on a blue PED Key. The second, and all future HSMs to be administered by that person (or role/job in your organization) would accept that secret from a provided blue PED Key, rather than creating their own unique SO PED Keys. In that situation, you would choose to "Reuse an existing keyset" when initializing every HSM after the first one.

Alternatively, you might have a very compartmentalized organization where a separate individual must have administrative authority over each HSM, so in that case you would use blank blue keys each time you initialized a new HSM, and each HSM would imprint its own uniquely generated SO secret onto a unique blue key. As well, you would have the opportunity to apply PED PINs to any or all of the unique SO PED Keys.

Each person who is to act as SO for an HSM must be able to access the appropriate blue PED Key when needed. Either they carry it with them, or they sign it out when they are using it and sign it back into a secure lockup. If PED PINs are in use, then each SO and each SO backup/alternate personnel must know the PED PIN(s) for every HSM in their charge.

If your organization enforces a policy of password changes at certain intervals, or at events like firings and personnel turnover, then you have options and requirements - you might need to change the secret on the PED Key (`hsm changePw` command) or you might satisfy the password-changing requirement by simply changing the PED PIN.

Furthermore, when you initialize an HSM with a new secret, you have the opportunity to split that secret using the MofN feature. In this way, you ensure that a certain minimum number of personnel must be present with their blue PED Keys whenever the SO must log in. While making that choice, you should choose "M" to be the smallest number that satisfies the requirement. Similarly, "N" should be large enough to ensure that you have enough "spare" qualified SO split holders that you can assemble a quorum even when some holders are unavailable (such as for business travel, vacations, illness). Just as with a single, non-split SO secret, you can apply PED PINs to each blue key in an MofN set. Consider, before you do, how complicated your administration and key-handling/key-update procedures could become.

Before you begin the HSM init process, have your blue PED Keys ready, either with an existing SO secret to reuse, or blank (or outdated secret) to be overwritten by a unique new SO secret generated by the HSM. At the same time, you

must also have appropriate red PED Keys ready, because assigning/creating a cloning domain for the HSM is part of the HSM init process. See the next section, below.

HSM Cloning Domain and the Red Domain PED Key

All the points, options, decisions listed above for the SO key apply equally to the Cloning domain key, with two exceptions.

First, you **MUST** apply the same red key Cloning Domain secret to every HSM that is to :

- clone objects to/from each other
- participate in an HA group (synchronization uses cloning)
- backup/restore.

By maintaining close control of the red PED Key, you control to which other HSMs the current HSM can clone.

Second, unlike the case of the blue SO PED Key secret and the black Partition Owner/User PED Key secret, there is no provision to reset or change a Cloning Domain. An HSM domain is part of an HSM until it is initialized. An HSM Partition domain is part of an HSM partition for the life of that partition. Objects that are created in an HSM with a particular domain can be cloned only to another HSM having the same domain.

Before you begin the HSM init process, have your red PED Keys ready, either with an existing cloning domain secret to reuse, or blank (or outdated secret) to be overwritten by a unique cloning domain secret generated by the HSM.

See ["Domain Planning" on page 90](#).

Partition Owner/User and the black PED Key

All the points listed above for the SO key apply equally to the black PED Key when an HSM partition is created.

The black PED Key Partition Owner/User secret secures the HSM partition to which it is applied, and all contents of the partition.

The black PED Key for a partition (or a group of partitions) :

- allows the holder to log in as the Partition Owner/User to perform administrative tasks on the partition
- set the partition "open for business" by Activating the partition - when a partition is activated, applications can present the partition challenge secret and make use of the partition

When a partition is created, after the black PED Key is imprinted, you are prompted to provide a domain for the new partition.

At your option, your partition can:

- take on the same Cloning Domain (red PED Key) as the HSM in which it resides
- take on a new, unique Cloning Domain, generated by the HSM at partition creation (no other partition can share objects with this partition or be configured in HA with this partition, until the newly created domain is shared),
- take on a cloning domain (from an existing, imprinted red PED Key) that already holds the domain secret for another partition - this is how you allow the new partition to accept objects from a Backup HSM or to be part of an HA group)

This is how you control which partitions (on the same or different HSMs) share a domain.

Regardless of whether the HSM (SO space) and the partition share a domain, it is not possible to copy/clone objects between the two. A shared domain between partitions allows you to clone between/among those partitions, and to make such partitions members of an HA group. All members of an HA group must share a common cloning domain.

On an HSM that supports multiple partitions, all partitions could have the same domain, or all could have different domains, or some combination could be in effect.

Before you begin the HSM init process, have your black PED Keys ready, either with an existing Partition Owner or User secret to reuse, or blank (or outdated secret) to be overwritten by a unique new partition Owner secret generated by the HSM. At the same time, you must also have appropriate red PED Keys ready, because assigning/creating a cloning domain for the partition is part of the partition creation process. See the previous section, above.

Remote PED Orange PED Key (RPK)

This key is not tied to a fundamental activity like initializing an HSM or creating a partition. Instead, if you don't expect to use the Remote PED option, you never need to create an orange PED Key.

If you do have a Remote capable SafeNet PED, and want to use it for remote authentication, rather than always having the PED locally connected to the HSM, then the HSM and the PED that is remotely hosted must share a Remote PED Vector (RPV). The RPV is generated by the HSM when you instruct it to set a PED vector and imprinted onto an orange PED Key, or it is accepted from an existing Remote PED Key and imprinted onto the HSM.

When you invoke "ped vector set" or similar command, to create/imprint a Remote PED Vector, the PED prompt sequence is similar to the sequence for the blue or black PED keys, with the same questions/choices for you to make about "reuse" (or a fresh, new secret), about MofN, about duplicates, etc.

Before you begin the PED vector init process, have your orange PED Keys ready, either with an existing RPV secret to reuse, or blank (or outdated secret) to be overwritten by a unique new RPV secret generated by the HSM. The first time you set an RPV for an HSM, the PED must be locally connected. After that, you can take the orange PED Key (and your other PED Keys for that HSM) to any host anywhere that has PedServer running and has a remote-capable SafeNet PED attached.

Auditor

The Audit role is completely separate from other roles on the HSM. It is optional for operation of the HSM, but might be mandatory according to your security regime. The Audit role can be created at any time, and does not require that the HSM already be initialized.

When you invoke audit init, to create/imprint an Audit role secret, the PED prompt sequence is similar to the sequence for the blue or black PED keys, with the same questions/choices for you to make about "reuse" (or a fresh, new secret), about MofN, about duplicates, etc.

Before you begin the Audit init process, have your white PED Keys ready, either with an existing Auditor secret to reuse, or blank (or outdated secret) to be overwritten by a unique new Auditor secret generated by the HSM.

Secure Recovery Purple PED Key (SRK)

The Secure Recovery Vector is imprinted onto a purple Secure Recovery Key, only if you have invoked SRK. The Master Tamper Key and the recovery components (one of which can be brought outside the HSM and kept on a purple PED Key) are explained elsewhere. What you need to know is that there is no need to create a purple PED Key unless you :

- need to enforce acknowledgment of tamper events by your personnel, before returning the HSM to service, or
- wish to invoke Secure Transport Mode.

When you invoke SRK, to remove one of the MTK recovery secret splits from the HSM and imprint it onto a purple PED Key, the PED prompt sequence DOES NOT include a "reuse" option. The purple PED Key is the only one that is unique to its HSM and cannot be reused. The secret is generated within the HSM and goes onto a purple PED Key (or several,

if you choose MofN), but there is no ability for the HSM to accept an already imprinted purple key secret that came from another HSM. SRKs are always unique. That is, you can make as many copies as you wish, but they will work with only one HSM in the world.

Other than that, the PED prompt sequence is similar to the sequence for the blue or black PED keys, with the same questions/choices for you to make about MofN, about duplicates, etc.

Before you begin the SRK process, have your purple PED Keys ready, either a blank key, or outdated secret, to be overwritten by a unique new Secure Recovery Vector generated by the HSM.

Other Considerations

In each case, have your materials and notes about your previously-made decisions on hand before you launch a command that invokes key creation or imprinting.

Predetermine which of your personnel will have access to which PED Keys, how many people should be required to perform a given authentication action, whether they will carry their PED Key(s), or will need to retrieve them from a secure lockup for each occasion that they are used, how many backup sets you expect to maintain.

Keep in mind that backups are good, but each backup set must be updated if the operational or master set is changed for any reason.

If your security policies do not require periodic changes to PED Key secrets (possible for any of the other PED Keys, but effectively impossible for red domain PED Keys), and if your physical and procedural security is strong enough, then it is quite possible to just create the set(s) of PED Keys that you need, and then not need to touch them again for years.

By contrast, if your policies demand periodic change, or if you think you might be forced to change PED Key secrets due to personnel departures or other events, then have a clear plan in place about how you will deal with such situations before you create your various PED Key sets.

Password-authenticated HSM Planning

Planning for configuration of a password-authenticated SafeNet HSM is straightforward.

- Determine whether the HSM authentication secrets should fall under your organization's rules for password change cycles.
- Decide whether application partitions should be owned and administered by the HSM SO (pre-firmware 6.22.0 legacy) or by a partition SO (with firmware 6.22.0 or newer, and the Per-partition SO CUF installed)
- Determine HSM and partition labels, in keeping with your organization's requirements
- Determine passwords for each role
 - the SO of the HSM,
 - the SO of each application partition (optional),
 - the Crypto Officer and Crypto User,
 - and the Auditor (optional))
- Determine the cloning domain for each partition.

HSM Initialization

When you initialize, you are creating an SO (security officer) identity and attaching it to the Admin partition on the HSM. This is an administrative position and the only keys or objects that are ever stored there are system keys, not user keys. The SO sets policy for the overall HSM, and creates partitions.

When creating an access secret for the SO, you are creating a secret for an administrator who sets up the HSM and then rarely is needed thereafter. You might have a single person who has the job of overseeing several HSMs, in which case you could re-use the HSM SO password.

In the legacy model, the HSM SO is also the SO of an application partition that is created on the HSM. That means the SO can see application partition contents.

In the new, Per-Partition SO (PPSO) model, the SO of the partition is a completely separate role from the HSM SO. As long as they do not use the same secret, the HSM SO is completely excluded from the application partition. This separation of roles is important in some organizations.

HSM Cloning Domain

Like all secrets for a Password-authenticated SafeNet HSM, the cloning domain is a simple text string. It governs whether an HSM can clone its contents to another HSM (for backup, or for HA). There is no provision to change the cloning domain, without re-initializing, unlike a password for one of the roles, which can be reset or changed when desired.

You have the option to use the same cloning domain for the HSM as for an application partition on that HSM, or different domain secrets, if desired.

Application Partition Owner or Crypto-Officer/Crypto-User

SafeNet HSM application partitions can have a single "Owner" role that has unrestricted administrative and cryptographic access to the partition, or you can choose to divide the access into an unrestricted Crypto Officer and restricted Crypto User role.

A Password-authenticated HSM's application partition has a single text string for Owner or Crypto Officer that grants both administrative access and application access to the partition. It has a single text string for Crypto User that grants both restricted administrative access and restricted application access to the partition. This contrasts with a PED-authenticated application partition, where a black PED Key allows administrative access as Owner/Crypto Officer, while a separate challenge secret is used by unrestricted client applications, and a black PED Key allows administrative access as Crypto User, while a separate challenge secret is used by restricted client applications.

Application Partition Cloning Domain

The application partition requires a cloning domain, which must match the cloning domain of any other application partition (on any HSM) to which it should be able to clone objects. The domain is required to match for backup or for HA group creation and operation.

See ["Domain Planning" on page 90](#).

Auditor

The Audit role is completely separate from other roles on the HSM. It is optional for operation of the HSM, but might be mandatory according to your security regime. The Audit role can be created at any time, and does not require that the HSM already be initialized.

Effect of PPSO on SafeNet Network HSM

The older way - The legacy pattern for SafeNet Network HSM configuration is that it is made known that an application partition is needed and the appliance administrator, who is also the HSM SO does everything and hands the application owner the finished product, an address to connect and a text secret for crypto application access to the partition.

It is the HSM SO, connected to the appliance via SSH to a LunaSH (lunash:>) session, who

- configures everything related to the appliance outside the HSM,
- creates the appliance certificate
- initializes the HSM,
- creates the partition, complete with Crypto Officer /"Owner", and possibly Crypto User, if desired,
- adjusts Partition policies if necessary,
- guides the application owner through the NTLS certificate exchange and registration of client and partition, and
- communicates the partition's application access secret (sometimes called the challenge secret) to the remote owner of the application that is to use the partition.

The various management functions (including the partition domain and the Crypto Officer authentication) might be retained by the HSM SO, or might be given to some other person, depending on the organization's requirements. The administrative functions were traditionally accessed via LunaSH (lunash:>). The HSM SO remains the ultimate owner of the application partition, with visibility into the partition.

The newer way - For Per-Partition Security Officer (PPSO), the initial steps are the same to set up the appliance, create a certificate, and initialize the HSM. All these actions are identical to above, and are performed at the appliance via SSH connection to a LunaSH session (lunash:>), as above. When someone wants a partition for use by an application,

- the application owner sends a request to the SafeNet Network HSM admin, via e-mail, attaching a client certificate that they have generated
- the HSM SO creates an application partition, specifying that the partition is to have its own SO (partition create - haspso)
- the appliance admin (also the HSM SO) registers the received client certificate against the created partition; this is the final action done in LunaSH.
- the created partition is an empty structure, with no identities associated
- the appliance admin sends the appliance server certificate to the client application owner, along with the contact information (IP or hostname) via return e-mail, including instructions for the succeeding steps (or directions to the relevant guide in these instructions).
- the client application owner has SafeNet HSM Client installed and uses the supplied utility to create the client end of the NTLS connection
- the client application owner uses lunacm to discover and select the cryptographic slot that represents the remote, empty partition to which they have been given access [the actions that follow are identical for a remote SafeNet Network HSM partition or for a locally installed/connected HSM partition]
- the client application owner uses the role command to create the Partition SO identity and cloning domain for the partition
- the client application owner, logs in as the Partition SO and optionally uses the "partition changepolicy" command to adjust any partition policies that need adjustment

- the client application owner, logged in as the Partition SO, uses the role command to create the Crypto Officer identity for the partition
- the client application owner optionally logs in as Crypto Officer and creates a Crypto User
- the client application owner provides either the Crypto Officer or Crypto User text string challenge secret to the application, which uses it to perform cryptographic operations against the currently-selected crypto slot.

[Step 2] Configure Your Network Settings


In this chapter you will gather the needed information and then set the values that allow your HSM appliance to work within your network, to connect to external services (like NTP), and prepare it to engage in secure communication links.

Gather appliance network setting information

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

- New appliance admin Password

HSM Appliance Network Parameters

- the IP address assigned to this device (if you are using static IP, which is recommended)
- the hostname for the HSM appliance (registered with network DNS)
- domain name
- default gateway IP address
- DNS Name Server IP address(es)
- Search Domain name(s)
- device subnet mask
- Ethernet device (use eth0, which is the uppermost network jack on the HSM appliance back panel, closest to the power supply, and is labeled **1** )

DNS Entries

- Ensure that you have configured your DNS Server(s) with the correct entries for the appliance and the client.

If you are using DHCP, then all references to the Client and the HSM appliance (as in Certificates) should use hostnames.

Client Requirements

- If you are using a client workstation with Linux or UNIX, then SSH (secure shell) and the scp utility, should be installed and ready to use (normally they are provided with the operating system).
- If you are using a Windows-based workstation, then the freeware PuTTY utility suite is supplied in our SafeNet HSM Client Software, and is installed in c:\Program Files\SafeNet\LunaClient\putty.exe.
The pscp utility is also included in SafeNet HSM Client Software installer, and is required for this installation.

Go to ["Recommended Network Characteristics" on the next page](#)

Recommended Network Characteristics

Determine whether your network is configured optimally for use of SafeNet appliances.

Bandwidth and Latency Recommendation

Bandwidth

- Minimum supported: 10 Mb half duplex
- Recommended: at least 100 Mb full duplex - full Gigabit Ethernet is supported



Note: Ensure that your network switch is set to AUTO negotiation, as the SafeNet appliance negotiates at AUTO. If your network switch is set to use other than automatic negotiation, there is a risk that the switch and the SafeNet appliance will settle on a much slower speed than is actually possible in your network conditions.

Network Latency

- Maximum supported: 500ms
- Recommended: 0.5ms

About Latency and Testing

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

Here is a description of one common cause of such a situation, and what you can do about it.

When you disconnect the network cable between any SafeNet appliance and a switch, and then reconnect, traffic should resume immediately, but with certain network switch configurations it might take 30 seconds for traffic to resume.

The problem here is at the switch (and not the SafeNet appliance). See <http://www.cisco.com/warp/public/473/12.html#bkg> for some descriptions of Cisco switches. If the switch is configured to run the Spanning Tree Protocol on the port (which appears to be the default configuration, at least for Cisco switches), then there is a delay of about 30 seconds while it runs through a series of discovery commands and waits for responses. The switches can be configured to run in "PortFast" mode in which the Spanning Tree Protocol still runs on the port, but the port is placed directly into 'forwarding mode' and starts the traffic flowing immediately.

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

Go to "[Power-up the HSM Appliance](#)" below .

Power-up the HSM Appliance

Instructions on this page assume that the HSM appliance has been installed, including

- **power connections** [We suggest that each of the two power supplies be connected to an independent electrical

source, and that at least one of those sources should be protected by UPS (uninterruptible power supply) and generator backup.],

- **connection to your network** [gigabit or 100 megabit ethernet], and
- **a null-modem serial connection** between the HSM appliance's serial Console Port and your administration computer or a terminal [recommended option - this is for convenience, during initial setup, so your administrative connection remains active when you assign new IP addresses; later, you would need a local serial link if you ever need to log in to the Recover account].

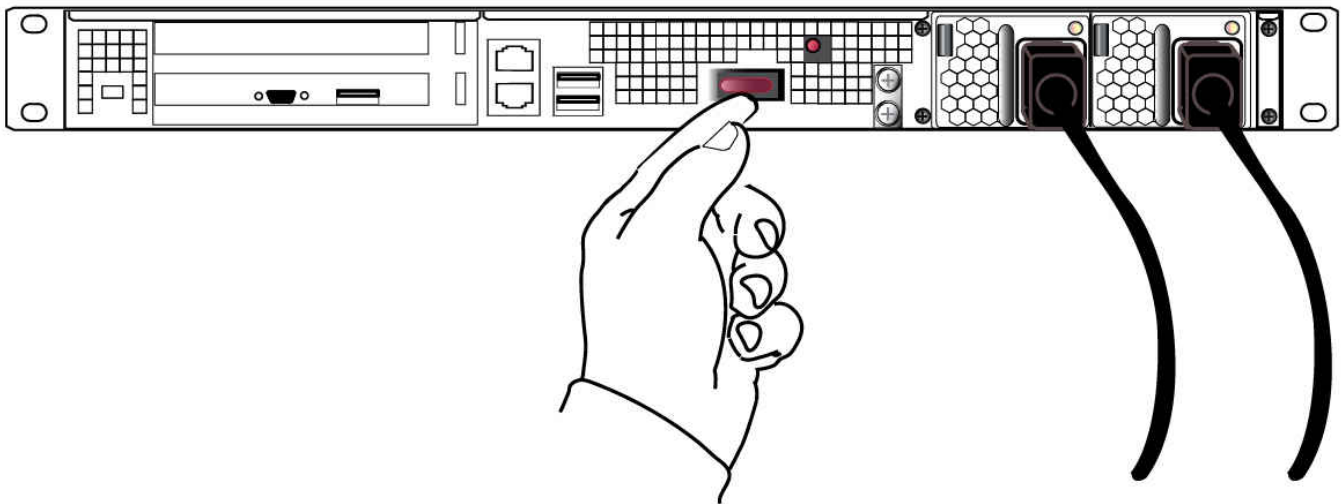
The following instructions require the HSM appliance to be connected and running.

Power On Instructions for the SafeNet Network HSM Appliance

If the appliance is currently powered off, perform the following actions.

Power switch

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



If the appliance does not immediately begin to start up, press and release the START/STOP switch near the center of the back panel (marked with the symbol below). The HSM appliance begins to power up.



Network LEDs



The “Network” LEDs glow or blink to indicate the exchange of traffic. The network LEDs do not illuminate if there is no network connection (check your network cable connections on the back panel and at hub or switch). Here is a summary.

Ethernet connector LED	State Indicated	Indication
NIC 1 (Right)	Activity status	Green (Blinking): NIC1 activity detected
		Off : NIC1 is not active, or LAN cable has no connection
NIC 1 (Left)	Speed range	Orange : 1G
		Green : 100M
		Off : 10M/No connection
NIC 2 (Right)	Activity status	Green (Blinking): NIC2 activity detected
		Off : NIC2 is not active, or LAN cable has no connection
NIC 2 (Left)	Speed range	Orange : 1G
		Green : 100M
		Off : 10M/No connection

The front-panel LCD ("[Front-panel Display](#)" on page 16) begins showing activity, then settles into the ongoing system status display, once the appliance has completed its boot-up and self-test activity.

Power Off

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



Note: Never disconnect the power by pulling the power plug. Always use the START/STOP switch.

To switch off the HSM appliance from the lunash command line, use the command:

```
lunash:> sysconf appliance poweroff
```

Next, see ["Open a Connection" below](#).

Resuming appliance power

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 by a power failure, or because 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 automatic resumption from power outage would never be needed, because [adhering to best practices for mission-critical equipment] 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.

Open a Connection

Perform your initial configuration via direct serial connection to the SafeNet appliance. Once network parameters are established, you can switch to an SSH session over your network.

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

- The specific IP address, randomly assigned to your SafeNet appliance by an automated testing harness during final factory testing, is unknown.
- Configuring network settings via SSH, in addition to requiring the original IP address, necessarily involves losing that connection when a new IP is set.
- A direct serial connection is the only route to log into the "recover" account, in case you ever lose the appliance's admin password and need to reset. Therefore, you should verify, before you need it, that the connection works - performing the appliance's network configuration is an ideal test.
- Similarly, if you ever need to issue the `hsm factoryreset` command, you must be connected through a local serial console for that command to be accepted.

To open a connection

1. Connect a null-modem serial cable (supplied) between the serial port on the HSM appliance front panel and a dumb terminal or a PC (for example a laptop) that will serve as the administration computer.



Note: A standard null-modem serial cable with DB9 connectors is included with the HSM appliance, as is a USB-to-serial adapter if needed. For security reasons, the USB port on the SafeNet Network HSM appliance recognizes only SafeNet HSMs and peripheral devices - therefore it is prohibited from supporting general USB operations and thus does not accept a serial console link; the 9-pin serial connector must be used.

2. Use a terminal emulation package provided with your operating system. Set the Serial connection parameters:

- Serial port baud rate: 115200
 - N,8,1 (no parity, 8 data-bits, one stop-bit)
 - VT-100 terminal emulation
 - hardware flow control selected.
3. When the connection is made, the HSM appliance login prompt appears. [DEFAULTHOSTNAME]lunash:> The [DEFAULTHOSTNAME] is replaced by the new hostname that you assign to your HSM appliance, later in these instructions. The prompt changes the next time you start a secure command-line interface connection.



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

Now that you have established a connection, go immediately to the next page to log in as “admin” and begin configuring. Next, see ["First Login and Changing Password" below](#).

First Login and Changing Password

Following the instructions in the previous pages, you have already:

- gathered the necessary network and security information
- made a connection (preferably serial) between your administration computer and your HSM appliance.

When you have connected to the HSM Server, the onboard secure Command Line Interface (with the lunash:> prompt) is independent of the platform (Linux, BSD, Windows, Solaris, HP-UX or AIX) that you used to connect (however, we assume that most lab/server rooms have a Linux or Windows PC available)

Password defaults	
Admin (appliance) default password	PASSWORD (via local serial link or via SSH)
Operator (appliance) default password	PASSWORD (via local serial link or via SSH)
Monitor (appliance) default password	PASSWORD (via local serial link or via SSH)
Recover account (appliance) default password	PASSWORD (accessed via local serial link only)

To login to the appliance

1. At the prompt, log in as “admin”. The initial password is “PASSWORD” (without the quotation marks).

```
login as: admin admin@<hostname>'s password: PASSWORD
```
2. For security, you are immediately prompted to change the factory-default password for the ‘admin’ account.

```
SafeNet Network HSM 5.4.0-14 [Build Time: 20131223 11:55]
```

```
Authorized Use Only
```

```
[localhost] ttyS0 login: admin
```

```
Password:
```

```
You are required to change your password immediately (root enforced)
```

```
Changing password for admin
```

```
(current) UNIX password:
```

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:

Last login: Mon Jan 30 11:24:00 from 172.20.10.180

SafeNet Network HSM 5.4.0-14 Command Line Shell - Copyright (c) 2001-2013
SafeNet, Inc. All rights reserved.

Command Result: 0 (Success)

[local_host] lunash:>

(The above represents a local serial connection; text will differ slightly for an SSH connection)



Note: The username and passwords are case-sensitive.



Note: To protect the HSM appliance and its HSM from vulnerabilities due to weak passwords, new passwords must be at least eight characters in length, and must include characters from at least three of the following four groups:

- lowercase alphabetic (abcd...xyz)
- uppercase alphabetic (ABCD...XYZ)
- numeric (0123456789)
- special (non-alphanumeric, -_!@#\$%&*...)



Note: You must login within two minutes of opening an administration session, or the connection will time out.

3. Record the new password on a worksheet.



CAUTION: Keep your passwords secure, as you would for any device.



Note: If you forget your password, you can use a local serial connection to login to the Recover account. See ["Forgotten Passwords / Lost Authentication" on page 54](#).

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

Example – lunash Command

lunash:>?

The following top-level commands are available:

Name	(short)	Description
help	he	Get Help
exit	e	Exit Luna Shell
client	c	> Client
hsm	hs	> Hsm
htl	ht	> Htl
my	m	> My
network	ne	> Network
ntls	nt	> Ntls
package	pac	> Package
partition	par	> Partition
service	se	> Service
status	sta	> Status
stc	stc	> Secure Trusted Channel
sysconf	sysc	> Sysconf
syslog	sysl	> Syslog
token	t	> Token
user	u	> User

Keywords which must be used as the first argument on the command line.

Type "help" (without the double quotes) followed by a command name for further information. For example: type "help help" for help on the help command. Note that a question mark ("?") can be used as an alias for "help".

Command Result : 0 (Success)

Go to ["Set the System Date and Time and SSH Certificate"](#) below

Set the System Date and Time and SSH Certificate

Before proceeding with HSM and HSM Partition setup, ensure that the HSM Server's system date, time and timezone are appropriate for your network. Setting correct system time is important because the next step is to generate your own server certificate. The certificate becomes valid at the time of its creation, which is recorded as part of the certificate, as a GMT value. If your local time is set with an inappropriate local timezone, then the GMT time on the certificate could be incorrect by several hours. When other systems (clients) attempt to reference your certificate, they might find that it has not yet become valid.

To set the date and time

1. First, verify the current date and time on the HSM Server, to see if they need to change.

At the lunash prompt, type the command:

```
lunash:> status date
```

which returns the current settings of date, time and timezone.

If desired,

```
lunash:> status time
```

and/or

```
lunash:> status zone
```

can also be used.

2. If the date, time, or timezone are incorrect for your location, change them using the `lunash sysconf` command. For example:

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



Note: You must set the timezone before setting the time and date, otherwise the timezone change adjusts the time that you just set.



Note: For a new SafeNet Network HSM appliance, or for one that has been factory reset, the steps occur in the order presented here [set the date and time, configure the IP, generate certs, connect, initialize the HSM...]. However, if the SafeNet Network HSM has been used before, then it might have been initialized with the option `.-authtimeconfig`, which requires that the SO/HSM-Admin be logged in before you are allowed to set time/timezone. If that is the case, then you will need to log in with the old SO credentials, or initialize the HSM first, before you can set time and timezone.

Timezone Codes

A list of timezone codes is provided in the *Appliance Administration Guide*.

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

The code that you must apply from the list in the appendix may not look exactly like the code displayed by `"status date"`. For example, `"status date"` shows EDT (i.e., Eastern Daylight Time), but to set that you must type `"EST5EDT"`, or `"Canada/Eastern"` or `"America/Montreal"` – a number of values produce the same setting.

3. Use `sysconf time` to set the system time and date, `<HH:MM YYYYMMDD>` in the format shown.

Note that the time is set on a 24-hour clock (00:00 to 23:59).

```
lunash:> sysconf time 12:55 20140410
Sun April 10 12:55:00 EDT 2014
```

Possible alternate scenario

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

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

That message appears only if the HSM has been previously initialized with the `.-authtimeconfig` option set. The work-around at this stage is to run the command `hsm init -label <yourlabeltext>` without the `.-authtimeconfig` option, which releases that flag. That is, you can just skip ahead in these instructions and perform your intended initialization out of order, and then set the appliance time and zone, and carry on. We chose an order for these configuration instructions that is usually convenient and easy to understand, but having the system time set before initializing is not required. You can perform those actions out of order. It is important to have the time set before you create certificates, later on.

Network Time Protocol [optional]

To use NTP, add one or more servers to the HSM appliance's NTP server list, and then activate (enable) the servers. Use the `sysconf ntp` command as follows:

Add servers

```
lunash:> sysconf ntp addserver <hostnameoripaddress>
```

Activate servers

```
lunash:> sysconf ntp enable
```



Note: If you wish to use Network Time Protocol (NTP), you must set the system time to within 20 minutes of the time given by the servers that you select. If the difference between NTP server time and the HSM appliance time is greater than 20 minutes, the NTP daemon ignores the servers and quits.

Drift correction for the system clock

If you require that your appliance's system clock be as correct as is practical, but are unable to use NTP for the most accurate timekeeping possible, then you might wish to use the system's clock-drift correction protocol. See ["Correcting Time Drift" on page 61](#) in the *Appliance Administration Guide* for further information.

Create a new SSH Certificate



Note: All SafeNet Network HSMs come from the factory with the same SSH key. For proper security, run the `sysconf regencert` command before configuring your system for first use.

4. Set a new SSH certificate for your appliance by running `sysconf regencert` :

```
lunash:>sysconf regencert
```

```
WARNING !! This command will overwrite the current server certificate and private key.
           All clients will have to add this server again with this new certificate.
If you are sure that you wish to proceed, then type 'proceed', otherwise type 'quit'
```

```
> proceed
Proceeding...
```

```
ERROR. Partition named "Cryptoki User" not found
```

```
'sysconf regenCert' successful. NTLS and STC must be (re)started before clients can connect.
```

```
Please use the 'ntls show' command to ensure that NTLS is bound to an appropriate network
device or IP address/hostname
for the network device(s) NTLS should be active on. Use 'ntls bind' to change this binding if
necessary.
```

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

Go to ["Configure the IP Address and Network Parameters" on the next page](#).

Configure the IP Address and Network Parameters

The HSM appliance is pre-configured with network settings left over from our manufacturing process and not recommended for your production network. The following procedure assumes that your network uses DNS. If you are configuring without a DNS server available, some of the commands on this and subsequent pages might be affected.

The SafeNet Network HSM supports port bonding, which allows you to bond eth0 and eth1 into a single port, bond0, to provide redundancy. See ["SafeNet Network HSM Appliance Port Bonding" on page 41](#) for configuration instructions.



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

1. Use the `network show` command to display the current settings, to see how they need to be modified for your network.

```
lunash:>network show
```

```

Hostname:          "mylunasa6"
Domain:            "amer.sfnt.local"

IP Address (eth0): 172.20.17.200
HW Address (eth0): 00:15:B2:A1:AC:00
Mask (eth0):       255.255.255.0
Gateway (eth0):    172.20.17.10

Name Servers:      172.20.10.20      172.16.2.14
Search Domain(s):  amer.sfnt.local  sfnt.local
```

```
Kernel IP routing table
```

Destination	Gateway	Genmask	Flags	Metric	Ref	Use	Iface
172.20.17.0	0.0.0.0	255.255.255.0	U	0	0	0	eth0
0.0.0.0	172.20.17.10	0.0.0.0	UG	0	0	0	eth0

```
Link status
```

```
eth0: Configured
```

```
Settings for eth0:
```

```

Supported ports: [ TP ]
Supported link modes:  10baseT/Half 10baseT/Full
                      100baseT/Half 100baseT/Full
                      1000baseT/Full

Supports auto-negotiation: Yes
Advertised link modes: 10baseT/Half 10baseT/Full
                      100baseT/Half 100baseT/Full
                      1000baseT/Full

Advertised auto-negotiation: Yes
Speed: 100Mb/s
Duplex: Full
Port: Twisted Pair
PHYAD: 2
Transceiver: internal
Auto-negotiation: on
Supports Wake-on: pumbg
Wake-on: g
Current message level: 0x00000007 (7)
Link detected: yes
```



```
eth1: Not configured
```

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

2. Use `network hostname` to set the hostname of the HSM appliance (use lowercase characters).

```
lunash:> network hostname myluna3
```



Note: To access the HSM appliance, the hostname must be resolvable to an IP address on your network. See your Network Administrator for assistance with completing this step.



Note: The `net hostname` command expects a single-word text string. If you supply a name that includes a space, all text after the space is ignored. For example, if you typed: `net hostname host name` the system would assign a hostname of "host". Therefore, if you want "host name", use "host_name" or "host-name" or "hostname" or similar.



Note: Enter a meaningful hostname to allow you to identify and manage multiple SafeNet appliances in your network.

3. Use `network domain` to set the name of the network domain in which the HSM Server (appliance) is to operate.

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

4. Use `'network dns add nameserver'` to set the Nameserver IP Address (address for the local name server).

```
lunash:> net dns add nameserver 192.168.1.3
```

(substitute an appropriate address for the example; ask your Network Administrator).



Note: Your network could have multiple DNS name servers. Repeat this step for any additional name servers.



Note: This command manually sets a DNS parameter for the HSM appliance. If you elect to use a DHCP server (see the `net -interface` command later in this section) rather than static IP, then this parameter is overwritten for the HSM appliance. In general, we strongly recommend against using DHCP for HSM appliances.

5. Use `net dns add searchdomain` to set the DNS Search Domain (the search list to be used for hostname lookups).

```
lunash:> net dns add searchdomain safenet-inc.com
```



Note: Setting the Search Domain is important so that you can use short names for your client machines.



Note: Your network could have multiple DNS search domains. Repeat this step to add all search domains.



Note: This command manually sets a DNS parameter for the HSM appliance. If you elect to use a DHCP server (see the `net -interface` command later in this section) rather than static IP, then this parameter is overwritten for the SafeNet Network HSM.



6. Use `network interface` to change network configuration settings.

All of the `network interface` parameters are required for the IP setup of the ethernet device, and must be set at the same time for the HSM appliance to connect with your network.

```
lunash:>net interface -device eth0 -ip 192.168.11.82 -netmask 255.255.0.0 -
gateway 192.168.1.1
```

Use addresses and mask values as provided by your network administrator.



Note: The first [top] ethernet port (eth0) and the [bottom] ethernet port (eth1) on the HSM appliance's back panel, are labeled **1**  **/2** .

If you choose to configure the second ethernet port (eth1), repeat the `network interface` command, above, substituting 'eth1' and the appropriate address for that device. Even if you do not have a need for the second ethernet port, you should configure it, specifically to a test network (e.g., `network interface -device eth1 -ip 192.168.1.254 -netmask 255.255.255.0`) so that it does not affect the behavior of other SafeNet features (e.g., remote PED).



Note: If either interface is configured to use DHCP, then the DNS parameters are overwritten for the entire HSM appliance. It is not possible to have manual settings preserved for one interface, while DHCP-derived settings are used for the other. In general, we recommend against using DHCP for HSM appliances.



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

View the new network settings with `network show`.

```
lunash:> network show
```

The `network show` command (described earlier) displays the current settings, so you can verify that they are now correct for your environment before attempting to use them.

(Next, go to ["Make Your Network Connection" below](#))

Make Your Network Connection

If you have been connecting via serial terminal, and the direct administration connection, to configure the HSM Server, you can now make an ethernet connection to your network.

To make a network connection to the appliance

1. Connect the ethernet cable to the upper ethernet port on the HSM appliance back panel and use ssh to open a

session on the HSM appliance.

2. Login as admin.
3. Verify correctness of your network setup by pinging another server (with the `lunash net ping <servername>` command) and having the other server ping this HSM appliance. Try pinging by IP address, if pinging by hostname is not successful. If your company uses nameservers, but you are unable to ping by hostname, then verify the "Name Servers" displayed by `net show`.



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

4. Verify your Client's network configuration by attempting to ping the HSM appliance by hostname and by IP address, from the Client. Repeat for each Client where the Client Software was installed.

[OPTIONAL] Once you know your network setup is correct, you can invoke network time protocol. To use NTP, you must add one or more servers to the HSM appliance's NTP server list, and then activate (enable) the servers. Use the `sysconf ntp` command as follows:

Add servers

```
lunash:> sysconf ntp addserver <hostname-OR-ipaddress>
```

Activate servers

```
lunash:> sysconf ntp enable
```

If you then check your NTP status with **`sysconf ntp status`**, you might see immediate success (return code 0), or you might get an error message like this...

```
[myLuna] lunash:>sysconf ntp status
NTP is running
NTP is enabled
```

Peers:

```
=====
remote refid st t when poll reach delay offset jitter
=====
```

```
*LOCAL(0) .LOCL. 10 1 8 64 1 0.000 0.000 0.000
time-c.timefreq .ACTS. 1 u 7 64 1 78.306 -55560. 0.000
=====
```

Associations:

```
=====
ind assid status conf reach auth condition last_event cnt
=====
```

```
1 21859 963a yes yes none sys.peer sys_peer 3
2 21860 9024 yes yes none reject reachable 2
=====
```

NTP Time:

```
=====
ntp_gettime() returns code 0 (OK)
time d1504c28.95777000 Wed, Apr 14 2014 12:22:00.583, (.583854),
maximum error 7951596 us, estimated error 0 us
```

```
ntp_adjtime() returns code 0 (OK)
  modes 0x0 (),
offset 0.000 us, frequency 0.000 ppm, interval 1 s,
maximum error 7951596 us, estimated error 0 us,
status 0x1 (PLL),
time constant 2, precision 1.000 us, tolerance 512 ppm,
=====
```

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

Note: The return code "5 (ERROR)" indicates a gap between your system time and the NTP server's time. You can expect one of two outcomes:



- if the initial time-gap between your appliance and the server is greater than twenty minutes, the appliance gives up and never synchronizes with that server
 - if the initial time-gap is less than twenty minutes, the appliance synchronizes with the server, slowly, over several minutes; this ensures that there is no sudden jump in system time which would be unwelcome in your system logging.
-

When your connection is working , go to ["Generate a New HSM Server Certificate" below](#).

Generate a New HSM Server Certificate

Although your HSM appliance came with a server certificate, good security practice dictates that you should generate a new one.

To generate a new server certificate

1. Use `sysconf regenCert` to generate a new Server Certificate:

The command `sysconf regenCert` (with no IP address appended) is suitable if your network is using DNS and, during the execution of the regeneration command, the HSM appliance is able to retrieve correct DNS information about itself. If DNS is not used, or it does not know about the HSM appliance, an invalid certificate will be generated that prevents NTLS running later.

In situations where DNS is not used or contains unreliable information, use this form of the command "`sysconf regenCert <ip_of_hsm_appliance>`" to generate a usable NTLS certificate.

`Sysconf regenCert` (without the IP argument) populates the CN field of the server's certificate with the unqualified hostname of the appliance. If the appliance is set up correctly for use in a DNS environment, then it will work. The command does not check.

`Sysconf regenCert` with the IP argument results in a certificate with the appliance's IP address in the CN field.

Using SafeNet Network HSM with the link configured for IP-only speeds the NTLS client connection lookup, and bypasses such potential issues as transient DNS lookup failures and typing errors.

```
lunash:>sysconf regencert
```

```
WARNING !! This command will overwrite the current server certificate and private key.
All clients will have to add this server again with this new certificate.
```

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

```
> proceed
Proceeding...
```

```
ERROR. Partition named "Cryptoki User" not found
```

```
'sysconf regenCert' successful. NTLS and STC must be (re)started before clients can connect.
```

```
Please use the 'ntls show' command to ensure that NTLS is bound to an appropriate network
device or IP address/hostname
for the network device(s) NTLS should be active on. Use 'ntls bind' to change this binding if
necessary.
```

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

- From the factory, the network trust link service (NTLS) is bound to the loopback device, by default. In order to use the appliance on your network, you must bind the NTLS to one of the two Ethernet ports, ETH0 or ETH1, or to a hostname or IP address. You can use the `ntls show` command to see current status.

Use `ntls bind` to bind the service:

```
[luna23] lunash:>ntls bind eth0

Success: NTLS binding network device eth0 set.

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

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

> proceed

Proceeding...

Restarting NTLS service...

Stopping ntlsl: [ OK ]

Starting ntlsl: [ OK ]

Command Result : 0 (Success)

[luna23] lunash:>
```

Or, an example using an IP address:

```
[myluna] lunash:>ntls
bind eth0 -bind 192.20.10.96
Success: NTLS binding hostname or IP Address 192.20.10.96 set.
NOTICE: The NTLS service must be restarted for new settings to take effect.
If you are sure that you wish to restart NTLS, then type 'proceed', otherwise type 'quit'
> proceed
Proceeding...
Restarting NTLS service...
Stopping ntlsl: [ OK ]
Starting ntlsl: [ OK ]
```

```
Command Result : 0 (Success)
[myluna] lunash:>ntls show
NTLS bound to network device: eth0 IP Address: "192.20.10.96" (eth0)
Command Result : 0 (Success)
```



Note: The “Stopping ntlm” operation might fail in the above example, because NTLS is not yet running on a new HSM appliance. Just ignore the message. The service starts again, whether the stop was needed or not.

If you have been following the instructions in these pages as part of setting up a new HSM appliance then the next step is to initialize the HSM on your SafeNet Network HSM appliance. Choose one of the following links, according to the type of HSM appliance that you have:

- ["Initializing a Password Authenticated HSM" on page 121.](#)
- ["Initializing a PED-Authenticated HSM" on page 126.](#)

[Step 3] Initialize the HSM

In this chapter you will initialize your HSM. To initialize an HSM is to prepare it for operation under the control of an HSM Security Officer or SO (the entity that administers the HSM).

Password-Authenticated versus PED-Authenticated HSMs

The HSM is available in PED-authenticated or password-authenticated versions. Follow the initialization steps in this chapter to initialize the type of HSM that you have purchased.

There is no externally visible difference between a password-authenticated or PED-authenticated HSM. For an installed HSM, you can determine its mode of authentication by attempting to log in. A PED-authenticated version will direct you to the SafeNet PED. A Password Authenticated version will prompt you for the password. You cannot change the authentication type of a SafeNet HSM. It is a manufacturing configuration, set at the factory. If you have a PED-authenticated version, you cannot access the HSM and partitions by means of passwords.

For password-authenticated HSMs, you authenticate to the HSM as Security Officer, or Crypto Officer, or User, etc., by typing a password on your computer keyboard.

For PED-authenticated HSMs, you authenticate to the HSM as Security Officer, or Crypto Officer, or User, etc., by presenting an iKey PED Key device that contains the authentication.

Which kind do I have?

SafeNet HSMs are shipped from the factory as one or the other type. This is not a field-changeable setting. If you are not sure which kind you have, verify the type of HSM with the command

hsm displayLicenses in lunash.

That command is one of several non-sensitive HSM commands that does not require HSM authentication. The output lists the configuration packages (additions to the basic build) that make up your SafeNet HSM. Look for the term **FIPS3** appearing in that list to indicate that your SafeNet HSM is PED Authenticated - otherwise, your HSM is Password Authenticated.

See a comparison of Password-authenticated versus PED-authenticated at ["Comparing Password and PED Authentication" on page 1](#).

What if I make a mistake about the type of authentication I present?

No harm. Offering the wrong kind of authentication is not harmful - the only result is a brief delay. However, offering the wrong authentication of the correct type starts the counter for "bad login" attempts. The following paragraphs offer a little more detail.

As a general rule, when you attempt to login to the HSM or to issue any command that requires authentication, the command-line prompts you for the needed authentication. If yours is a Password Authenticated HSM, you are asked for the password, and the command eventually times out if the password is not given. (Of course, if you provide a wrong

password, that is applied against the count of bad login attempts. However, connecting a PED and offering a PED Key to a Password Authenticated HSM has no effect; it is ignored.)

If yours is a PED Authenticated (Trusted Path) HSM, the prompt asks you to attend to the PED for further instructions. If a PED is not connected and/or you don't supply the appropriate PED Keys and keypad actions, the command eventually times out. (If you do have a PED connected and supply the wrong PED Key [of the type requested], then that action is applied against the count of bad login attempts. However, if you mistakenly provide a password [at the command-line] for a PED Authenticated SafeNet HSM, that password is ignored and the bad-login-attempt count is not incremented.)

In either case, just wait for the timeout (a few minutes) to conclude, then begin again, using the correct authentication method.



Note: We recommend that you read through the pages in the Configuration Guide at least once in advance of starting the procedure, so that you can resolve any questions before beginning any time-limited operations. For a Password Authenticated SafeNet HSM, you should have passwords already determined according to your organization's security policies. For a PED Authenticated SafeNet HSM, you should have a SafeNet PED connected, and an appropriate set of PED Keys available.

If this is your only PED Authenticated SafeNet HSM, then you should have received a PED and PED Keys along with the HSM/appliance. If you have other PED Authenticated units at your location, then you can use a PED from one of them.

High-Level Configuration Steps

1. Initialize the HSM. Choose one or the other of:
 - a. ["About Initializing a Password Authenticated HSM"](#)
 - b. ["About Initializing a PED Authenticated HSM"](#)
2. Change the HSM policies, if desired, as described in ["\[Step 4\] Set the HSM Policies" on page 141](#)
 If any of the policies you set are destructive, you must re-initialize the HSM after setting the policies.
3. Create a partition on the HSM, as described in ["\[Step 5\] Create Application Partitions" on page 147](#)
4. Change the partition policies, if desired, as described in ["Setting SafeNet PCIe HSM Partition Policies \[Optional\]" on page 1.](#)

About Initializing a Password-Authenticated HSM

In this section, you initialize the HSM portion of the SafeNet appliance, and set any policies that you require. In normal operation, you would perform these actions just once, when first commissioning your SafeNet appliance.



Note: Perform initialization only after you have set the system-level parameters (time, date, timezone, use of NTP (Network Time Protocol), etc.), and configured network and IP settings to work with your network.

Initialization prepares the HSM for use by setting up the necessary identities, ownership and authentication that are to be associated with the HSM. You must initialize an HSM one time before you can generate or store objects, allow clients to connect, or perform cryptographic operations.

Once you have initialized an HSM, you would return to this section only to clear an entire HSM and all its contents and HSM Partitions, by re-initializing.

Go to ["Initializing a Password Authenticated HSM" below](#).

Initializing a Password Authenticated HSM

Initialize the HSM to set up the necessary identities, ownership and authentication on the HSM. This is required before you can create Partitions and use the HSM.

Start the Initialization Process

The `hsm init` command takes several options.

See ["hsm init" on page 1](#) in the *Lunash Command Reference*.

For an HSM with Password Authentication, you need to provide a label, password, and cloning domain. The only one that you should type at the command line is the label. The password and cloning domain can be typed at the command line, but this makes them visible to anyone who can see the computer screen, or to anyone who later scrolls back in your console or ssh session buffer.

If you omit the password and the domain, the system prompts you for them, and hides your input with "*" characters. This is preferable from a security standpoint. Additionally, you are prompted to re-enter each string, thus helping to ensure that the string you type is the one you intended to type.

Label

The label is a string of up to 32 characters that identifies this HSM unit uniquely. A labeling convention that conveys some information relating to business, departmental or network function of the individual HSM is commonly used.

HSM password

The HSM password is a password for the HSM Security Officer (SO).

For proper security, it should be different from the appliance admin password.

It should employ standard password-security characteristics:

- at least 8 characters,
- not easily guessable (therefore, no words that occur in any dictionary)
- no dates like birthdays or anniversaries, no proper names
- should include miXEd-CAse letters, numbers, special (non-alphanumeric, `-_!@#$%&*...`).

Cloning domain

The cloning domain is a shared identifier that makes cloning possible among a group of HSMs. Cloning is required for backup or for HA. Cloning cannot take place between HSMs that do not share a common domain.

Always specify a cloning domain when you initialize a Password Authenticated SafeNet HSM in a production environment. The HSM allows you to specify "defaultdomain" at initialization, the 'factory-default' domain. This is deprecated, as it is insecure. Anyone could clone objects to or from such an HSM. The default domain is provided, for the time being, for benefit of customers who have previously used the default domain. When you prepare a SafeNet HSM to go into service in a real "production" environment, always specify a proper, secure domain string when you initialize.

Initialize a Password Authenticated HSM

Type the `hsm init` command at the prompt, supplying a text label for the new HSM.

```
lunash:> hsm -init -label myLuna
> Please enter a password for the security officer
> *****
Please re-enter password to confirm:
> *****
Please enter the cloning domain to use for initializing this
HSM :
> *****
Please re-enter domain to confirm:
> *****
CAUTION: Are you sure you wish to re-initialize this HSM?
All partitions and data will be erased.
Type 'proceed' to initialize the HSM, or 'quit'
to quit now.
>proceed
'hsm - init' successful.
```

When activity is complete, the system displays a “success” message.

You have initialized the HSM and created an HSM SO identity, which is an additional capability set, overlaid on the HSM appliance administrator identity.

- Appliance “admin” alone can use lunash to perform some administrator operations on the HSM server, such as network configuration, but cannot access the HSM without additional authentication
- HSM SO (equivalent to the Cryptoki “Security Officer” or “SO”) can administer the HSM, but requires that the system “admin” be logged in first (same ssh session), before HSM Admin can login.

In order to perform all possible administrative functions on the HSM appliance, you must have both the “admin” password for lunash and the HSM Admin authentication.

You are ready to adjust HSM Policies (if desired) and begin creating HSM Partitions for your Client's applications to use.

["Set HSM Policies \(Password Authentication\)" on page 141](#)

About Initializing a PED-Authenticated HSM

In this section, you initialize the HSM portion of the SafeNet appliance, and set any policies that you require. In normal operation, you would perform these actions just once, when first commissioning your SafeNet appliance.

Note: Perform initialization only after you have set the system-level parameters (time, date, timezone, use of NTP (Network Time Protocol), etc.), and configured network and IP settings to work with your network.

...but there's an exception ...



The statement above applies reliably to a new SafeNet Network HSM appliance, or one that has been factory reset. One of the options when initializing an HSM is to forbid changing of time/timezone without HSM login (`hsm init -label myluna -authtimeconfig`). If you make that choice, then it remains in force until you change it. Therefore, if you are following these steps for a SafeNet Network HSM appliance that is not fresh from the factory, or freshly factoryReset, then you might need to take these instructions slightly out of order and perform time-related setting changes after you initialize, rather than before.

Initialization prepares the HSM for use by setting up the necessary identities, ownership and authentication that are to be associated with the HSM. You must initialize an HSM one time before you can generate or store objects, allow clients to connect, or perform cryptographic operations.

If you have not used SafeNet HSMs and PED Keys before, please read the sub-section ["PED Key Management Overview" on page 1](#) in the *Administration Guide*, before you start initializing.

Once you have initialized an HSM, you would return to this section only to clear an entire HSM and all its contents and HSM Partitions, by re-initializing.

If you received your SafeNet HSM in Secure Transport Mode, then a preliminary step is required before you can initialize; see ["Recover the SRK" below](#).

Otherwise, go directly to ["Initializing a PED-Authenticated HSM" on page 126](#).

Recover the SRK



Note: This step is required only if your HSM was shipped in Secure Transport Mode. If not, then proceed to [Initializing the HSM](#). You can read this page later if you choose to enable SRK and/or to invoke Secure Transport Mode at some future time.

PED-authenticated SafeNet HSMs can be shipped from the factory in Secure Transport Mode (your option, at the time you place your order). In this mode, and similar to the state following an HSM tamper event, the Master Tamper Key (MTK) is invalidated.

Here is a brief summary of how MTK and STM (secure transport) are related.

By default, two pieces of data are stored separately on the HSM, that can be brought together by the HSM to recreate the Master Tamper Key, which encrypts all HSM content.

If the HSM has both recovery pieces of the Master Tamper Key on-board, then:

1. It recovers the MTK automatically following any tamper event, when the HSM is restarted. The HSM can carry on immediately.

2. You cannot place the HSM in Secure Transport Mode (a form of controlled, intentional tamper).

You have the option to move one of the recovery pieces of the Master Tamper Key off-board, in the form of the Secure Recovery Vector which gets imprinted on a purple Secure Recovery Key or SRK). If you choose to generate the SRK, then:

3. The HSM retains only one piece of the recovery data and does not recover the MTK automatically following a tamper event, even after restart, until you provide the external piece (the purple key). This gives you control and oversight over tamper events. Your personnel must be aware and must respond before the HSM is allowed to recover from a tamper.
4. With one of the pieces stored externally, you can set the HSM into Secure Transport Mode, and it can recover from STM only when that purple PED Key is presented - this is what we do at the factory if you request that we ship in STM. Then we ship you the purple key by a separate channel.

Before you can begin configuring and using the HSM, you must recover the SRK.

The SRK external secret is held on the purple SRK PED Key(s), shipped to you separately from the HSM.

With the SafeNet Network HSM powered and connected to a SafeNet PED, and also connected to a computer having the SafeNet Client software installed (using local serial connection, or ssh session over the network), log in as appliance 'admin'. Verify that the HSM is in "Hardware tampered" or "Transport mode" state.

```
lunash:> hsm srk show
Secure Recovery State flags:
=====
External split enabled: yes
SRK resplit1 required: no
Hardware tampered: no
Transport mode: yes

Command Result : No Error
lunash:>
```

Recover the srk with the command

```
lunash:> hsm srk transportMode recover
```

With the SafeNet HSM powered and connected to a SafeNet PED, verify that the HSM is in "Hardware tampered" or "Transport mode" state.

```
lunacm:> srk show
Secure Recovery State flags:
=====
External split enabled: yes
SRK resplit2 required: no
Hardware tampered: no
Transport mode: yes

Command Result : No Error
lunash:>
```

¹[or "re-split"] split the MTK secret into a new internal and external recovery vectors, and install the new external portion [the Secure Recovery Vector or SRV] on a new purple PED Key - renders the previous SRV, and any external split of the previous SRV on a purple (SRK) PED Key useless.

²[or "re-split"] split the MTK secret into a new internal and external recovery vectors, and install the new external portion [the Secure Recovery Vector or SRV] on a new purple PED Key - renders the previous SRV, and any external split of the previous SRV on a purple (SRK) PED Key useless.

Recover the srk with the command

```
lunash:> hsm srk transportMode recover
```

Refer to the SafeNet PED and follow the prompts to insert the purple PED Key, enter responses on the PED keypad, etc. During the process, a validation string is shown. You should have received your HSM's validation string by separate mail. Compare that to the string that you see during SRK recovery. They should match. If so, acknowledge the match when requested, and the recovery process concludes with the SRK recreated on the HSM.

When the SRK has been used to recover the MTK on the HSM, the HSM is still in zeroized state, but you can now continue to the next configuration step, initializing the HSM.

Urgent SRK Action

As long as the SRK (purple PED Key) remains valid, it is tied to that HSM and there is risk if it is mishandled or lost. If you do not need to have an external split (the SRV) of the MTK recovery key component, you should immediately perform an **srk disable** operation to bring the external split back into the HSM. Do not overwrite (or lose) the purple PED Key while it contains a valid SRV, unless you have copies.

Some security regimes require that the SRV remains external to the HSM, on an SRK (purple PED Key) to enforce specific, hands-on, oversight and recovery actions, in the case of a tamper event at the HSM. In that case, keep the external split and handle with care (including having on-site and off-site backup copies, just as you would with the Security Officer (blue) PED Key). You are not "done" with a purple PED Key until its contents have been returned to its HSM with **srk disable**.

Re-split the SRK

You have the option to re-split the SRK at any time - you need the current external SRK split (the purple PED Key(s)) to initiate the action. The purpose would be to ensure that the SRK for your HSM is secure and that you have the only copies of the external portion of the secret. That is, by re-splitting at your convenience, you remove the risk that somebody kept a copy of the purple PED Key before they sent your HSM to you. Any copy of the previous secret becomes useless when a re-split operation is performed. Similar logic applies if a copy of your new SRK goes missing (or is thought to have been compromised) - a re-split/regeneration of the secure recovery vector onto a new external key (SRK) or keys renders the lost/stolen/compromised SRK useless to anyone.

Other Uses of the SRK

The SRK is also used to recover from a real tamper event on the HSM or its appliance.

The steps are the same as above, except that the HSM resumes granting access with its contents intact - [re-] initialization is not required.

You can set the HSM to Secure Transport Mode before placing it into storage, or before shipping to your organization's remote location, or before shipping to your customer (offering them the same Secure Shipping option as is available from SafeNet).

If you have just received an HSM from SafeNet in Secure Transport Mode, and recovered from STM, your next step should be to initialize the HSM. Go to ["Initializing a PED-Authenticated HSM" on the next page](#).

See also ["re-split required"](#).

To view a table that compares and contrasts various "deny access" events or actions that are sometimes confused, see ["Comparison of destruction/denial actions"](#).

Initializing a PED-Authenticated HSM

Your SafeNet HSM arrives in "Zeroized" state, and in a default, pre-initialized condition (see below). It might also be in Secure Transport Mode, if you selected that option at purchase time.

In this section, you initialize the HSM portion of the SafeNet appliance, and set any policies that you require. In normal operation, you would perform these actions just once, when first commissioning your SafeNet appliance.

Note: Perform initialization only after you have set the system-level parameters - time, date, timezone, use of NTP (Network Time Protocol), etc. - and configured network and IP settings to work with your network.



Exception: The statement (above) applies to a new SafeNet Network HSM appliance, or one that has been factory reset. One of the options when initializing an HSM is to forbid changing of time/timezone without HSM login (`hsm init -label myluna -authtimeconfig`). If you make that choice, then it remains in force until you change it. Therefore, if you are following these steps for a SafeNet Network HSM appliance that is not fresh from the factory, or freshly factoryReset, then you will need to take these instructions slightly out of order and perform time-related setting changes after you initialize, rather than before.

Initialization prepares the HSM for use by setting up the necessary identities, ownership and authentication that are to be associated with the HSM. You must initialize an HSM one time before you can generate or store objects, allow clients to connect, or perform cryptographic operations.

If you have not used SafeNet HSMs and PED Keys before, please read the sub-section ["PED Key Management Overview" on page 1](#) in the *Administration Guide*, before you start initializing.

Once you have initialized an HSM, you would return to this section only to clear an entire HSM and all its contents and HSM Partitions, by re-initializing.

Preparing to Initialize a SafeNet Network HSM [PED-version]

The last thing that the production workers do, before placing your SafeNet Network HSM into its shipping carton, is to press the "Decommission" button on the back of the appliance. This sets the HSM in Factory Reset mode, ensuring that when you receive it, it does not contain left-over objects and settings from factory burn-in and final-test. Depending on the options that you chose when ordering, your SafeNet Network HSM might also arrive in "Secure Transport Mode". If the HSM is in Factory Reset mode only, then it is ready to be initialized by you. If the HSM is also in Secure Transport Mode, then you must run the `hsm srk transportMode recover` command.

How do you know?

After making an SSH or serial connection, and logging on as 'admin', show the Secure Recovery State :

```
[myluna] lunash:>hsm srk show
```

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

```
Command Result : No Error
lunash:>
```

Show other HSM status info :

```
[myluna] lunash:>hsm show
Appliance Details:
=====
Software Version:          5.1.0-25
HSM Details:
=====
HSM Label:      [none]
Serial #:       700022
Firmware:       6.2.1
Hardware Model:  Luna K6
Authentication Method:  PED keys
HSM Admin login status:  Not   Logged In
HSM Admin login attempts left:  3 before HSM zeroization!
RPV Initialized:  Yes
Manually Zeroized:  No

Partitions created on HSM:
=====
Partition: 700022012,          Name: mypar1
Partition: 700022013,          Name: mypar2
Partition: 700022016,          Name: mypar3
FIPS 140-2 Operation:
=====
The HSM is NOT in FIPS 140-2 approved operation mode.
HSM Storage Informaton:
=====
Maximum HSM Storage Space (Bytes):  2097152
Space In Use (Bytes):                2097152
Free Space Left (Bytes):              0
Command Result : 0 (Success)
[myluna] lunash:>
```

“Transport Mode” refers to a user-invoked tamper event, which preserves all contents of the HSM, but protects them behind encryption until you run the recovery command. In addition, whether or not the HSM contains useful secrets, Transport Mode assures you that nobody has interfered with the HSM while it was in storage or in transit.

“Hardware tampered” refers to a state where a hardware intrusion or failure has been detected, such as tripping of a detector. Similar to the user-invoked Transport Mode, “Hardware tampered” requires you to unlock the HSM with `hsm srk transportMode recover`, before you can resume using it. On a PED-authenticated HSM (with SRK enabled), that requirement takes the HSM out of service and forces you to acknowledge that the tamper has occurred before the HSM can go back into service. On a password-authenticated HSM - or a PED-authenticated HSM without SRK enabled - a tamper event is just a logged event that does not take the HSM out of service, even temporarily.

“Zeroized” state is different, and results from any of:

- Factory reset by command.
- The “Decommission” button being pressed.
- The HSM detecting 3 bad login attempts on the SO account.

This renders any HSM contents unrecoverable. At the factory, we would have created only unimportant test objects on the HSM - if you have previously had the HSM in service, and then either “decommissioned” it or performed `hsm factoryreset` your valid objects and keys are similarly rendered permanently unrecoverable and the HSM is completely safe to store or ship.

The above states are addressed by configuring and initializing your SafeNet Network HSM. Instructions start on this page.

If you requested Secure Transport Mode shipment from SafeNet, then a couple of additional steps are required (also included in these instructions).

Why Initialize?

Before you can make use of it, the HSM must be initialized. This establishes your ownership for current and future HSM administration. Initialization assigns a meaningful label, as well as Security Officer authentication (PED Key) and cloning Domain (another PED Key), and places the HSM in a state ready to use.

Use the instructions on this page if you have a SafeNet HSM with PED authentication.



Note: Not the first time? Some HSM Policy changes are destructive. A destructive policy change is one that requires the HSM to be initialized again, before it can be used. Thus if you intend to perform a destructive HSM Policy change, you might need to perform this initialization step again, after the Policy change.

Start a Serial Terminal or SSH session

```
bash#: ssh 192.20.10.203
login as: admin
admin@172.20.10.202's password:_____
Last login: Fri Dec 2 20:16:54 2014 from 192.17.153.225
SafeNet Network HSM 6.0.0 Command Line Shell - Copyright (c) 2001-2014 SafeNet, Inc. All rights reserved.
```

```
[myluna] lunash:>
```

Initialize the HSM

1. Have the Luna PED connected and ready (in local mode and "Awaiting command...").
2. Insert a blank PED Key into the USB connector at the top of the PED.
3. In a serial terminal window or with an SSH connection, log into LunaSH as the appliance administrator 'admin':
lunash:>
4. Run the hsm init command, giving a label for your SafeNet Network HSM. [If Secure Transport Mode was set, you must unlock the HSM with the purple PED Key before you can proceed; see earlier on this page and the [Recover the SRK](#) page.]

The following is an example of initialization dialog, with PED interactions inserted to show the sequence of events.

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

The following warning appears:

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



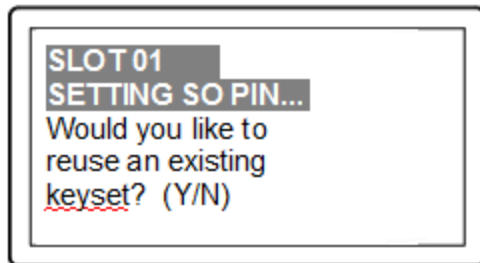

Note: Respond promptly to avoid PED timeout Error. At this time, the PED becomes active and begins prompting you for PED Keys and other responses. For security reasons, this sequence has a time-out, which is the maximum permitted duration, after which an error is generated and the process stops. If you allow the process to time-out, you must re-issue the initialization command. If the PED has timed out, press the [CLR] key for five seconds to reset, or switch the PED off, and back on, to get to the “Awaiting command...” state before re-issuing another lunash command that invokes the PED.

See ["Initialization - some additional options and description " on page 135](#) for additional information and a summary of the options you might choose or encounter during this process - this procedure (below) assumes a relatively straightforward process.

SafeNet PED asks preliminary setup questions.

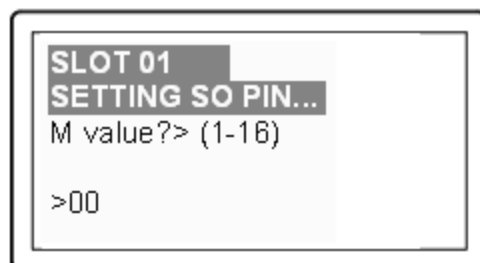
The simplest scenario is your first-ever HSM and new PED Keys. However, you might have previously initialized this HSM and be starting over. Or you might have other HSMs already initialized and need to share the authentication or the domain with your new HSM.

The HSM and PED need to know, prior to imprinting the first SO PED Key.

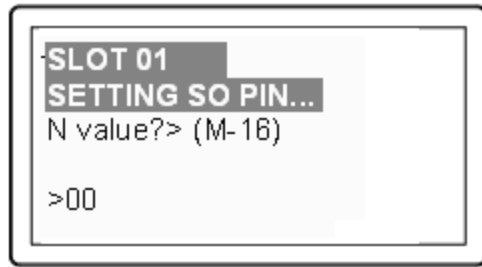


If you say [NO] (on the PED keypad), then you are indicating there is nothing of value on your PED Keys to preserve. On the assumption that you will now be writing onto a new blank PED Key, or onto one that contains old unwanted authentication, SafeNet PED asks you to set MofN values.

If you say [YES], you indicate that you have a PED Key (or set of PED Keys) from another HSM and you wish your current/new HSM to share the authentication with that other HSM. Authentication will be read from the PED Key that you present and imprinted onto the current HSM.



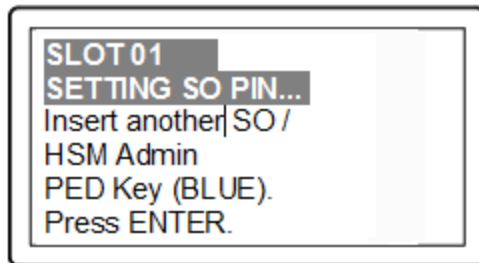
and



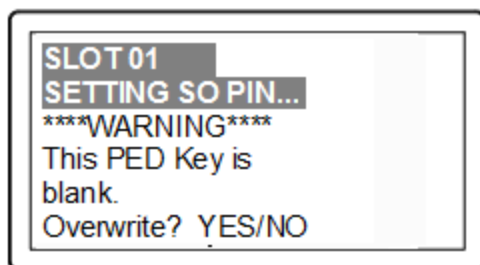
Setting M and N equal to "1" means that the authentication is not to be split, and only a single PED Key will be necessary when the authentication is called for in future.

Setting M and N larger than "1" means that the authentication is split into N different "splits", of which quantity M of them must be presented each time you are required to authenticate. MofN allows you to enforce multi-person access control - no single person can access the HSM without cooperation of other holders.

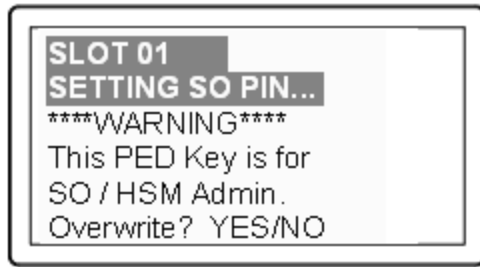
SafeNet PED now asks you to provide the appropriate PED Key - a fresh blank key, or a previously used key that you intend to overwrite, or a previously used key that you intend to preserve and share with this HSM.



Insert a blue HSM Admin / SO PED key [of course, the unlabeled PED Key is generically black - we suggest that you apply the appropriate color sticker either immediately before or immediately after imprinting the key; before, just to ensure it gets done, or after, as a helpful indicator as to which ones are imprinted (with which secret), and which ones still blank] and press [Enter].



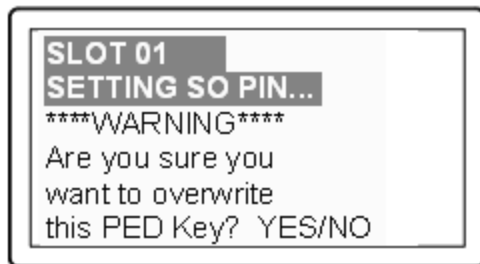
OR



Answer (press the appropriate button on the PED keypad)

- **"NO"** if the PED key that you provided carries SO authentication data that must be preserved. In that case, you must have made a mistake so the PED goes back to asking you to insert a suitable key.
- **"YES"** if the PED should overwrite the PED Key with a new SO authentication.
If you overwrite a never-used PED Key, nothing is lost; if you overwrite a PED Key that contains authentication secret for another HSM, then this PED Key will no longer be able to access the other HSM, only the new HSM that you are currently initializing with a new, unique authentication secret - therefore "YES" means 'yes, destroy the contents on the key and create new authentication information in its place' - be sure that this is what you wish to do. (This will be matched on the SafeNet Network HSM during this initialization).

SafeNet PED makes very sure that you wish to overwrite, by asking again.

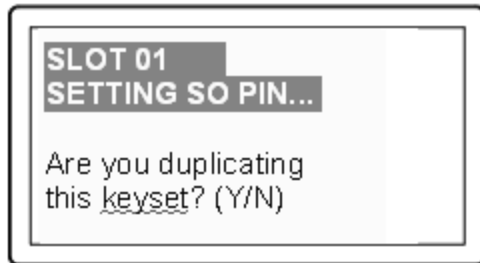


For any situation other than reusing a keyset, SafeNet PED now prompts for you to set a PED PIN. For multi-factor authentication security, the physical PED Key is "something you have". You can choose to associate that with "something you know", in the form of a multi-digit PIN code that must always be supplied along with the PED Key for all future HSM access attempts.



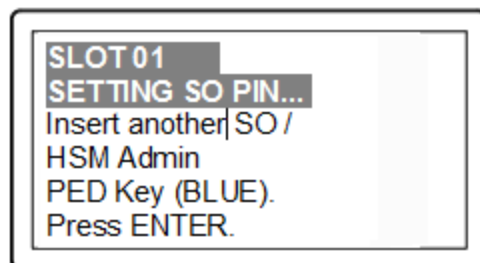
Type a numeric password on the PED keypad, if you wish. Otherwise, just press [Enter] twice to indicate that no PED PIN is desired.

SafeNet PED imprints the PED Key, or the HSM, or both, as appropriate, and then prompts the final question for this key:

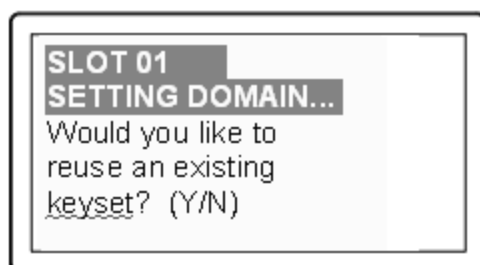


You can respond [YES] and present one or more blank keys, all of which will be imprinted with exact copies of the current PED Key's authentication, or you can say [NO], telling the PED to move on to the next part of the initialization sequence. (You should always have backups of your imprinted PED Keys, to guard against loss or damage.)

To begin imprinting a Cloning Domain (red PED Key), you must first log into the HSM, so in this case you can simply leave the blue PED Key in place.

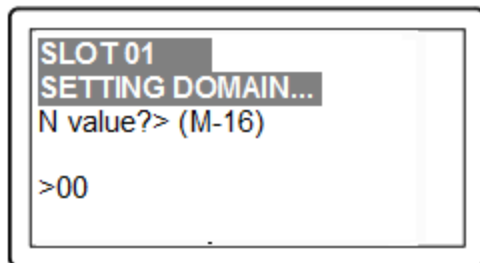
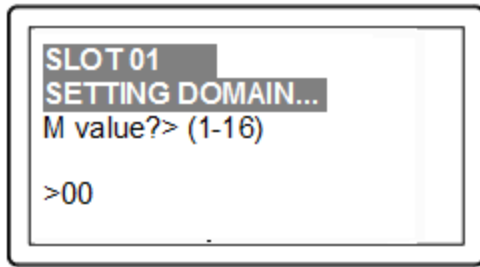


SafeNet PED passes the authentication along to the HSM and then asks the first question toward imprinting a cloning domain:

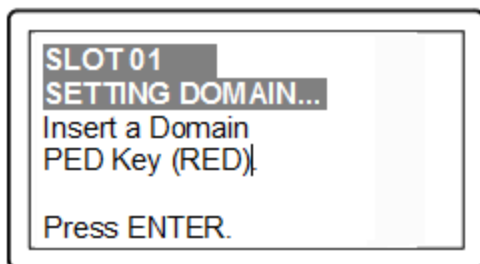


If this is your first SafeNet HSM, or if this HSM will not be cloning objects with other HSMs that are already initialized, then answer [NO]. SafeNet PED prompts for values of M and N.

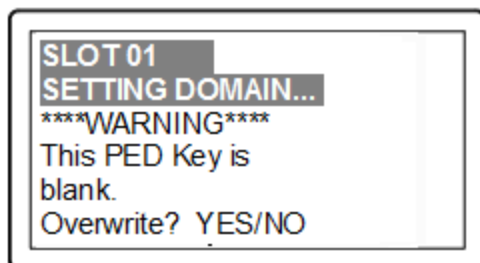
If you have another HSM and wish that HSM and the current HSM to share their cloning Domain, then you must answer [YES]. In that case, SafeNet PED does not prompt for M and N.



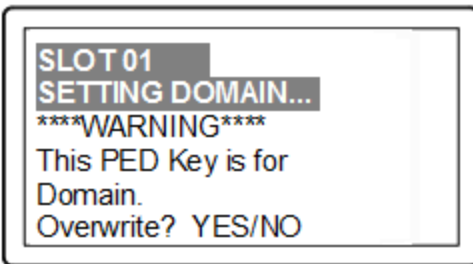
SafeNet PED goes through the same sequence that occurred for the blue SO PED Key, except it is now dealing with a red Domain PED Key.



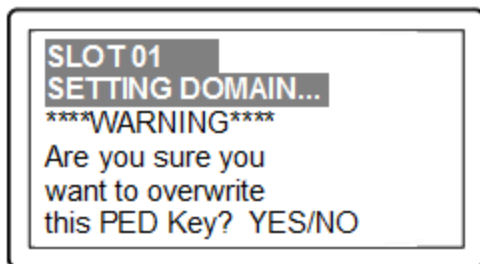
Insert a red HSM Cloning Domain PED key [of course, the unlabeled PED Key is generically black - we suggest that you apply the appropriate color sticker either immediately before or immediately after imprinting the key; before, just to ensure it gets done, or after, as a helpful indicator as to which ones are imprinted (with which secret), and which ones still blank] and press [Enter].



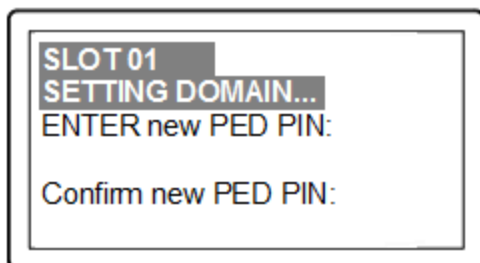
OR



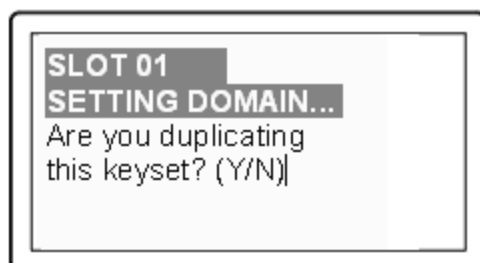
Just as with the blue SO PED Key, the next message is:



When you confirm that you do wish to overwrite whatever is (or is not) on the currently inserted key, with a Cloning Domain generated by the PED, the PED asks:



And finally:



Once you stop duplicating the Domain key, or you indicate that you do not wish to make any duplicates (you should have backups of all your imprinted PED Keys...), SafeNet PED goes back to "Awaiting command...".

Lunash says:

```

Command Result : No Error
lunash:>
lmyluna] lunash:>hsm show
Appliance Details:
=====
Software Version:                    5.1.0-25
HSM Details:
=====
HSM Label:                          mylunahsm
Serial #:                           700022
Firmware:                           6.2.1
Hardware Model:                      Luna K6
Authentication Method:              PED keys
HSM Admin login status:             Logged In
HSM Admin login attempts left:      3 before HSM zeroization!
RPV Initialized:                    Yes
Manually Zeroized:                  No
Partitions created on HSM:
=====

FIPS 140-2 Operation:
=====
The HSM is NOT in FIPS 140-2 approved operation mode.
HSM Storage Information:
=====
Maximum HSM Storage Space (Bytes):  2097152
Space In Use (Bytes):                0
Free Space Left (Bytes):             2097152
Command Result : 0 (Success)
[myluna] lunash:>

```

Notice that the HSM now has a label.

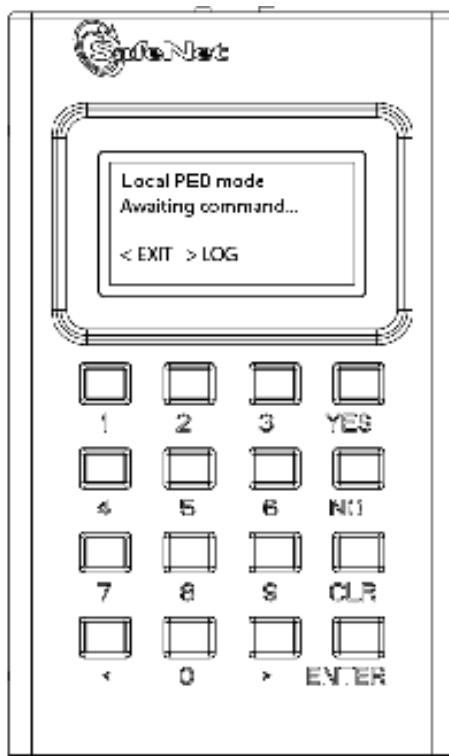
The next step is ["Prepare to Create a Partition \(PED Authenticated\)" on page 152](#) on the HSM.

Initialization - some additional options and description

Anywhere there are choices, options abound. Rather than clutter the main initialization instruction page with a variety of possible paths and branches, this section presents some of the other situations that you might encounter while initializing a SafeNet HSM. So, assume that you have issued the hsm init command. The system told you to attend to the SafeNet PED, which you already had connected.

SafeNet PED demands the first "SO/HSM Admin" PED Key.

Insert the Blue PED Key



This table (below) summarizes the steps involving SafeNet PED immediately after you invoke the command "hsm init...".

The first column is the simplest, and most like what you would encounter the very first time you initialize, using "fresh from the carton" iKey PED Keys.



The next two columns of the table show some differences if you are using previously-imprinted PED Keys, choosing either to reuse what is found on the key (imprint it on your new HSM - see [Group PED Keys](#)) or, in the third column example to overwrite what is found and generate a new secret to be imprinted on both the PED Key and the HSM.

Below the table are some expanded comments about the choices that you might encounter.

"Fresh" PED Keys	Pre-used PED Keys (reuse)	Pre-used PED Keys (overwrite)
SLOT 01 SETTING SO PIN... Would you like to reuse an existing keyset? (Y/N)	SLOT 01 SETTING SO PIN... Would you like to reuse an existing keyset? (Y/N)	SLOT 01 SETTING SO PIN... Would you like to reuse an existing keyset? (Y/N)

"Fresh" PED Keys	Pre-used PED Keys (reuse)	Pre-used PED Keys (overwrite)
[The above question is always asked first. Answering "No" requires the PED to write/overwrite any keys that you present, so it must test and query each time.]	[The above question is always asked first. Answering "Yes" shortens the sequence. The PED will copy a secret from a PED Key to the HSM, and therefore does not need to overwrite a PED Key.]	[The above question is always asked first. If the PED is not told to reuse PED Keys, then it must overwrite and therefore must test and warn each time. This column is similar to the sequence in the first column, except that the answers to the questions are more important, since the keys to be overwritten already have material on them.]
SLOT 01 SETTING SO PIN... Insert a SO / HSM Admin PED Key Press ENTER.	SLOT 01 SETTING SO PIN... Insert a SO / HSM Admin PED Key Press ENTER.	Slot 01 SETTING SO PIN... Insert a SO / HSM Admin PED Key Press ENTER.
This PED Key is blank. Overwrite? (YES/NO)	****Warning!**** This PED Key is for SO / HSM Admin Overwrite? (YES/NO)	****Warning!**** This PED Key is for SO / HSM Admin Overwrite? (YES/NO)
[The key is blank, so no harm can be done when you say "Yes" on SafeNet PED to proceed with writing to the key]. Saying "No" would just loop back to the previous prompt.	[If you respond "NO" the key content is preserved and is imprinted onto the current HSM. This key can now unlock the current HSM and any previous HSM that uses the same secret.]	[If you respond "YES" the key content is overwritten and can now unlock only this HSM. It is no longer able to unlock any previous HSM or token.]
Enter a new PED PIN Confirm new PED PIN	Enter a new PED PIN Confirm new PED PIN	Enter a new PED PIN Confirm new PED PIN
You can type a number and press ENTER to impose a PED PIN "something you know", or you can just press ENTER (with no digits) for	Same as in first column.	Same as in first column.

"Fresh" PED Keys	Pre-used PED Keys (reuse)	Pre-used PED Keys (overwrite)
no PED PIN (thus nothing to remember in future).		
Are you duplicating this keyset? YES/NO	Are you duplicating this keyset? YES/NO	Are you duplicating this keyset? YES/NO
If you respond "YES", you can keep inserting additional blank (or old-to-be-reused) PED Keys to be imprinted with this same secret. If you say "NO", you have just the one key with that secret - don't lose it.	Same as in first column.	Same as in first column.
Login SO / HSM Admin... Insert a SO/ HSM Admin PED Key Press ENTER	Login SO / HSM Admin.. Insert a SO/ HSM Admin PED Key Press ENTER	Login SO / HSM Admin.. Insert a SO/ HSM Admin PED Key Press ENTER
Having created/imprinted the HSM Admin or SO secret, the HSM now requires you to login, in order to go further. This is a verification step.	Same as in first column.	Same as in first column.
SETTING DOMAIN... Would you like to reuse an existing keyset? (Y/N)	SETTING DOMAIN... Would you like to reuse an existing keyset? (Y/N)	SETTING DOMAIN... Would you like to reuse an existing keyset? (Y/N)
The PED prompts in similar fashion to the steps for the HSM Admin/SO key above (overwrite, copy, etc.). If asked to "Reuse Id", the best option is to say "YES", unless you have good reason to create a new domain not shared with any previous HSM.	Here, your response to "Reuse ID?" might or might not be the same as you chose for the blue key, above. You might have good reason to make this HSM part of an existing Domain.	Here, your response to "Reuse ID?" might or might not be the same as you chose for the blue key, above. You might have good reason to make this HSM part of an existing Domain.

"Fresh" PED Keys	Pre-used PED Keys (reuse)	Pre-used PED Keys (overwrite)
HSM Init process is finished.	HSM Init process is finished.	HSM Init process is finished.

Table 1: PED prompt sequences

Some additional comments about some of the choices:

Provide a PED PIN (optional)

A PED PIN can be 4-to-16 digits, or can be no digits if a PED PIN is not desired .

Enter a PIN if you wish, and press [Enter] to inform SafeNet PED that you are finished entering PED PIN digits, or that you have decided not to use a PED PIN (no digits entered).

Confirm, by entering the same PIN (or nothing if you did not enter a PIN the first time), and pressing [Enter] again. (When you provide a PED PIN – even if it is the null PIN (by just pressing [Enter] with no digits) – SafeNet PED asks for it a second time, to ensure that you entered it correctly.)

In future, every time you are required to present that PED Key, you must also enter the PED PIN on the PED keypad - if you created a PED PIN at initialization time, then you must provide that exact PED PIN along with the PED Key, in order to gain access to the HSM. If you did not create a PED PIN when you initialized, then just press [Enter] at the PED prompt when you insert the requested PED Key during login.

When you are attempting to log in, the PED always asks for a PED PIN, regardless whether or not a real PED PIN is expected. That's a security feature, similar to password-protected systems that tell you if you have entered incorrect credentials, but don't specify if it was the login name or the password that was individually the faulty part.

Duplicating Your PED Key

"Are you duplicating this keyset? (Y/N)"

If you respond "NO", SafeNet PED imprints just the one blue HSM Admin key (or Domain key (see below) and goes on to the next step in initialization of the HSM.

If you respond "YES", SafeNet PED imprints the first blue key and then asks for more blue PED Keys, until you have imprinted (duplicated) as many as you require.



Note: It is recommended to have at least one full backup set of imprinted PED Keys, stored in a safe place, in case of loss or damage to the primary keys. Of course, a backup set does not need to be stored in one location. Your security protocols might require that individual backup PED Keys be stored at separate locations according to role.



Note: You can also make additional copies of a PED Key at any time, using the PED's own "Admin" menu. This does not require you to log into the HSM or issue commands from the appliance - the PED needs to be connected only to have power supplied to it when you are using the onboard PED menus. One implication of this ability is that you must maintain strict oversight and control of your PED Keys at all times, so that you can be sure that you know how many copies of a given PED Key exist, where they are, and in whose possession.

Creating a Cloning Domain

You create the domain for future cloning of the HSM, or you adopt the domain from a previous token or SafeNet HSM, so that the current SafeNet HSM (or token) can clone with the previous. A common domain (common between HSM and Backup HSM) is required for HSM backups.

If the red PED Key is blank, then SafeNet PED goes ahead and imprints a domain, which is matched on the HSM. However, if SafeNet PED detects that the red PED Key contains data, then SafeNet PED now needs to know:

a. If the domain data on the key should be preserved as valid, and recorded on the current HSM or token

[What to do] - This allows the PED Key to work with both the previous and the current HSM or token – that is, they will all share the same cloning/backup domain. Therefore, to preserve the existing domain answer “YES” to “...reuse an existing keyset?”]

OR

b. If the domain data that was found on the red key must be overwritten with a new domain that is exclusive to the current HSM or token

[What to do] - This prevents the red key from working with any previous HSM or token. To overwrite and create a new domain that applies to only this HSM, answer “NO” to “... reuse an existing keyset?”].

About Backup HSMs - Always choose to 'reuse' when initializing a SafeNet Backup HSM, so that the backup HSM will share the domain with the source SafeNet HSM, and so that the red Domain PED Key remains usable with the SafeNet HSM. (You do not want the red PED Key to be overwritten when creating a backup.)

At this point in the process of configuring your SafeNet HSM, you can :

optionally [modify some of the HSM's Policy settings](#)

or

go directly to "[Creating HSM Partitions](#)"

[Step 4] Set the HSM Policies

SafeNet HSMs are built on one of our general-purpose HSM platforms (hardware plus firmware), and then are loaded with what we call "personality", to make them into specific types of HSM with specific abilities and constraints, to suit different markets and applications.

The built-in attributes are called "Capabilities" and describe what the HSM can do as it comes to you from the factory.

Some capabilities are unalterable, except by re-manufacturing the HSM.

Many HSM capabilities can be altered by means of HSM Policies, which coincide one-for-one with the capabilities that they alter.

You can view the current HSM capabilities and policies with the **hsm showpolicies** command:

You can change a current HSM policy in LunaSH with the **hsm changepolicy** command.

This section describes how to modify HSM Policies, and suggests some examples of changes best made before the HSM is further configured for use in your environment. Refer to the instructions for your HSM authentication type:

- ["Set HSM Policies \(Password Authentication\)" below](#)
- ["Set HSM Policies - PED \(Trusted Path\) Authentication" on page 143](#)

Set HSM Policies (Password Authentication)

Set any of the alterable policies that are to apply to the HSM.



Note: Capability vs Policy Interaction

Capabilities identify the purchased features of the product and are set at time of manufacture. Policies represent the HSM Admin's enabling (or restriction) of those features.

1. Type the **hsm showPolicies** command, to display the current policy set for the HSM.

```
[myluna] lunash:>hsm showPolicies
```

```
HSM Label:    myhsm
Serial #:     700022
Firmware:     6.21.0.
```

The following capabilities describe this HSM, and cannot be altered except via firmware or capability updates.

Description	Value
=====	=====
Enable PIN-based authentication	Allowed
Enable PED-based authentication	Disallowed
Performance level	15
Enable domestic mechanisms & key sizes	Allowed
Enable masking	Allowed
Enable cloning	Allowed
Enable special cloning certificate	Disallowed

Enable full (non-backup) functionality	Allowed
Enable ECC mechanisms	Allowed
Enable non-FIPS algorithms	Allowed
Enable SO reset of partition PIN	Allowed
Enable network replication	Allowed
Enable Korean Algorithms	Disallowed
FIPS evaluated	Disallowed
Manufacturing Token	Disallowed
Enable Remote Authentication	Allowed
Enable forcing user PIN change	Allowed
Enable portable masking key	Allowed
Enable partition groups	Disallowed
Enable Remote PED usage	Disallowed
Enable external storage of MTK split	Disallowed
HSM non-volatile storage space	2097152
Enable HA mode CGX	Disallowed
Enable Acceleration	Allowed
Enable unmasking	Disallowed

The following policies are set due to current configuration of this HSM and cannot be altered directly by the user.

Description	Value
PIN-based authentication	True

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

Description		Value	Code	Destructive
=====		=====	=====	=====
Allow masking	On	6	Yes	
Allow cloning	On	7	Yes	
Allow non-FIPS algorithms		On	12	Yes
SO can reset partition PIN		On	15	Yes
Allow network replication		On	16	No
Allow Remote Authentication		On	20	Yes
Force user PIN change after set/reset	Off	21	No	
Allow off-board storage		On	22	Yes
Allow acceleration		On	29	Yes
Allow unmasking		On	30	Yes

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

According to the above example, the fixed capabilities require that this HSM be protected with HSM Password Authentication, meaning that the PED and PED Keys are not used for authentication, and instead values are typed from a keyboard.

The alterable policies have numeric codes. You can alter a policy with the `hsm changePolicy` command, giving the code for the policy that is to change, followed by the new value.



Note: The FIPS 140-2 standard mandates a set of security factors that specify a restricted suite of cryptographic algorithms.

The SafeNet HSM is designed to the standard, but can permit activation of additional non-

FIPS-validated algorithms if your application requires them.



The example listing above indicates that non-validated algorithms have been activated. The HSM is just as safe and secure as it is with the additional algorithms switched off. The only difference is that an auditor would not validate your configuration unless the set of available algorithms is restricted to the approved subset.

2. In order to change HSM policies, the HSM SO must first login.

```
lunash:> hsm login
```

(If you are not logged in, the above command logs you in, prompting for the HSM Admin password. If you are already logged in, the HSM tells you so, with an error message, that you can ignore.)

3. If you need to modify a policy setting to comply with your operational requirements, type:

```
lunash:> hsm changePolicy -policy <policyCode> -value <policyValue>
```

As an example, change code 15 from a value of 1 (On) to 0 (Off).

Example – Change of HSM Policy

```
lunash:> hsm changePolicy -policy 15 -value 0
```

That command assigns a value of zero (0) to the policy for “HSM Admin can reset partition PIN”, turning it off.

Refer to the Reference section for a description of all and their meanings.

If you have been following the instructions on this page as part of setting up a new HSM system, then the next step is to create virtual HSMs or HSM Partitions on the HSM that you just configured. ["Prepare to Create a Legacy Partition \(Password Authenticated\)" on page 149](#)

Set HSM Policies - PED (Trusted Path) Authentication

Set any of the alterable policies that are to apply to the HSM.



Note: Capability vs Policy Interaction

Capabilities identify the purchased features of the product and are set at time of manufacture. Policies represent the HSM Admin's enabling (or restriction) of those features.

1. Type the **hsm showPolicies** command, to display the current policy set for the HSM.

```
lunash:> hsm showPolicies
```

```
HSM Label:  mysahsm
Serial #:    7000022
Firmware:   6.22.0
```

The following capabilities describe this HSM, and cannot be altered except via firmware or capability updates.

Description	Value
=====	=====
Enable PIN-based authentication	Disallowed
Enable PED-based authentication	Allowed
Performance level	15

Enable domestic mechanisms & key sizes	Allowed
Enable masking	Disallowed
Enable cloning	Allowed
Enable special cloning certificate	Disallowed
Enable full (non-backup) functionality	Allowed
Enable non-FIPS algorithms	Allowed
Enable SO reset of partition PIN	Allowed
Enable network replication	Allowed
Enable Korean Algorithms	Allowed
FIPS evaluated	Disallowed
Manufacturing Token	Disallowed
Enable Remote Authentication	Allowed
Enable forcing user PIN change	Allowed
Enable portable masking key	Allowed
Enable partition groups	Disallowed
Enable remote PED usage	Allowed
Enable External Storage of MTK Split	Allowed
HSM non-volatile storage space	16252928
Enable Acceleration	Allowed
Enable unmasking	Allowed
Enable FW5 compatibility mode	Disallowed
Maximum number of partitions	100
Enable ECIES support	Disallowed
Enable Single Domain	Allowed
Enable Unified PED Key	Allowed
Enable MofN	Allowed
Enable small form factor backup/restore	Disallowed
Enable Secure Trusted Channel	Allowed
Enable decommission on tamper	Disallowed
Enable Per-Partition SO	Allowed
Enable partition re-initialize	Allowed

The following policies are set due to current configuration of this HSM and cannot be altered directly by the user.

Description	Value
=====	=====
PED-based authentication	True
Store MTK Split Externally	False

The following policies describe the current configuration of this HSM and may be changed by the HSM Administrator.

Changing policies marked "destructive" will zeroize (erase completely) the entire HSM.

Description	Value	Code	Destructive
=====	=====	=====	=====
Allow cloning	On	7	Yes
Allow non-FIPS algorithms	On	12	Yes
SO can reset partition PIN	On	15	Yes
Allow network replication	On	16	No
Allow Remote Authentication	On	20	Yes
Force user PIN change after set/reset	Off	21	No
Allow offboard storage	On	22	Yes

Allow remote PED usage	On	25	No
Allow Acceleration	On	29	Yes
Allow unmasking	On	30	Yes
Current maximum number of partitions	100	33	No
Force Single Domain	Off	35	Yes
Allow Unified PED Key	Off	36	No
Allow MofN	On	37	No
Allow Secure Trusted Channel	Off	39	No
Allow partition re-initialize	Off	42	No

Command Result : 0 (Success)

According to the above example, the fixed capabilities require that this HSM be protected at FIPS 140-2 level 3, meaning that the PED and PED Keys are required for authentication, and values typed from a keyboard are ignored.

The alterable policies have numeric codes. You can alter a policy with the `hsm changePolicy` command, giving the code for the policy that is to change, followed by the new value.



Note: The FIPS 140-2 standard mandates a set of security factors that specify a restricted suite of cryptographic algorithms. The HSM is designed to the standard, but can permit activation of additional non-FIPS-validated algorithms if your application requires them. The example listing above indicates that non-validated algorithms have been activated. The HSM is just as safe and secure as it is with the additional algorithms switched off. The only difference is that an auditor would not validate your configuration unless the set of available algorithms is restricted to the approved subset.

2. In order to change HSM policies, the HSM SO must first login.

```
lunash:> hsm login
```

(If you are not logged in, the above command begins the login process, directing you to the PED. If you are already logged in, the SafeNet Network HSM tells you so, with an error message, that you can ignore.)

Control is passed to the PED, which prompts you for the blue PED Key.

Insert the appropriate PED Key for this HSM, and press [ENT] on the PED keypad.

3. If you need to modify a policy setting to comply with your operational requirements, type:

```
lunash:> hsm changePolicy -policy <policyCode> -value <policyValue>
```

As an example, change code 15 from a value of 1 (On) to 0 (Off).

Example – Change of HSM Policy

```
lunash:> hsm changePolicy -policy 15 -value 0
```

That command assigns a value of zero (0) to the “HSM Admin can reset partition PIN” policy, turning it off.



WARNING! The above example is a change to a destructive policy, meaning that, if you apply this policy, the HSM is zeroized and all contents are lost. For this reason, you are prompted to confirm if that is what you really wish to do. You must now re-initialize the HSM.

While this is not an issue when you have just initialized an HSM, it may be a very



important consideration if your HSM system has been in a “live” or “production” environment and the HSM contains useful or important data, keys, certificates.

If you have been following the instructions on this page as part of setting up a new HSM system, then the next step is to create virtual HSMs or HSM Partitions on the HSM that you just configured. Click the following link: [Create Partition \(Trusted Path Authentication\)](#)

SafeNet Network HSM 6 does not currently have a Scalable Key Storage (formerly SIM) configuration. Certain HSM policy settings exist to enable migration from SafeNet Network HSM 4.x to SafeNet Network HSM 5.x or 6.x, specifically the “Enable masking” and “Enable portable masking key” values.

[Step 5] Create Application Partitions

This chapter describes how to create application partitions on the HSM.

Choose Partition Type

The options are:

- Legacy-style application partitions are owned and administered by the HSM SO, who retains complete control.
- PPSO-style application partitions each have their own SO, independent of the HSM SO, and all control except partition creation and deletion resides with the Per-Partition SO

Legacy-style Partitions

Choose the authentication method that applies to your HSM.

See ["Prepare to Create a Legacy Partition \(Password Authenticated\)" on page 149](#) .

See ["Prepare to Create a Partition \(PED Authenticated\)" on page 152](#).

Per-Partition SO (PPSO) Partitions

For an overview of the procedure to set up a PPSO partition, see ["About Configuring an Application Partition with Its Own SO " on page 168](#). The selection of Password or PED authentication is done on that page.

About Configuring Legacy Partitions

Before SafeNet HSM release 6.0, an HSM could have one kind of application partition. It was administratively owned by the HSM SO who created it, and was operationally managed by a unified Partition User entity (black PED Key for PED-authenticated HSMs) or by a Crypto Officer and Crypto User (again, the black PED Key for PED-auth HSMs) who simply split the role of Partition User into a role that could create, delete and modify partition objects (the CO), and a role that could use partition objects but not create or change them (the CU).

SafeNet HSM release 6.0 introduced firmware 6.22.0, along with library updates and new commands and revisions of previously existing commands in the major management tools SafeNet Shell (lunash) for SafeNet Network HSM, and LunaCM for SafeNet USB HSM, SafeNet PCIe HSM, and also for SafeNet Network HSM.

Now, the possibilities are:

- a pre-existing application partition, created with older tools on an HSM with firmware older than version 6.22.0 (before you updated to release 6.0 software and version 6.22.0 firmware)
 - a legacy partition,
 - the application partition is administratively owned by the HSM SO,

- SafeNet PCIe HSM and SafeNet USB HSM application partitions are seen by a client application like *lunacm* and operated using commands that were available before firmware 6.22.0 (those HSMs support only one application partition, so it appears in *lunacm* that there is just one partition to which you log in as HSM SO for administration, or as Crypto Officer (or Crypto User) for operation)
- SafeNet Network HSM application partitions are seen, via NTLS, by a client application like *lunacm*, and operated using commands that were available before firmware 6.22.0 (no administration can be done on such slots/partitions from the client side, because the administrating authority is the HSM SO who operates from the HSM administrative partition (at the SafeNet Network HSM, using *lunash*), and cannot be reached via a client connection)
- to create a new legacy application partition, or to destroy an existing one and create again, you can follow the configuration instructions in the original documentation that came with your HSM and original software; nothing has changed until you change HSM firmware
- an application partition created with version 6.0 or newer tools, on an HSM with firmware 6.22.0 or newer, and with no partition SO specified
 - a legacy-style partition
 - the application partition is administratively owned by the HSM SO,
 - SafeNet PCIe HSM and SafeNet USB HSM application partition, as seen by *lunacm*, are operated using commands similar to those that were available before release 6.0, but with some changes, and with the addition of role commands
 - SafeNet Network HSM application partitions are seen, via NTLS, by a client application like *lunacm*, and operated using commands similar to those that were available before firmware 6.22.0, but with some changes, and with the addition of role commands (no administration can be done on such slots/partitions from the client side, because the administrating authority is the HSM SO who operates from the HSM administrative partition, and cannot be reached via a client connection)
- an application partition created with version 6.0 or newer tools, on an HSM with firmware 6.22.0 or newer, and with its own private SO as its administrative owner
 - a PPSO partition
 - the application partition is created or destroyed by the HSM SO, but the HSM SO has limited ability to touch the partition, otherwise
 - SafeNet PCIe HSM and SafeNet USB HSM application partition, as seen by *lunacm*, are operated using commands updated for release 6.0, and with the new role commands
 - SafeNet Network HSM application partitions are seen, via NTLS, by a client application like *lunacm*, and operated using commands that are updated for release 6.0 and newer, including the new role commands (only creation of the empty PPSO application partitions is done at the SafeNet Network HSM, by the HSM SO using *lunash:>* commands; PPSO partitions are turned over to the Partition SO and all further administration is done from the client side) .

This section is concerned with the first two types - pre-existing true legacy partitions and newly-created legacy-style partitions.

Prepare to Create a Legacy Partition (Password Authenticated)

This section is HSM Partition setup for Password Authentication. The activities in this section are required in three circumstances.

- if you just prepared an HSM on the SafeNet appliance for the first time and must now create your first HSM Partition, or
- if you have purchased a SafeNet appliance capable of supporting multiple HSM Partitions and you wish to create those additional partitions (this procedure creates one HSM Partition at a time, and you would need to repeat it once for each Partition, up to the number supported by your SafeNet HSM) , or
- if you have deleted an HSM Partition and wish to create a new one to replace it.

About HSM Partitions on the Initialized HSM

At this point, the SafeNet appliance should already:

- have its network settings configured by "[\[Step 2\] Configure Your Network Settings](#)" on page 102,
- have its HSM SO assigned by "[About Initializing a Password-Authenticated HSM](#)" on page 121.

Within the HSM, separate cryptographic work-spaces must be initialized and designated for clients. A workspace, or Partition, and all its contents are protected by encryption derived (in part) from its authentication. Only a Client that presents the proper authentication is allowed to see the Partition and to work with its contents.

In this section, you will:

- Create an HSM Partition

First, Establish a Connection to your SafeNet Appliance

If you do not already have a connection open, connect your administration computer to the serial Console port of the SafeNet appliance and open a Terminal session, or use ssh to connect via the network.

Then, Login as HSM Admin

To create HSM Partitions, you must login to the SafeNet HSM as HSM Admin. At the lunash prompt, type:

```
lunash:> hsm login
```

Authenticate as HSM Admin by supplying the appropriate HSM Admin password when you are prompted — this is generally preferable to typing the password on the command line, because your response to the password prompt is hidden from view by "*" characters.



WARNING! If you fail three consecutive login attempts as HSM Admin, the HSM is zeroized and cannot be used — it must be re-initialized. Re-initializing zeroizes the HSM contents. Zeroizing destroys all key material. Please note that the SafeNet HSM must actually receive some information before it logs a failed attempt, so if you just press [Enter] without typing a password, that is not logged as a failed attempt. Also, when you successfully login, the counter is reset to zero.

If you are not sure that you are currently logged in as HSM Admin, perform an 'hsm logout'.

Next, see ["Create \(Initialize\) a Password Authenticated Legacy-style Application Partition "](#) below.

Create (Initialize) a Password Authenticated Legacy-style Application Partition

Having logged in, you can now use the 'partition' command.

When you issue the partition create command, to create an HSM Partition, you must supply a label or name for the new Partition.



Note: Choose a partition name that is meaningful, in the context of your operations. Partition names must be unique in the HSM. You are not permitted to create two partitions with the same label on one HSM. This will be the label seen by PKCS #11 applications.

Rules for names and passwords

A partition **name** or a partition **label** can include any of the following characters :

`!#$%&'()*+,-./0123456789:=@ABCDEFGHIJKLMNOPQRSTUVWXYZ[]^_abcdefghijklmnopqrstuvwxyz~`

No spaces, unless you wish to surround the name or label in double quotation marks every time it is used.

No question marks, no double quotation marks within the string.

Minimum name or label length is 1 character. Maximum is 32 characters.

Valid characters that can be used in a **password** or in a cloning **domain**, when entered via LunaSH ^[1], are:

`!#$%&'()*+,-./0123456789:=?@ABCDEFGHIJKLMNOPQRSTUVWXYZ[]^_abcdefghijklmnopqrstuvwxyz~`

(the first character in that list is the space character)

Invalid or problematic characters, not to be used in passwords or cloning domains are

`"&';<>\'`()`

Valid characters that can be used in a **password** or in a cloning **domain**, when entered via *lunacm*, are:

`!"#$%&'()*+,-./0123456789;<=>?@ABCDEFGHIJKLMNOPQRSTUVWXYZ[\]^_`abcdefghijklmnopqrstuvwxyz{|}~`

(the first character in that list is the space character)

Minimum password length is 7 characters; maximum is 255 characters in *lunash* or *lunacm*.

Minimum domain string length is 1 character; maximum domain length is 128 characters via *lunash*. No arbitrary maximum domain string length is enforced for domain strings entered via *lunacm*, and we have successfully input domain strings longer than 1000 characters in testing.

^[1] LunaSH on the SafeNet Network HSM has a few input-character restrictions that are not present in LunaCM, run from a client host. It is unlikely that you would ever be able to access, via LunaSH, a partition that received a password or domain via LunaCM, but the conservative approach would be to avoid the few "invalid or problematic characters" generally.

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

number.

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

CAUTION:

Tips for using strong passwords:



- use at least eight characters (a Partition policy controls the minimum length)
- mix the case of alphabetic characters
- include at least one numeral
- include at least one punctuation character or special character such as @#\$%&, etc.
- avoid words that can be found in the dictionary (any language)
- avoid proper names (especially family and pets)
- avoid birthdays and other easily identifiable dates.

For password-auth HSMs, valid characters that can be used in passwords are:

!#\$%&'()*+,-./0123456789:;=?@ABCDEFGHIJKLMNPOQRSTUVWXYZ[]^_`
abcdefghijklmnopqrstuvwxyz{|~

(the first character in that list is the space character)

Invalid characters, not to be used in passwords are "&';<>\"

Minimum password length is 7 characters. Maximum is 255 characters.

1. Create and name an HSM Partition. At the lunash prompt, for legacy (no partition SO) type:

```
lunash:> partition create -partition myPartition1  
for a partition with its own SO, type:
```

```
lunash:> partition create -partition myPartition1 -haspso
```

2. For legacy partition (owned by the HSM SO), continue at step 3, below.
For partition with its own SO, go to ["About Configuring an Application Partition with Its Own SO " on page 168](#).
3. Supply the appropriate new HSM Partition password when you are prompted (that is, don't supply the password as a command option — waiting to be prompted is generally preferable to typing the password on the command line, because a password that is typed in response to the prompt is hidden from view by "*" characters).
NOTE: You may not set the Password to be "PASSWORD", which is reserved as the partition creation-time default, only, and is too easy to guess for a real, operational password.
4. Write down the application Partition password. This is the password that will be used:
 - a) to authenticate the administrator performing Partition management tasks via `lunash`
 - b) to authenticate Client applications that wish to use the SafeNet HSM.

Repeat the above actions for each HSM Partition that you wish to create (to the limits of your SafeNet system's configuration).

Partition creation audit log entry

Each time a partition is created, an entry is added to the audit log. Any subsequent actions logged against the partition are identified by the partition serial number that was generated when the partition was created.

Determining the serial number of a created partition from the audit log

An audit log entry similar to the following is generated when a partition is created on the HSM:

```
5,12/12/17 16:14:14,S/N 150718 session 1 Access 2147483651:2669 SO container operation LUNA_
CREATE_CONTAINER returned RC_OK(0x00000000) container=20 (using PIN (entry=LUNA_ENTRY_DATA_
AREA))
```

It is not obvious from this entry what the serial number is for the created partition. This information, however, can be derived from the log entry, since the partition serial number is simply a concatenation of the HSM serial number and the partition container number, which are specified in the log entry, as highlighted below:

```
5,12/12/17 16:14:14,S/N 150718 session 1 Access 2147483651:2669 SO container operation LUNA_
CREATE_CONTAINER returned RC_OK(0x00000000) container=20 (using PIN (entry=LUNA_ENTRY_DATA_
AREA))
```

In the example above, the HSM serial number is 150718 and the partition container number is 20. Note that the partition container number is a three-digit number with leading zeros suppressed, so that the actual partition container number is 020. To determine the partition serial number concatenate the two numbers as follows:

```
150718020
```

Use this number to identify the partition in subsequent audit log entries.

Next steps

If you have been following the instructions on these pages as part of setting up a new SafeNet appliance, then the next step is to adjust the Partition Policy settings for the new Partition that you just configured.

You might wish to adjust "[\[Step 6\] Set the Partition Policies for Legacy Partitions](#)" on page 179 (Optional).

Otherwise, go to "[Creating an NTL Link Between a Client and a Partition](#)" on page 191 .

Prepare to Create a Partition (PED Authenticated)

This section is HSM application partition setup for PED Authenticated HSMs. The activities in this section are required in these circumstances.

- if you just initialized the HSM for the first time and must now create your first application Partition, or
- if you have purchased a SafeNet HSM capable of supporting multiple HSM Partitions and you wish to create those additional partitions (this procedure creates one HSM Partition at a time, and you would need to repeat it once for each Partition, up to the number supported by your SafeNet HSM) , or
- if you have deleted an HSM Partition and wish to create a new one to replace it.

About HSM Partitions on the Initialized HSM

At this point, the HSM *should already*:

- have its network settings configured (see "[Configuring the SafeNet Appliance Network Settings](#)")
- have appliance and client-side certificates exchanged and registered (see "[\[Step 7\] Create a Network Trust Link Between the Client and the Appliance](#)" on page 183)

- have its HSM SO and its Cloning Domain assigned (see " [About Initializing a PED-Authenticated HSM](#)" on page 123).

Within the HSM, separate cryptographic work-spaces must be initialized and designated for client operations. A workspace, or Partition, and all its contents are protected by encryption derived (in part) from its authentication. Only a Client that presents the proper authentication is allowed to see the Partition and to work with its contents.

In this section, you will:

- Decide the type of application partition to create
- Create an HSM application partition

Establish a Connection to your HSM Appliance

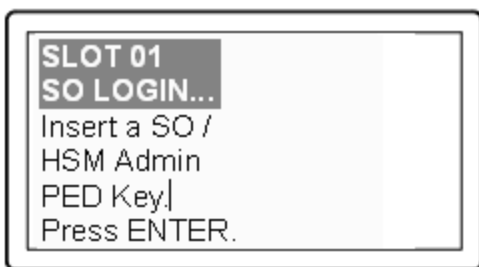
1. If you do not already have a connection open, connect your administration computer to the serial Console port of the HSM appliance, and open a Terminal session, or use ssh to connect via the network (for Windows, we provide PuTTY; for UNIX/Linux, your operating system provides the ssh client, either as part of the distribution, or as a separate down-loadable utility).

Login as HSM SO

1. To create HSM Partitions, you must login to the HSM as HSM Security Officer or SO.
Ensure that the PED is connected to the PED port on your HSM host , and that the PED is powered on and "Awaiting command..."

Or, ensure that you have set up a Remote PED connection, and the PED is ready (see "[Installing and Configuring a SafeNet Remote PED](#)" on page 1 and "[Configuring Remote PED](#)" on page 1).
2. At the command prompt, type the login command.


```
lunash:> hsm login
```
3. Authenticate as HSM SO:
The PED prompts for the blue PED Key



Provide the blue HSM Admin PED Key that has been imprinted (initialized) for this HSM.

If you had set a PED PIN, you are prompted for that, as well.

4. At this point, you are about to create an application partition. The options are:
 - a. *a legacy-style partition* old firmware
 - HSMs with firmware earlier than 6.22.0 (only legacy partitions possible),
 - the HSM SO owns and administers the partition

- the remaining partition configuration steps are carried out at the command line, as you have been doing to this point - go to ["Create a PED Authenticated Legacy-style Application Partition \(f/w pre-6.22.0\)" on the next page](#)
- b. *a legacy-style partition* newer firmware
 - HSMs with f/w 6.22.0 or newer without PPSO capability installed (only legacy partitions possible), or HSMs with f/w 6.22.0 or newer, with PPSO capability installed, but you choose to create a legacy partition, rather than a PPSO partition
 - the HSM SO owns and administers the partition
 - the remaining partition configuration steps are carried out at the command line, as you have been doing to this point - go to ["Create a PED Authenticated Legacy-style Application Partition \(f/w 6.22.0 or newer\)" on page 162](#)
- c. *a PPSO or Per-Partition SO partition* (optional in HSMs with firmware 6.22.0 or newer, and with the PPSO capability installed),
 - each partition has its own SO, and the HSM SO has no access other than to delete the application partition
 - the creation of an empty partition is performed next at the LunaSH command line, but subsequent steps are performed at a registered SafeNet HSM Client computer, over NTL or STC link
 - go to ["HSM SO Configures PED-authenticated SafeNet Network HSM Partition with SO " on page 171](#)

If you don't remember whether you are logged in as HSM SO, you can use the **hsm show** command to find out:

```
[mylunasa6] lunash:>hsm show
```

```
Appliance Details:
=====
Software Version:                6.0.0-33

HSM Details:
=====
HSM Label:                      mysa6
Serial #:                       7000022
Firmware:                       6.22.0
HSM Model:                      K6 Base
Authentication Method:          PED keys
HSM Admin login status:         Not Logged In      (alternatively could show "Logged in")
HSM Admin login attempts left:  3 before HSM zeroization!
RPV Initialized:                Yes
Audit Role Initialized:         Yes
Remote Login Initialized:       No
Manually Zeroized:              No

Partitions created on HSM:
=====
Partition:      16298193222733, Name: mypsopar1
Partition:      16298193222735, Name: mylegacypar1

Number of partitions allowed:    100
Number of partitions created:    2

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

```
HSM Storage Information:
=====
Maximum HSM Storage Space (Bytes): 16252928
Space In Use (Bytes): 325058
Free Space Left (Bytes): 15927870
```

```
Command Result : 0 (Success)
[mylunasa6] lunash:>
```

Create a PED Authenticated Legacy-style Application Partition (f/w pre-6.22.0)

This section is HSM Application Partition setup for a SafeNet HSM with PED Authentication, where the partition is to remain under the ownership of the HSM Security Officer. The activities in this section are required in two circumstances.

- if you just prepared an HSM for the first time and must now create your first application Partition, or
- if you have deleted or zeroized an application Partition and wish to create a new one to replace it.

About Application Partitions on the Initialized HSM

At this point, the SafeNet HSM should already have its Security Officer assigned.

Within the HSM, a separate cryptographic work-space must be created. A workspace, or Partition, and all its contents are protected by encryption derived (in part) from its authentication. Only a User who presents the proper authentication is allowed to see the Partition and to work with its contents. That User (or Crypto Officer and Crypto User) and authentication can be separate from the Security Officer identity, but the application partition is still ultimately owned and administered by the HSM SO, who can modify it at any time.

In this section, you will:

- Create an application Partition
- Set application Partition Policies (Optional)

These instructions assume that your SafeNet HSM is at a version lower than 6.22.0. The commands available at the SafeNet command line are the traditional ones that have been used with SafeNet HSMs. The outcome of this sequence is the creation of a legacy-style application partition that is owned and managed by the HSM SO and does not have its own independent SO.

If your HSM firmware is at version 6.22.0 or higher, then some of the commands have changed, and are the same as those listed for creation of a PPSO application partition, in another section of this guide. That is, with the newer firmware you can use the newer commands to create either a legacy-style partition or a PPSO partition. With the pre-6.22.0 firmware, you have only the older commands, and you can create only a legacy partition.

For the following procedure, you must have previously initialized the HSM, and logged into the HSM as HSM SO.

Having logged in as HSM SO, you can now use the `partition create` command, to create an HSM Partition.

You must supply a label or name for the new Partition when you issue the command.

```
lunash:> partition create -partition <name-for-new-Partition>
```

(The angle brackets "<" and ">" indicate that you fill in text of your choice. Do not type the brackets.)

Rules for names and passwords

A partition **name** or a partition **label** can include any of the following characters :

```
!#$%&'()*+,-./0123456789:=@ABCDEFGHIJKLMNOPQRSTUVWXYZ[]^_abcdefghijklmnopqrstuvwxyz~
```

No spaces, unless you wish to surround the name or label in double quotation marks every time it is used.

No question marks, no double quotation marks within the string.

Minimum name or label length is 1 character. Maximum is 32 characters.

Valid characters that can be used in a **password** or in a cloning **domain**, when entered via LunaSH ^[1], are:

```
!#$%&'()*+,-./0123456789:=?@ABCDEFGHIJKLMNOPQRSTUVWXYZ[]^_abcdefghijklmnopqrstuvwxyz~
```

(the first character in that list is the space character)

Invalid or problematic characters, not to be used in passwords or cloning domains are

```
"&';<>\'|()
```

Valid characters that can be used in a **password** or in a cloning **domain**, when entered via *lunacm*, are:

```
!"#$%&'()*+,-./0123456789:;<=>?@ABCDEFGHIJKLMNOPQRSTUVWXYZ[\]^_`abcdefghijklmnopqrstuvwxyz{|}~
```

(the first character in that list is the space character)

Minimum password length is 7 characters; maximum is 255 characters in *lunash* or *lunacm*.

Minimum domain string length is 1 character; maximum domain length is 128 characters via *lunash*. No arbitrary maximum domain string length is enforced for domain strings entered via *lunacm*, and we have successfully input domain strings longer than 1000 characters in testing.

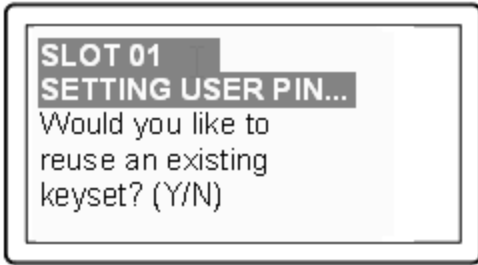
^[1] LunaSH on the SafeNet Network HSM has a few input-character restrictions that are not present in LunaCM, run from a client host. It is unlikely that you would ever be able to access, via LunaSH, a partition that received a password or domain via LunaCM, but the conservative approach would be to avoid the few "invalid or problematic characters" generally.

1. Create the application Partition. Type:

```
lunash:> partition create -partition myPartition1
(substitute the name of your choice for "myPartition1")
Please ensure that you have purchased licenses for at least this number of
partitions: -1
If you are sure you wish to continue then type 'proceed', otherwise type 'quit'
> proceed
Proceeding...

Please ensure that you copy the password from the SafeNet PED and
that you keep it in a safe place.
Luna PED operation required to create a partition - use User or Partition Owner
(black) PED key.
```

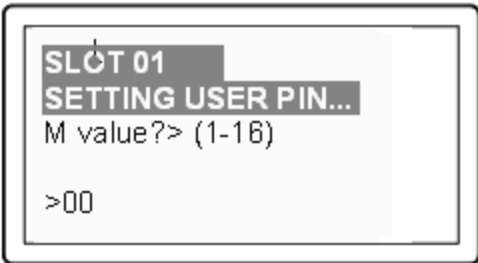
2. The PED inquires if you intend to reuse a pre-existing imprinted black PED Key.



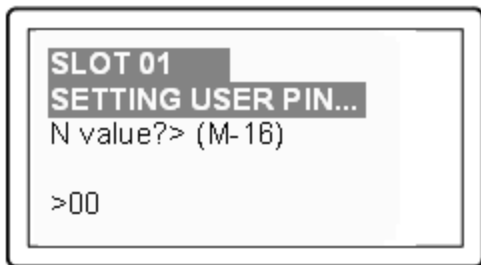
Respond "Yes" if you have a key from another HSM partition with a partition Owner ID already imprinted on it, that you wish to share/reuse. The authentication data on that PED Key will be preserved and used for this partition. Respond "No" if you have a fresh, never-imprinted key, or if you have a key previously imprinted with an ID that you do not wish to preserve. The authentication data on that PED Key will be overwritten by freshly-generated authentication data.

(See ["Shared or Group PED Keys" on page 1](#) for more detail)

3. The PED requests values for :



and



(enter "1" for both, unless you wish to invoke MofN split-secret, multi-person access control, ["Using MofN" on page 1](#)).

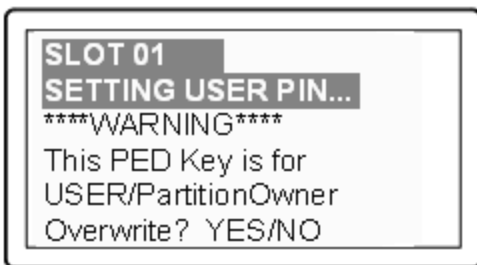
4. The PED then demands the black Owner PED key with the message



Insert the black HSM Partition Owner PED key [of course, the unlabeled PED Key is generically black - we suggest that you apply the appropriate color sticker either immediately before or immediately after imprinting the key; before, just to ensure it gets done, or after, as a helpful indicator as to which ones are imprinted (with which secret), and which ones still blank] and press [Enter]. A unique Partition Owner PIN is to be imprinted on both the PED key and the HSM Partition.

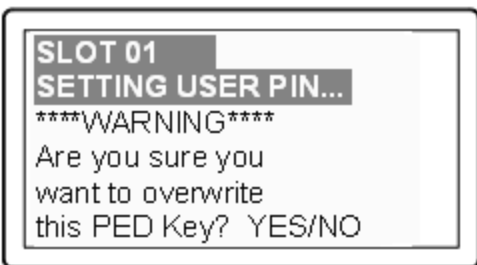


5. The PED *might* continue with:



Decide whether this should be a group PED Key (see ["Shared or Group PED Keys" on page 1](#)), press [YES] or [NO] on the PED keypad, and press [Enter].

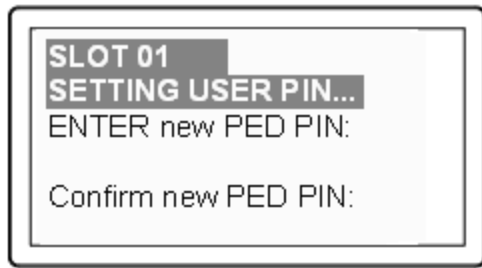
6. This is potentially serious business (if you unintentionally overwrite a PED Key that is needed for other purposes), so SafeNet PED asks one more time if you truly intend to overwrite the key's content.



Press [YES] or [NO] on the PED keypad, and press [Enter].

7. Next, you are asked to provide a PED PIN (optional, see ["What is a PED PIN?" on page 1](#) — can be 4-to-48 digits,

or can be *no* digits if a PED PIN is not desired).



You must press [Enter] to inform the PED that you are finished entering PED PIN digits, *or* that you have decided not to use a PED PIN (no digits entered).

When you provide a PED PIN – even if it is the null PIN (by just pressing [Enter] with no digits) – the PED requests it a second time, to ensure that you entered it correctly, as you intended.

Press [ENTER] again.

8. You are then prompted

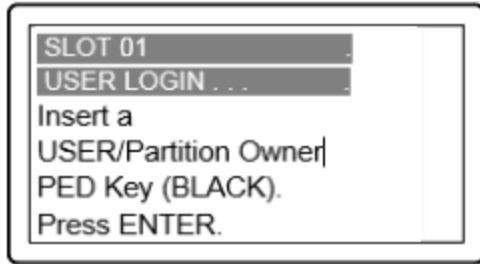


See ["Duplicating PED Keys" on page 1](#).

Respond "No", if you want the PED to imprint just the one black HSM Admin PED Key and go on to the next step in creation of the application Partition.

Respond "Yes", if you want the PED to imprint the first black key and then ask for more black PED Keys, until you have imprinted (duplicated) as many as you wish. After each duplicate is made, the PED asks: Would you like to make another duplicate set? Answer "Yes" until you have enough copies, and then press "No".

9. Having created the black key User or Crypto Officer, the HSM needs you to log in as that identity, and prompts:



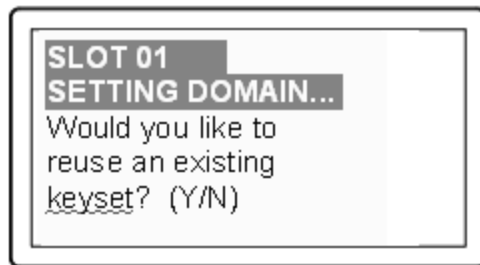
Leave the black key inserted, and press Enter.

At the command-line session, the next part of the sequence is displayed

```
Luna PED operation required to generate cloning domain on the partition - use
Domain (red) PED key.
```

and control once again goes to the SafeNet PED.

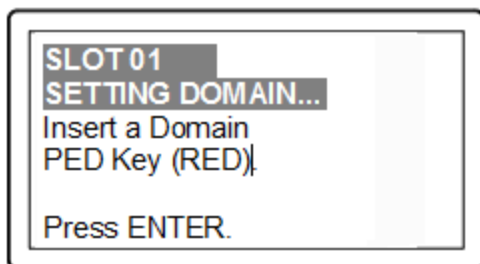
10. The PED inquires if you intend to reuse a previously imprinted red Domain PED Key.



Respond "Yes" if you have a key from another HSM partition with a cloning domain ID already imprinted on it, that you wish to share/reuse.

Respond "No" if you have a fresh, never-imprinted key, or if you have a key previously imprinted with an ID that you do not wish to preserve.

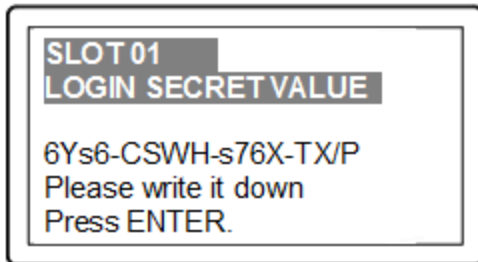
11. As it did for the black key, the PED now requests values for M and N. Again, enter 1 for each unless you wish to invoke MofN splitting of the domain secret.
12. The PED then prompts for a red Domain PED key with the message



Insert the red HSM Partition Domain PED key [of course, the unlabeled PED Key is generically black - we suggest that you apply the appropriate color sticker either immediately before or immediately after imprinting the key; before, just to ensure it gets done, or after, as a helpful indicator as to which ones are imprinted (with which secret), and which ones still blank] and press [Enter]. A cloning domain is to be imprinted on both the PED key and the HSM Partition.



13. The PED goes through the same prompts as for the black PED Key. Respond as appropriate.
14. SafeNet PED presents the generated partition challenge secret (password), which you must record:



We suggest recording the string in a text editor, which should be more legible than handwriting. The hyphens are inserted for ease of reading, but are not part of the challenge secret. Remove them before pasting the recorded secret.



CAUTION: We recommend that you have at least one backup set of imprinted PED Keys, stored in a safe place, in case of loss or damage to the primary keys.

You might wish to adjust ["Partition Policies" on page 1](#) (Optional).
Otherwise, go to ["Assigning a Client to a Partition" on page 191](#).

Partition creation audit log entry

Each time a partition is created, an entry is added to the audit log. Any subsequent actions logged against the partition are identified by the partition serial number that was generated when the partition was created.

Determining the serial number of a created partition from the audit log

An audit log entry similar to the following is generated when a partition is created on the HSM:

```
5,12/12/17 16:14:14,S/N 150718 session 1 Access 2147483651:2669 SO container operation LUNA_
CREATE_CONTAINER returned RC_OK(0x00000000) container=20 (using PIN (entry=LUNA_ENTRY_DATA_
AREA) )
```

It is not obvious from this entry what the serial number is for the created partition. This information, however, can be derived from the log entry, since the partition serial number is simply a concatenation of the HSM serial number and the partition container number, which are specified in the log entry, as highlighted below:

```
5,12/12/17 16:14:14,S/N 150718 session 1 Access 2147483651:2669 SO container operation LUNA_
CREATE_CONTAINER returned RC_OK(0x00000000) container=20 (using PIN (entry=LUNA_ENTRY_DATA_
AREA) )
```

In the example above, the HSM serial number is 150718 and the partition container number is 20. Note that the partition container number is a three-digit number with leading zeros suppressed, so that the actual partition container number is 020. To determine the partition serial number concatenate the two numbers as follows:

```
150718020
```

Use this number to identify the partition in subsequent audit log entries.

Create a PED Authenticated Legacy-style Application Partition (f/w 6.22.0 or newer)

This section assumes that the HSM firmware is version 6.22.0 or newer, and that you are creating a legacy-style application partition that will remain under administrative control of the HSM SO. (For instructions to create PPSO partitions on an HSM with firmware 6.22.0 or newer, or to create true legacy partitions on an HSM with firmware older than 6.22.0, see the appropriate instruction sequences elsewhere in this document.)

For the following procedure, you must have previously initialized the HSM, and logged into the HSM as HSM SO.

Having logged in as HSM SO, you can now use the `partition create` command, to create an HSM Partition.

You must supply a label or name for the new Partition when you issue the command.

```
lunash:> partition create -partition <name-for-new-Partition>
```

(The angle brackets “<” and “>” indicate that you fill in text of your choice. Do not type the brackets.)

Rules for names and passwords

A partition **name** or a partition **label** can include any of the following characters :

```
!#$%()'*,+,-./0123456789:=@ABCDEFGHIJKLMNOPQRSTUVWXYZ[]^_abcdefghijklmnopqrstuvwxyz{|}~
```

No spaces, unless you wish to surround the name or label in double quotation marks every time it is used.

No question marks, no double quotation marks within the string.

Minimum name or label length is 1 character. Maximum is 32 characters.

Valid characters that can be used in a **password** or in a cloning **domain**, when entered via LunaSH [¹], are:

```
!#$%'*+,-./0123456789:=?@ABCDEFGHIJKLMNOPQRSTUVWXYZ[]^_abcdefghijklmnopqrstuvwxyz{|}~
```

(the first character in that list is the space character)

Invalid or problematic characters, not to be used in passwords or cloning domains are

```
"&';<>\'|()
```

Valid characters that can be used in a **password** or in a cloning **domain**, when entered via *lunacm*, are:

```
!#$%&\'()*+,-./0123456789:;<=>?@ABCDEFGHIJKLMNOPQRSTUVWXYZ[\]^_`abcdefghijklmnopqrstuvwxyz{|}~
```

(the first character in that list is the space character)

Minimum password length is 7 characters; maximum is 255 characters in *lunash* or *lunacm*.

Minimum domain string length is 1 character; maximum domain length is 128 characters via *lunash*. No arbitrary

maximum domain string length is enforced for domain strings entered via *lunacm*, and we have successfully input domain strings longer than 1000 characters in testing.

[¹] LunaSH on the SafeNet Network HSM has a few input-character restrictions that are not present in LunaCM, run from a client host. It is unlikely that you would ever be able to access, via LunaSH, a partition that received a password or domain via LunaCM, but the conservative approach would be to avoid the few "invalid or problematic characters" generally.

1. Create and name an application Partition. Type:

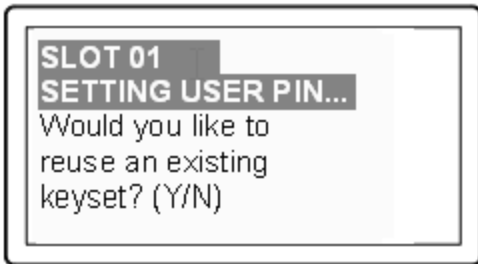
```
lunash:> partition create -partition mylegacypar1
(substitute the name of your choice for "mylegacypar1")
```

```
Please ensure that you have purchased licenses for at least this number of partitions: -1
If you are sure you wish to continue then type 'proceed', otherwise type 'quit'
> proceed
Proceeding...
```

```
Please ensure that you copy the password from the Luna PED and
that you keep it in a safe place.
```

```
Luna PED operation required to create a partition - use User or Partition Owner (black) PED
key.
```

2. The PED inquires if you intend to reuse a pre-existing imprinted black PED Key.

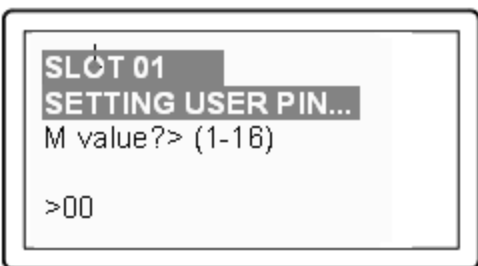


Respond "Yes" if you have a key from another HSM partition with a partition Owner ID already imprinted on it, that you wish to share/reuse.

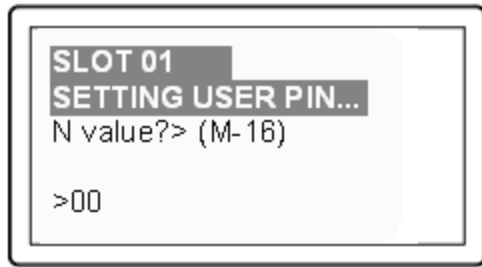
Respond "No" if you have a fresh, never-imprinted key, or if you have a key previously imprinted with an ID that you do not wish to preserve.

(See "Shared or Group PED Keys" on page 1 for more detail)

3. The PED requests values for :

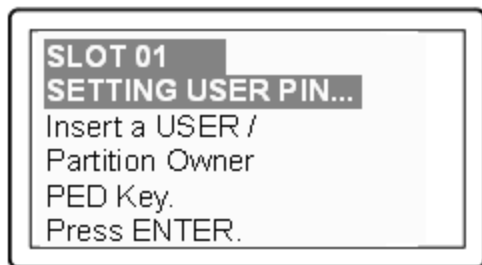


and



(enter "1" for both, unless you wish to invoke MofN split-secret, multi-person access control, "Using MofN" on page 1).

4. The PED then demands the black Owner PED key with the message



Insert the black HSM Partition Owner PED key [of course, the unlabeled PED Key is generically black - we suggest that you apply the appropriate color sticker either immediately before or immediately after imprinting the key; before, just to ensure it gets done, or after, as a helpful indicator as to which ones are imprinted (with which secret), and which ones still blank] and press [Enter]. A unique Partition Owner PIN is to be imprinted on both the PED key and the HSM Partition.

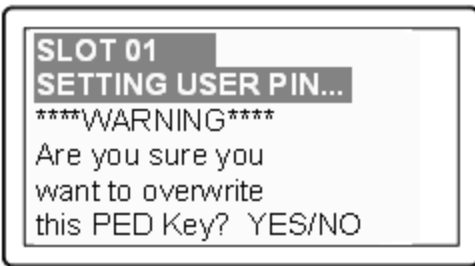


5. The PED *might* continue with:



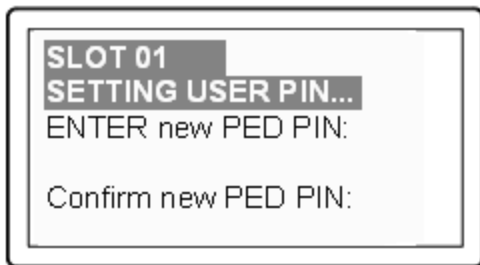
Decide whether this should be a group PED Key (see "What is a Shared or Group PED Key?"), press [YES] or [NO] on the PED keypad, and press [Enter].

6. This is potentially serious business (if you unintentionally overwrite a PED Key that is needed for other purposes), so SafeNet PED asks one more time if you truly intend to overwrite the key's content.



Press [YES] or [NO] on the PED keypad, and press [Enter].

7. Next, you are asked to provide a PED PIN (optional, see ["What is a PED PIN?"](#) — can be 4-to-48 digits, or can be no digits if a PED PIN is not desired).

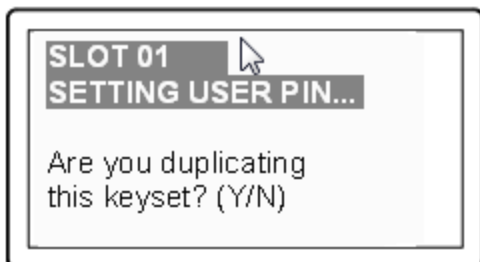


You must press [Enter] to inform the PED that you are finished entering PED PIN digits, or that you have decided not to use a PED PIN (no digits entered).

When you provide a PED PIN – even if it is the null PIN (by just pressing [Enter] with no digits) – the PED requests it a second time, to ensure that you entered it correctly, as you intended.

Press [ENTER] again.

8. You are then prompted



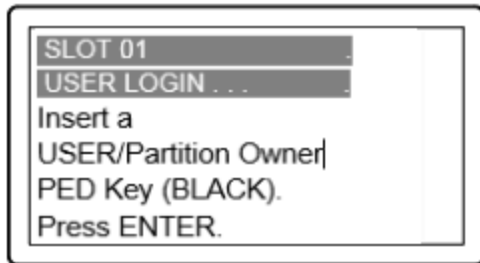
See ["What is a duplicate PED Key?"](#).

Respond "No", if you want the PED to imprint just the one black HSM Admin PED Key and go on to the next step in

creation of the application Partition.

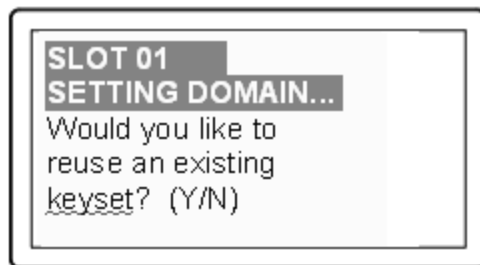
Respond "Yes", if you want the PED to imprint the first black key and then ask for more black PED Keys, until you have imprinted (duplicated) as many as you wish. After each duplicate is made, the PED asks: Would you like to make another duplicate set? Answer "Yes" until you have enough copies, and then press "No".

9. Having created the black key User or Crypto Officer, the HSM needs you to log in as that identity, and prompts:



Leave the black key inserted, and press Enter.

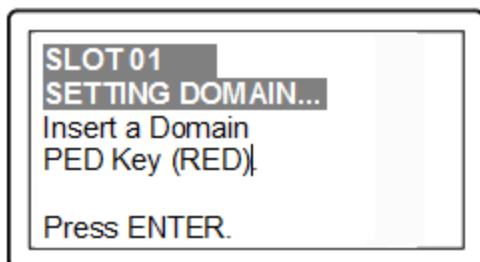
10. Next, the partition's cloning domain must be set, The PED inquires if you intend to reuse a previously imprinted red Domain PED Key.



Respond "Yes" if you have a key from another HSM partition with a cloning domain ID already imprinted on it, that you wish to share/reuse.

Respond "No" if you have a fresh, never-imprinted key, or if you have a key previously imprinted with an ID that you do not wish to preserve.

11. As it did for the black key, the PED now requests values for M and N. Again, enter 1 for each unless you wish to invoke MofN splitting of the domain secret.
12. The PED then prompts for a red Domain PED key with the message



Insert the red HSM Partition Domain PED key [of course, the unlabeled PED Key is generically black - we suggest that you apply the appropriate color sticker either immediately before or immediately after imprinting the key; before, just to ensure it gets done, or after, as a helpful indicator as to which ones are imprinted (with which secret), and which ones still blank] and press [Enter]. A cloning domain is to be imprinted on both the PED key and the HSM Partition.



13. The PED goes through the same prompts as for the black PED Key. Respond as appropriate.

14. Control returns to the command line:

```
'partition create' successful.
```

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

```
[myLuna] lunash:>
```



CAUTION: We recommend that you have at least one backup set of imprinted PED Keys, stored in a safe place, in case of loss or damage to the primary keys.

You might wish to adjust "[\[Step 6\] Set the Partition Policies for Legacy Partitions](#)" on page 179 (Optional).

Otherwise, go to "[Creating an NTL Link Between a Client and a Partition](#)" on page 191 .

Partition creation audit log entry

Each time a partition is created, an entry is added to the audit log. Any subsequent actions logged against the partition are identified by the partition serial number that was generated when the partition was created.

Determining the serial number of a created partition from the audit log

An audit log entry similar to the following is generated when a partition is created on the HSM:

```
5,12/12/17 16:14:14,S/N 150718 session 1 Access 2147483651:2669 SO container operation LUNA_
CREATE_CONTAINER returned RC_OK(0x00000000) container=20 (using PIN (entry=LUNA_ENTRY_DATA_
AREA))
```

It is not obvious from this entry what the serial number is for the created partition. This information, however, can be derived from the log entry, since the partition serial number is simply a concatenation of the HSM serial number and the partition container number, which are specified in the log entry, as highlighted below:

```
5,12/12/17 16:14:14,S/N 150718 session 1 Access 2147483651:2669 SO container operation LUNA_
CREATE_CONTAINER returned RC_OK(0x00000000) container=20 (using PIN (entry=LUNA_ENTRY_DATA_
AREA))
```

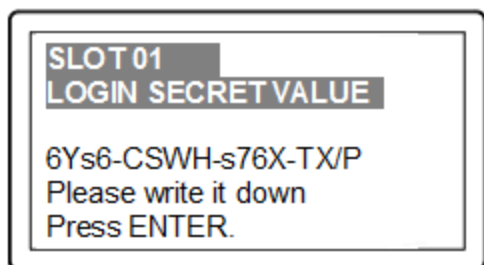
In the example above, the HSM serial number is 150718 and the partition container number is 20. Note that the partition container number is a three-digit number with leading zeros suppressed, so that the actual partition container number is 020. To determine the partition serial number concatenate the two numbers as follows:

```
150718020
```

Use this number to identify the partition in subsequent audit log entries.

Record the Partition Client Password (PED-Auth HSMs)

The PED now generates and displays the Client Password (login secret), by which Clients will later authenticate themselves to this HSM Partition.



Record the Login Secret Value from the PED screen – write it down legibly – because it will never be shown again. This is the HSM Partition password, used to authenticate Client applications that wish to use the HSM Partition on the SafeNet Network HSM.



Note: It might be best to use a text editor, because the majority of errors tend to occur when reading hand-written values. The password/challenge secret is case-sensitive.



Note: The PED times out after eight minutes. You must complete recording the password and press the ENTER button before time-out occurs.

When you press [ENTER] on the PED keypad, control returns to the command prompt, where a success message is displayed:

```
'partition create' successful
```

At the same time, SafeNet PED goes back to "Awaiting command...".

Next you might need to adjust the Partition Policy settings for the new Partition. (Optional see "[Step 6] Set the Partition Policies for Legacy Partitions" on page 179)

Otherwise, see "[Step 7] Create a Network Trust Link Between the Client and the Appliance" on page 183.

About Configuring an Application Partition with Its Own SO

When you are ready to create and configure an application partition, it is assumed that you have already initialized and configured the HSM that is to contain the application partition.

SafeNet HSMs have two types of partition spaces:

- HSM administrative partition - where HSM-wide policies are set and changed, application partitions are created/destroyed, HSM firmware and capabilities are updated, etc.
- Application partition - where cryptographic operations are performed by your applications

Starting with SafeNet HSM firmware version 6.22.0, the ability to have an independent Security Officer per partition was implemented, which results in some changes from previous handling. To distinguish the different styles of partition

we will call them "legacy" and "PPSO" application partitions. The options, when running SafeNet HSM Client software at the most current release are:

HSM firmware version	PPSO Capability applied?	Ownership/oversight of partition (type)	Commands visible in lunacm when this HSM partition is the currently selected slot
<6.22.0	cannot	legacy (see note 1) - <ul style="list-style-type: none"> HSM SO has full ownership of application partition and controls the application throughout its life 	All commands are as they were before SafeNet HSM release 6.0 and firmware 6.22.0
>=6.22	no	legacy option (see note 2) - <ul style="list-style-type: none"> HSM SO has full ownership of application partition and controls the application throughout its life 	lunacm HSM and partition login commands and others are replaced by "role" commands; some other commands have new options/parameters
>=6.22	yes	PPSO option (see note 2) - <ul style="list-style-type: none"> an application partition has its own SO (which is the optional newer way to configure a new application partition) the HSM SO can create or delete the partition, but has no visibility or control in the partition through its life; complete separation of roles 	lunacm HSM and partition login commands, and others, are replaced by "role" commands; some other commands have new options/parameters

Note 1 - No choice. With older firmware, only legacy-style partition management is available.

Note 2 - With firmware 6.22.0 and newer, you can choose to create a partition to be owned/controlled by the HSM SO (legacy), or you can choose to create a partition to be owned and managed by its own SO (the PPSO option, invoked when you specify "slot" while creating a partition in lunacm, or when you specify "hasps" while creating a partition in lunash).

To summarize, until firmware 6.22 (or newer) version of SafeNet HSM receives FIPS validation, and becomes the default version shipping from the factory, you could have a new SafeNet HSM, or one that you already owned, at a firmware version older than 6.22.0. If you install newer SafeNet HSM Client, the included lunacm utility version is capable of supporting both the older command set or the newer command set, depending on the HSM firmware of the currently selected slot. That is, if you have multiple SafeNet HSMs in, or connected to, your SafeNet HSM Client host, which could include:

- internally installed SafeNet PCIe HSM,
- USB-connected SafeNet USB HSM, or
- network (NTLS- or STC-connected) SafeNet Network HSM partitions,

you could see different available command sets as you switch slots in lunacm, depending on the firmware version in the currently selected slot.

The high-level steps are summarized below, to go from a new or factory reset HSM to having a configured application partition, ready for keys and objects and cryptographic operations. Normally, each set of actions would be performed by a different person with different responsibilities.

As the HSM Administrator or SO

1. Complete the certificate exchanges and registrations necessary to create the secure link between Client and application partitions on the appliance.
2. Initialize the HSM; create the SO role and the cloning domain for the HSM's administrative partition (see "[HSM Initialization and Zeroization](#)" on page 1).
3. Log into the administrative partition, as SO.
4. Create the empty application partition.

As the application partition Security Officer

5. Select/set the slot to the newly created application partition.
6. Initialize the SO role and the cloning domain for the application partition.
7. Log into the application partition as SO.
8. Initialize the Crypto Officer role.
9. Log out.

As the application partition Crypto Officer

10. Select/set the slot to the application partition.
11. Log into the application partition as Crypto Officer.
12. Initialize the Crypto User role.

Next step

Note: Before you begin configuring and initializing a PED-authenticated SafeNet HSM, we strongly urge that you familiarize yourself with the pages at "[PED Authentication](#)" on page 1.



Your responses to PED prompts are required during many of the steps. Most of the PED-prompt sequences require decisions that have serious implications for ongoing use of your HSM. PED operations are subject to timeout restrictions for security reasons, meaning that, if your selections and actions are not prompt, the PED will quit the current sequence. In the event of a timeout, you must reissue the HSM command that called the PED.

For PED-authenticated SafeNet Network HSM, the first step is to initialize the HSM; see "[HSM SO Configures PED-authenticated SafeNet Network HSM Partition with SO](#)" on the next page.

For Password-authenticated SafeNet Network HSM, the first step is to initialize the HSM; see "[HSM SO Configures SafeNet Network HSM Password-authenticated Partition with SO](#)" on page 175.

HSM SO Configures PED-authenticated SafeNet Network HSM Partition with SO

An application owner/user has requested an application partition on the HSM, in which applications will run cryptographic operations. These instructions are the actions to be taken by the HSM Security Officer or SO. These instructions assume a PED-authenticated SafeNet HSM supporting the creation of a partition with its own Security Officer.

These instructions assume a SafeNet Network HSM. Initially it is accessed via SSH to create the partition using LunaSH (lunash:>), to create the partition. After the PPSO partition is created, administrative access to that partition moves to a host computer where SafeNet HSM Client software is installed, and where administrative actions are carried out through a Network Trust Link (NTL) via the lunacm tool.

You will need:

- The HSM has firmware 6.22.0, or newer, and the Per-Partition SO capability installed.
- The appliance is configured for network operation and server certificate was created.
- SafeNet Network HSM and your application host computer have exchanged certificates.
- The HSM is in initialized state.
- For PED-Authenticated SafeNet HSM only, a SafeNet PED and PED Keys with labels. These instructions assume that you still have local physical access to your SafeNet Network HSM appliance, for local PED connection, or that your SafeNet PED is remotely connected and you have previously imprinted the HSM and an orange PED Key with a common Remote PED vector. See ["Configuring Remote PED" on page 1](#) and ["Using the Remote PED Feature" on page 1](#).



Note: If you have an existing legacy partition that shares the HSM Administrator (SO) as its SO, and you prefer that it have its own SO, it cannot be directly turned into a partition that has its own SO. You will need to back up any contents, delete the partition, and re-create with an application partition SO.

You can create either type of partition. They can co-exist without conflict on the HSM.



Note: Updating from pre-6.22.0 firmware to firmware version 6.22.0 or newer is necessary to support the PPSO capability, but does not, itself, confer the capability. To enable creation of application partitions with their own Per-Partition Security Officers, you must acquire and install the PPSO capability upgrade.

The PPSO capability Upgrade is destructive. Therefore, you must back up any existing application partition on your HSM, before performing the upgrade, as all partitions and contents are destroyed by the upgrade. After the upgrade is complete, you can create new partitions with Per-Partition SOs, or with legacy-style partitions where the HSM SO retains ownership, or a mix of both, and then restore the pre-existing content to your new partitions from backup.

Preliminary

If you are using a SafeNet PED connected locally to the SafeNet Network HSM, skip to step 4 below.

1. If necessary, have a SafeNet PED connected to a host computer (can be the same computer that acts as your SafeNet HSM Client, but can be another host if desired), with the PED set to "Remote PED mode", and an orange

PED Key ready, containing the same RPV as your SafeNet Network HSM.

2. On the host computer, launch PedServer.exe.

```
C:\Program Files\SafeNet\LunaClient>pedserver -mode start -ip 192.20.10.217 -port 1503
Ped Server Version 1.0.5 (10005)
```

Failed to load configuration file. Using default settings.

```
Ped Server launched in startup mode.
Starting background process
Background process started
Ped Server Process created, exiting this process.
```

```
C:\Program Files\SafeNet\LunaClient>pedserver -mode show
Ped Server Version 1.0.5 (10005)
```

Failed to load configuration file. Using default settings.

```
Ped Server launched in status mode.
failed to unlock: GetLastError(): 183 0xb7
```

```
Server Information:
  Hostname:                MyRPEDhost
  IP:                      172.20.10.217
  Firmware Version:        2.6.0-2
  PedII Protocol Version:  1.0.1-0
  Software Version:        1.0.5 (10005)

  Ped2 Connection Status:  Connected
  Ped2 RPK Count           0
  Ped2 RPK Serial Numbers  (none)

Client Information:        Not Available

Operating Information:
  Server Port:             1503
  External Server Interface: Yes
  Admin Port:              1502
  External Admin Interface: No

  Server Up Time:          52 (secs)
  Server Idle Time:        52 (secs) (100%)
  Idle Timeout Value:      1800 (secs)

  Current Connection Time:  0 (secs)
  Current Connection Idle Time: 0 (secs)
  Current Connection Total Idle Time: 0 (secs) (100%)
  Total Connection Time:    0 (secs)
  Total Connection Idle Time: 0 (secs) (100%)
```

Show command passed.

```
C:\Program Files\SafeNet\LunaClient>
```

3. On the SafeNet Network HSM, start the PED client service, pointing to the PedServer that you just started.

```
[mylunasa] lunash:>hsm ped connect -ip 192.20.10.217 -port 1503
```

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

Command Result : 0 (Success)

```
[mylunasa] lunash:>hsm login
```

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

'hsm login' successful.

Command Result : 0 (Success)

```
[mylunasa] lunash:>
```

4. Log into the SafeNet Network HSM, if not already logged in.

```
[mylunasa] lunash:>hsm login
```

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

'hsm login' successful.

Command Result : 0 (Success)

```
[mylunasa] lunash:>
```

Create the PPSO Partition

1. Run **partition create** command, specifying a partition name, and being sure to include the "-haspso" parameter.

```
[mylunasa] lunash:>partition create -haspso -partition mypsopar1
```

Please ensure that you have purchased licenses for at least this number of partitions: 1

```
    Type 'proceed' to create the uninitialized partition, or
    'quit' to quit now.
    > proceed
```

'partition create' successful.

Command Result : 0 (Success)

```
[mylunasa] lunash:>
```



Note: The command parameters include an option "-label". This is not used when creating PPSO partitions. If you include it, an error message appears, but the "-label" is ignored.

The "-partition <name>" parameter is required.

2. Verify that the partition has been created.

```
[mylunasa] lunash:>hsm show
```

```
Appliance Details:
=====
Software Version:                6.0.0-22

HSM Details:
=====
HSM Label:                      mysahsm
Serial #:                       7000022
Firmware:                       6.22.0
Hardware Model:                 Luna K6
Authentication Method:          PED keys
HSM Admin login status:         Logged In
HSM Admin login attempts left:  3 before HSM zeroization!
RPV Initialized:                Yes
Audit Role Initialized:         No
Remote Login Initialized:       No
Manually Zeroized:              No

Partitions created on HSM (1):
=====
Partition: 16298193222733, Name: mypsoparl

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):              20971
Free Space Left (Bytes):           2076181

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

The PPSO partition now exists, and all future configuration and management of that partition will be handed over to the person who is to become the SO of the new partition. The HSM SO can delete the partition via lunash command, but cannot reach inside the new partition to perform any further administrative actions. This is an important difference from legacy-style partitions, where the HSM SO remains the administrative owner of the application partition and can perform any desired administrative function by means of lunash commands.

In a PPSO partition, the partition SO (and any additional roles that are created for the partition) performs all configuration and management actions via a client connection using LunaCM.

The next step is "[Step 7] Create a Network Trust Link Between the Client and the Appliance" on page 183.

HSM SO Configures SafeNet Network HSM Password-authenticated Partition with SO

An application owner/user has requested an application partition on the HSM, in which applications will run cryptographic operations. These instructions are the actions to be taken by the HSM Security Officer or SO. These instructions assume a Password-authenticated SafeNet HSM supporting the creation of a partition with its own Security Officer.

These instructions assume a SafeNet Network HSM. Initially it is accessed via SSH to create the partition using LunaSH (lunash:>), to create the partition. After the PPSO partition is created, administrative access to that partition moves to a host computer where SafeNet HSM Client software is installed, and where administrative actions are carried out through a Network Trust Link (NTL) via the lunacm tool.

You will need:

- The HSM has firmware 6.22.0, or newer, and the Per-Partition SO capability installed.
- The appliance is configured for network operation and server certificate was created.
- SafeNet Network HSM and your application host computer have exchanged certificates.
- The HSM is in initialized state.



Note: If you have an existing legacy partition that shares the HSM Administrator (SO) as its SO, and you prefer that it have its own SO, it cannot be directly turned into a partition that has its own SO. You will need to back up any contents, delete the partition, and re-create with an application partition SO.

You can create either type of partition. They can co-exist without conflict on the HSM..



Note: Updating from pre-6.22.0 firmware to firmware version 6.22.0 or newer is necessary to support the PPSO capability, but does not, itself, confer the capability. To enable creation of application partitions with their own Per-Partition Security Officers, you must acquire and install the PPSO capability upgrade.

The PPSO capability Upgrade is destructive. Therefore, you must back up any existing application partition on your HSM, before performing the upgrade, as all partitions and contents are destroyed by the upgrade. After the upgrade is complete, you can create new partitions with Per-Partition SOs, or with legacy-style partitions where the HSM SO retains ownership, or a mix of both, and then restore the pre-existing content to your new partitions from backup.

Create the PPSO Partition

1. Log into the SafeNet Network HSM, if not already logged in.

```
[mylunasa] lunash:>hsm login
```

```
'hsm login' successful.
```

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

```
[mylunasa] lunash:>
```

2. Run **partition create** command, specifying a partition name, and being sure to include the "-haspso" parameter.

```
[mylunasa] lunash:>partition create -haspso -partition mypsopar1
```

Please ensure that you have purchased licenses for at least this number of partitions: 1

```

Type 'proceed' to create the uninitialized partition, or
'quit' to quit now.
> proceed
'partition create' successful.

```

```

Command Result : 0 (Success)
[mylunasa] lunash:>

```



Note: The command parameters include an option "-label". This is not used when creating PPSO partitions. If you include it, an error message appears, but the "-label" is ignored.

The "-partition <name>" parameter is required.

3. Verify that the partition has been created.

```
[mylunasa] lunash:>hsm show
```

```

Appliance Details:
=====
Software Version:                6.0.0-22

HSM Details:
=====
HSM Label:                      mysahsm
Serial #:                       7000022
Firmware:                      6.22.0
Hardware Model:                 Luna K6
Authentication Method:          Password
HSM Admin login status:         Logged In
HSM Admin login attempts left:  3 before HSM zeroization!
RPV Initialized:                Yes
Audit Role Initialized:         No
Remote Login Initialized:       No
Manually Zeroized:              No

Partitions created on HSM (1):
=====
Partition: 16298193222733, Name: mypsopar1

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):                20971
Free Space Left (Bytes):             2076181
```

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

The PPSO partition now exists, and all future configuration and management of that partition will be handed over to the person who is to become the SO of the new partition. The HSM SO can delete the partition via lunash command, but cannot reach inside the new partition to perform any further administrative actions. This is an important difference from legacy-style partitions, where the HSM SO remains the administrative owner of the application partition and can perform any desired administrative function by means of lunash commands.

In a PPSO partition, the partition SO (and any additional roles that are created for the partition) performs all configuration and management actions via a client connection using LunaCM.

The next step is "[\[Step 7\] Create a Network Trust Link Between the Client and the Appliance](#)" on page 183.

6

[Step 6] Set the Partition Policies for Legacy Partitions

At this point, you should have initialized the HSM and created one or more HSM Partitions. Before deploying the partitions, review and set the policies that constrain the use of the HSM Partition by clients, as described in the following sections:

- ["Displaying the Current Partition Policy Settings" below](#)
- ["Changing the Partition Policy Settings" on page 181](#)
- ["RSA Blinding Mode" on page 182](#)



Note: This section applies to application partitions that are owned and administered by the HSM SO. If the application partition was created with its own Partition SO, then you cannot use LunaSH (lunash) to administer the partition. All administration of a PPSO partition is carried out by the Partition SO, via LunaCM, from a registered client computer.

Secure Trusted Channel Partition Policy

If you want to use a Secure Trusted Channel (STC) to provide the network link between the partition and authorized clients, you must enable Policy 37: Force Secure Trusted Channel. See ["Enabling or Disabling STC on a Partition" on page 1](#) in the *Administration Guide* for more information.

Displaying the Current Partition Policy Settings

First, display the policies (default) of the created legacy-style application Partition. In order to run the `partition showPolicies` command, you do not need to be logged into the HSM Partition. However, to change policies of either the HSM or an individual Partition, you must login as HSM SO.

To display the current partition policy settings

1. Open a LunaSH session on the appliance.
2. Enter the following command to display current partition capability and policy settings. Capabilities are factory settings. Policies are the means of modifying the adjustable capabilities:

partition showpolicies -partition <partition_name>

For example:

```
lunash:> partition showPolicies -partition mypartition
```

```
Partition Name: mypartition
Partition Num: 65038002
```

The following capabilities describe this partition and can never be changed.

Description	Value
=====	=====
Enable private key cloning	Allowed
Enable private key wrapping	Disallowed
Enable private key unwrapping	Allowed
Enable private key masking	Disallowed
Enable secret key cloning	Allowed
Enable secret key wrapping	Allowed
Enable secret key unwrapping	Allowed
Enable secret key masking	Disallowed
Enable multipurpose keys	Allowed
Enable changing key attributes	Allowed
Enable PED use without challenge	Allowed
Allow failed challenge responses	Allowed
Enable operation without RSA blinding	Allowed
Enable signing with non-local keys	Allowed
Enable raw RSA operations	Allowed
Max failed user logins allowed	10
Enable high availability recovery	Allowed
Enable activation	Allowed
Enable auto-activation	Allowed
Minimum pin length (inverted: 255 - min)	248
Maximum pin length	255
Enable Key Management Functions	Allowed
Enable RSA signing without confirmation	Allowed
Enable Remote Authentication	Allowed
Enable private key unmasking	Allowed
Enable secret key unmasking	Allowed
Enable RSA PKCS mechanism	Allowed
Enable CBC-PAD (un)wrap keys of any size	Allowed
Enable private key SFF backup/restore	Disallowed
Enable secret key SFF backup/restore	Disallowed
Enable Secure Trusted Channel	Allowed

The following policies are set due to current configuration of this partition and may not be altered directly by the user.

Description	Value
=====	=====
Challenge for authentication not needed	False

The following policies describe the current configuration of this partition and may be changed by the HSM Administrator.

Description	Value	Code
=====	=====	=====
Allow private key cloning	On	0
Allow private key unwrapping	On	2
Allow secret key cloning	On	4
Allow secret key wrapping	On	5
Allow secret key unwrapping	On	6

Allow multipurpose keys	On	10
Allow changing key attributes	On	11
Ignore failed challenge responses	On	15
Operate without RSA blinding	On	16
Allow signing with non-local keys	On	17
Allow raw RSA operations	On	18
Max failed user logins allowed	10	20
Allow high availability recovery	On	21
Allow activation	Off	22
Allow auto-activation	Off	23
Minimum pin length (inverted: 255 - min)	248	25
Maximum pin length	255	26
Allow Key Management Functions	On	28
Perform RSA signing without confirmation	On	29
Allow Remote Authentication	On	30
Allow private key unmasking	On	31
Allow secret key unmasking	On	32
Allow RSA PKCS mechanism	On	33
Allow CBC-PAD (un)wrap keys of any size	On	34
Force Secure Trusted Channel	Off	37

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

Changing the Partition Policy Settings

Having viewed the Policy settings, you can now modify a Partition Policy for a given Partition, if required.

To change a partition policy

1. Open a LunaSH session on the appliance.
2. Enter the following command to change a Partition Policy:
partition changepolicy -partition <name of HSM Partition> -policy <policy_code> -value <new_policy_value>
3. Refer to the example below that is applicable to your SafeNet appliance's HSM type.

Policy setting example, SafeNet HSM with Password Authentication

The default minimum password length is 7 characters (which the SafeNet HSM calculates as 255 minus 248, where 255 is the maximum length and 248 is the number that can be subtracted from the maximum to yield the minimum length). We want the minimum Partition password length to be larger than 7 characters – for example, nine. To do that, we would need to change the number that is subtracted from 255 to be 246, instead of the current 248.

1. Login Before Changing Policies
2. Change the selected policy for a Partition labeled "myPartition1". Type:

```
lunash:> partition changePolicy -partition myPartition1 -policy 25 -value 246
'partition changePolicy' successful.
Policy "Minimum pin length (inverted: 255 - min)" is now set to: 246
lunash:>
```
3. Log out of the HSM whenever you finish operations that require HSM login.

```
lunash:> hsm logout
lunash:>
```

Policy setting example, SafeNet HSM with PED Authentication

This is just an example. You do not need to change this particular policy, or any other, except to configure the HSM Partition more appropriately for your use.

1. Login Before Changing Policies
2. Change a selected policy for a Partition labeled "myPartition1". Type:

```
lunash:> partition changePolicy -partition myPartition1 -policy 22 -value 1  
(allows Activation mode to be on)  
partition changePolicy successful  
Policy allow Activation is now set to: 1
```
3. And change the other policy for the same Partition.

```
lunash:> partition -changePolicy -partition myPartition1 -policy 23 -value 1  
(allows autoActivation mode to be on)  
partition changePolicy successful  
Policy allow autoActivation is now set to: 1
```
4. Log out of the HSM whenever you finish operations that require HSM login.

```
lunash:> hsm - logout  
lunash:>
```

RSA Blinding Mode

Blinding is a technique that introduces random elements into the signature process to prevent timing attacks on the RSA private key. Use of this technique may be required by certain security policies, but it does reduce performance.

The HSM Admin or Security Officer can turn this feature on or off.

If RSA blinding is enabled in Capabilities and allowed in Policies, the partition will always run in RSA blinding mode; performance will be lower than SafeNet published performance figures. This is because the deliberate introduction of random elements causes the average signature to take longer to complete.

For maximum performance, you can switch RSA blinding mode off, at the cost of slight additional risk of so-called timing attacks on your keys. It is your decision whether your network and other security measures are sufficiently rigorous that blinding is not needed.

SafeNet HSMs are normally shipped with the Capability set to allow switching blinding on or off, and with the Policy set to **not** use blinding, by default.

[Step 7] Create a Network Trust Link Between the Client and the Appliance

The first step in preparing your clients to use the cryptographic resources provided by the HSM appliance is to create a secure network trust link (NTL) between the client and the appliance. After you create the NTL link between the client and the appliance, you can configure links to individual partitions on the appliance using NTL or Secure Trusted Channel (STC), as described in ["\[Step 8\] Enable the Client to Access a Partition" on page 191](#).

About Network Trust Links

Network Trust Links (NTL) are secure, authenticated network connections between the SafeNet Network HSM and Clients. NTLs use two-way digital certificate authentication and TLS data encryption (version 1.2 is supported in SafeNet Network HSM 6.1) to protect sensitive data as it is transmitted between HSM Partitions on the SafeNet Network HSM and Clients. NTLs consist of the following parts:

- the Network Trust Link Service (NTLS). The NTL server daemon runs on the SafeNet Network HSM appliance and manages the NTL connections to the appliance. NTL uses port 1792 on the SafeNet Network HSM appliance.
- the Network Trust Link Agent (NTLA). The NTL agent runs on a SafeNet HSM client workstation and manages the NTL connections to the workstation. The NTL agent is included in the SafeNet HSM client software.
- The Network Trust Link itself, an encrypted, secure communications channel between the Client's NTLA and the HSM appliance's NTLS.

Network Trust Links use digital certificates to verify the identities of connecting clients. During the initial HSM appliance configuration (see ["Generate a New HSM Server Certificate" on page 116](#)), the appliance administrator generated a unique certificate that identifies the HSM appliance. Similarly, each Client must generate its own certificate that identifies it uniquely. Both the Client and the HSM appliance use these certificates to verify the other's identity before an NTL is created between them.

The Host Trust Link (HTL) Option for VM Clients

Clients running on virtual machines (VMs) are subject to an attack in which a clone of the VM instance is used to gain access to the HSM. To remove this risk, and ensure the integrity of the client, you can optionally specify that you want the network trust link to require host trust link (HTL) client authentication. HTL uses a client-specific, one-time-token on the client that is synchronized with the HSM server to ensure the integrity of the client, and prevent an unsynchronized cloned VM image from connecting to the HSM. See ["Host Trust Link Client Authentication" on page 1](#) in the Administration Guide for more information.

Although designed for VM clients, you can use HTL to secure the client on any NTL link.



CAUTION: To avoid a VM clone attack, do not register a VM client without invoking the HTL option.

Invoking HTL

To invoke the HTL option when creating an NTL, you do the following:

1. Specify the **-htl** option when using the **vtl addserver** command to register the SafeNet Network HSM appliance with the SafeNet HSM client workstation.
2. Specify the **-requirehtl** option when using the LunaSH **client register** command to register the SafeNet HSM client workstation with the SafeNet Network HSM appliance.
3. Generate a one-time token for the SafeNet HSM client workstation using the LunaSH **htl generateott** command
4. Use **scp/pscp** to export the one-time-token to the SafeNet HSM client workstation
5. Rename the one-time-token with the hostname/IP of the SafeNet Network HSM appliance and place it in the `<luna_client_root>/htl` directory. The HTL link is established automatically during the next HTL polling interval.

These steps are included as options in the procedure ["To create a network trust link" below](#).

Creating a Network Trust Link

To create an NTL, the Client and HSM appliance must first exchange certificates. Once the certificates have been exchanged, the Client registers the SafeNet Network HSM's certificate in a trust list, and the SafeNet Network HSM appliance, in turn, registers the Client's certificate in its list of clients. When the certificates have been exchanged and registered at each end, the NTL is ready to use.

"Ready to use" means that an application at the client host (such as *lunacm* or your crypto-using application) can see the registered SafeNet Network HSM application partition(s) as slot(s) in the client slot list, can select such registered partitions by slot number, and can then perform cryptographic operations in those slots after providing appropriate partition authentication (Crypto Officer, Crypto User).



Note: Administration commands can take a few seconds to be noted by the NTLS. If you have added or deleted a client, wait a few seconds before connecting.

To create a network trust link



Note: You must have administrator (or root) access to perform this procedure. Read/write access to the SafeNet HSM client installation directory is required for the certificate exchange.

1. Prepare the client workstation:
 - a. Install the SafeNet HSM client software. See ["SafeNet Client Software Installation " on page 1](#) in the *Installation Guide* for details.
 - b. Install an SSH client to provide secure shell access to the SafeNet appliance for certificate exchange and registration. The PuTTY SSH client (putty.exe) is included in the SafeNet HSM client for Windows.
 - c. Ensure that the client workstation has network access to the SafeNet Network HSM appliance. The appliance auto-negotiates network bandwidth up to Gigabit Ethernet speeds. See ["Recommended Network Characteristics" on page 103](#) for more information.
2. Open a SafeNet HSM client session:
 - a. Open a command prompt or terminal window.
 - b. Go to the SafeNet HSM client installation directory:

Windows	C:\Program Files\SafeNet\LunaClient
Linux/AIX	/usr/safenet/lunaclient/bin
Solaris/HP-UX	/opt/safenet/lunaclient/bin

3. Use **pscp** (Windows) or **scp** (Linux/UNIX) to import the HSM Appliance Server Certificate (**server.pem**) from the SafeNet Network HSM appliance to the SafeNet HSM client workstation. See ["Using the scp and pscp Utilities" on page 1](#) for details. You require the SafeNet Network HSM appliance admin password to complete this step:

If you are importing multiple SafeNet Network HSM appliance's certificates to a client, we suggest that you import the certificates and process each one as it arrives. The **vtl addServer** command (just ahead) copies, moves and renames the current server.pem certificate to reflect the originating appliance's hostname or IP address, as appropriate, and you are always assured that the certificates that are registered in the `.\cert\server` folder are unique. In this method, each appliance server cert arrives in the SafeNet HSM Client folder as (the default) "server.pem" and is safely registered uniquely (in the server cert folder) before the next server.pem arrives and overwrites any earlier version.

If you prefer to import server.pem certificates from multiple appliances, before registering them, then you must rename them as they arrive, to avoid overwriting and losing certificates that all arrive in the same folder with the same default filename.

Windows	<p>Syntax: pscp [options] <user>@<host>:<source_filename> <target_filename></p> <p>Example: To copy the server certificate from host myHSM to the current (.) directory, keeping the same name:</p> <pre>pscp admin@myHSM:server.pem . admin@myHSM's password: server.pem 1 kB 1.1 kB/s ETA: 00:00:00 100%</pre>
Linux/UNIX	<p>Syntax: scp [options] <user>@<host>:<source_filename> <target_filename></p> <p>Example: To copy the server certificate from host IP 192.168.0.123 to the current (.) directory, keeping the same name:</p> <pre>scp admin@192.168.0.123:server.pem . admin@192.168.0.123's password: server.pem 1 kB 1.1 kB/s ETA: 00:00:00 100%</pre>



Note: You must accept the SSH certificate first time you open an scp or ssh link. You can use `lunash:> sysconf fingerprint -ssh` to check the certificate fingerprint.



Note: If the HSM appliance IP or hostname is changed, SSH will detect a mismatch in the HSM appliance's server certification information and warn you of a potential security breach. To resolve this issue, delete the server's certificate information from the client's known host file at: `<user home dir>/.ssh/known_hosts2`, and re-import the server certificate.

4. Register the HSM Server Certificate with the client, using the **vtl addserver** command. Use the **-htl** option if the client is running in a VM, or if you want to the add extra client identity verification offered by HTL to the link (see ["The Host Trust Link \(HTL\) Option for VM Clients" on page 183](#)).

See ["VTL" on page 1](#) in the *Utilities Reference Guide* for full command syntax:

Non-VM clients (without HTL)	vtl addServer -n <SA_hostname_or_IP> -c <server_certificate>
VM clients (with HTL)	vtl addServer -n <SA_hostname_or_IP> -c <server_certificate> -htl



Note: If you specify the **-htl** option, you must also specify the **-requirehtl** option when you register the client with the server, in a subsequent step. If you do not, the server will reject requests to create the link, since it expects an HTL connection to be present.



Note: The **vtl** command is not interactive. It is called from the command line or a shell prompt, it completes its current task, and it exits back to the shell.

Examples:

The following command copies the **server.pem** file that was downloaded in the previous step, from <luna_install_dir> to <luna_install_dir>/cert/server, and registers the **myLunaSA** server certificate (<luna_install_dir>/cert/server/server.pem), with the client:

```
bash-2.05# ./vtl addServer -n myLunaSA -c server.pem
New server myLunaSA successfully added to the server list.
```

The following command copies the **server.pem** file that was downloaded in the previous step, from <luna_install_dir> to <luna_install_dir>/cert/server, and registers the server certificate for the SafeNet Network HSM appliance at IP address 192.168.0.123 (<luna_install_dir>/cert/server/server.pem), with the client and specifies that the link requires HTL client integrity verification:

```
bash-2.05# ./vtl addServer -n 192.168.0.123 -c server.pem -htl
New server 192.168.0.123 successfully added to the server list.
```

As shown, the server certificate from any SafeNet appliance arrives as the default named file **server.pem**. The **vtl addserver** command places a copy of the imported **server.pem** file in the **./cert/server** folder, (re-)naming the new file with the hostname (or IP) that you supply with **-n** in the command. In one example, above, the new copy would be **192.168.0.123Cert.pem**. In the other example, the new cert file would be **myLunaSACert.pem**. Additionally, the command updates the **CAFile.pem** at that location, adding the new, named SafeNet Network HSM server certificate to the list of certs that the client recognizes.

At a minimum you would have one named server certificate file along with the **CAFile.pem** containing a single entry, which must match the certificate. You could have as many unique certificates in that folder as you have SafeNet appliances, and the **CAFile.pem** would contain a matching entry for each cert. Server certificates that do not have an entry in the **CAFile.pem** are ignored. Entries in the **CAFile.pem** that do not correspond to a unique <servername>**Cert.pem** file are ignored.

The downloaded **server.pem** file, from the earlier step, is now redundant and can be deleted, or it will be replaced the next time you download a server certificate from a SafeNet appliance.

5. Create a certificate and private key for the client, using the **vtl createcert** command. See "VTI" on page 1 in the *Utilities Reference Guide* for full command syntax:

```
vtl createcert -n <Luna_client_hostname_or_IP>
```



Note: The client hostname or IP address must be an exact match for the client hostname, as reported using the **hostname** command. If you create a certificate using a hostname parameter that is not an exact letter-case match for the client's hostname, you will be unable to create an NTLS link.

The certificate and private key are saved to the `<luna_install_dir>/cert/client` directory and are named `<Luna_client_hostname_or_IP>.pem` and `<Luna_client_hostname_or_IP>Key.pem`, respectively. The **vtl createcert** command displays the full path-name to the key and certificate files that were generated.

Example: The following command creates a certificate and private key for the client named **myLunaClient**:

```
bash-2.05# ./vtl createCert -n myClient1
Private Key created and written to: /usr/safenet/lunaclient/bin/cert/client/myClientKey.pem
Certificate created and written to: /usr/safenet/lunaclient/bin/cert/client/myClient.pem
```

6. Export the client certificate to the HSM appliance, using **pscp** (Windows) or **scp** (Linux/UNIX). You require the SafeNet Network HSM appliance admin password to complete this step:



Note: You must **scp** to the admin account on the HSM appliance, or the client certificate will not register correctly. The file arriving at the HSM is automatically placed in the appropriate directory. Do not specify a target directory.

Windows	<p>Syntax: pscp [options] <source_filename> <user>@<host>[:<target_filename>]</p> <p>Example: To copy the client certificate (myLunaClient.pem) to the myLunaSA appliance, keeping the same name:</p> <pre>pscp myLunaClient.pem admin@myLunaSA: admin@myLunaSA's password: ***** myLunaClient.pem 1 kB 1.1 kB/s ETA: 00:00:00 100%</pre>
Linux/UNIX	<p>Syntax: scp [options] <source_filename> <user>@<host>[:<target_filename>]</p> <p>Example: To copy the client certificate (myLunaClient.pem) to the SafeNet Network HSM appliance with IP 192.168.0.123, keeping the same name:</p> <pre>scp myLunaClient.pem admin@192.168.0.123: admin@192.168.0.123's password: ***** myLunaClient.pem 1 kB 1.1 kB/s ETA: 00:00:00 100%</pre>

7. Register the client certificate with the HSM appliance using the LunaSH **client register** command. Use the **-requirehtl**, **-ottexpiry**, and **-generateott** options if the client is running in a VM, or if you want to add extra client identity verification offered by HTL to the link (see ["The Host Trust Link \(HTL\) Option for VM Clients" on page 183](#)). You need an admin or operator-level account on the SafeNet Network HSM appliance to complete this step.



Note: You must specify the **-requirehtl** option if you used the **-htl** option when you registered the server with the client. If you do not, the server will reject requests to create the link, since it expects an HTL connection to be present.

- a. Use an SSH client to connect to the SafeNet Network HSM appliance and login using an admin or operator-level account.
- b. Use the LunaSH **client register** command to register the client. See ["client register" on page 1](#) in the *LunaSH Reference Guide* for details.

Non-VM clients (without HTL)	By hostname	client register -client <client_name> -hostname <client_hostname> (Use this version if the client certificate was created using the client's hostname. You will then need to run client hostip command to map the hostname to an IP address. In the upcoming section [Step 8 Enable the Client to Access a Partition, see "Creating an NTL Link Between a Client and a Partition" on page 191 step 4 under sub-section "Assigning a Client to a Partition".)
	By IP address	client register -client <client_name> -ip <client_IP_address> (Use this version if the client certificate was created using the client's IP address as the certificate name.)
VM clients (with HTL)	By hostname	client register -client <client_name> -hostname <client_hostname> -requirehtl [-ottexpiry<seconds>]-generateott
	By IP address	client register -client <client_name> -ip <client_IP_address> -requirehtl [-ottexpiry<seconds>]-generateott



Note: The <client_name>, above can be any string that allows you to easily identify this client. Many people use the hostname, but the <client_name> can be any string that you find convenient. This might sound a little redundant (naming the client twice in one command), but it becomes especially useful if you are not using DNS - in that case, a well-considered <client_name> is likely going to be easier to remember or recognize than the client's IP address.



Note: If you are registering with HTL, you can omit the **-ottexpiry** parameter to use the default expiry; the default, and other options, are configurable. You can also use the htl commands to generate the one-time-token at a later time and configure the HTL options. See ["htl" on page 1 in the LunaSH Reference Guide](#) for details). The one-time token is generated in the current directory with filename <client_hostname_or IP>.**ott**.

Examples:

The following command registers the client at IP address **123.65.98.7** and assigns it a <client_name> of **Standard_Client**:

```
lunash:> client register -client Standard_Client -ip 123.65.98.7
'client register' successful.
Command Result : 0 (Success)
```

The following command registers the client at IP address **74.123.33.2**, assigns it a <client_name> of **VM_Client**, specifies that it requires HTL with the default expiry, and generates a one-time token for the client:

```
lunash:> client register -client VM_Client -ip 74.123.33.2 -requirehtl -generateott
'client register' successful.
One-time token for client VM_Client is ready to use.
Command Result : 0 (Success)
```

- Restart the Network Trust Link service. After registering a client, with a hostname certificate, or after registering a client with an IP certificate and then mapping the client hostname to its IP, stop and start the NTL service, to ensure that the new client is included.

```
lunash:>service restart ntls
```



Note: TCPKeepAliveTCPKeepAlive is a TCP stack option, available at the LunaClient, and at the SafeNet Network HSM appliance. For SafeNet purposes, it is controlled via an entry in the Chrystoki.conf /crystoki.ini file on the LunaClient, and in an equivalent file on SafeNet Network HSM. For SafeNet HSM 6.1 and newer, a fresh client software installation includes an entry "TCPKeepAlive=1" in the "LunaSA Client" section of the configuration file Chrystoki.conf (Linux/UNIX) or crystoki.ini (Windows). Config files and certificates are normally preserved through an uninstall, unless you explicitly delete them. As such, if you update (install) LunaClient software where you previously had an older LunaClient that did not have a TCPKeepAlive entry, one is added and set to "1" (enabled), by default. In the case of update, if TCPKeepAlive is already defined in the configuration file, then your existing setting (enabled or disabled) is preserved.

On the SafeNet Network HSM appliance, where you do not have direct access to the file system, the TCPKeepAlive= setting is controlled by the lunash:> **ntls TCPKeepAlive set** command.

The settings at the appliance and the client are independent. This allows a level of assurance, in case (for example) a firewall setting blocks in one direction.

9. If you are not using the HTL option, this procedure is complete. You can use the LunaSH **client list** command to verify the client registration.

Go to "[Step 8] Enable the Client to Access a Partition" on page 191.

If you are using the HTL option, complete the remaining steps to import the HTL one-time token, rename it to use the SafeNet Network HSM appliance name rather than the SafeNet HSM client workstation name, and activate HTL on the link by placing the token in the <Luna_install_dir>/htl directory.

10. Use **pscp** (Windows) or **scp** (Linux/UNIX) to import the one-time-token (<SA_appliance_hostname_or_IP>.ott) from the SafeNet Network HSM appliance to the SafeNet HSM client workstation. See "Using the scp and pscp Utilities" on page 1 for details. You require the SafeNet Network HSM appliance admin password to complete this step:

Windows	<p>Syntax: pscp [options] <user>@<host>:<source_filename> <target_filename></p> <p>Example: To copy the HTL one-time token from host myLunaClient to the current (.) directory, keeping the same name:</p> <pre>pscp admin@myLunaSA:myLunaClient.ott . admin@myLunaSA's password: myLunaClient.ott 100% ***** 928 00:00</pre>
Linux/UNIX	<p>Syntax: scp [options] <user>@<host>:<source_filename> <target_filename></p> <p>Example: To copy the HTL one-time token from host myLunaClient to the current (.) directory, keeping the same name:</p> <pre>scp admin@myLunaSA:myLunaClient.ott . admin@myLunaSA's password: myLunaClient.ott 100% ***** 928 00:00</pre>

11. Rename the HTL one-time token with the IP address or hostname, as relevant, of your SafeNet Network HSM appliance, and move it to the <Luna_client_install_dir>/htl directory to activate HTL on the link:

Windows	Use Windows Explorer, or enter the following commands from a command prompt window: cd "C:\Program Files\SafeNet\LunaClient" move <client_hostname_or_IP>.ott .\htl\<SA_appliance_hostname_or_IP>.ott
Linux/AIX	Enter the following commands from a terminal window: cd /usr/safenet/lunaclient/bin mv <client_hostname_or_IP>.ott ./htl/<SA_appliance_hostname_or_IP>.ott
Solaris/HP-UX	Enter the following commands from a terminal window: cd /opt/safenet/lunaclient/bin mv <client_hostname_or_IP>.ott ./htl/<SA_appliance_hostname_or_IP>.ott

Example:

```
bash-2.05# cd /usr/safenet/lunaclient/bin
bash-2.05# mv myLunaClient.ott ./htl/myLunaSA.ott
bash-2.05# cd htl
bash-2.05# ls
myLunaSA.ott
```

12. This part of the procedure is complete. After the token has been moved to its correct location and renamed to reflect the SafeNet Network HSM hostname or IP, it will be used during the next HTL polling interval. This happens automatically.

You can use the LunaSH **client list** command to verify the client registration, and the LunaSH **htl show** command to confirm the status of the Host Trust Link. The HTL Status changes to "Up" and the OTT Status changes to "In use" after the client has successfully established a Host Trust Link.

Example:

```
lunash:>client list
registered client 1: 74.123.33.2
Command Result : 0 (Success)

lunash:>htl show
HTL Grace period : 60 seconds
Default OTT expiry : 300 seconds
Client Name      HTL Status      OTT Status      OTT Expiry Time
-----
MyClient         Up              In Use          300 (default)
Command Result : 0 (Success)
```

De-registereing and Re-registering Clients

If you have multiple HSM appliances connected and registered with a client and you de-register that client from one of the HSM appliances, then you must also de-register that HSM appliance on the client side. Failure to do so will result in a "Broken pipe" error, which indicates an incomplete registration.

If you wish to de-register a client and then re-register with a new certificate, on the same HSM appliance, then you must copy the certificate to the HSM appliance (HSM server) and stop and re-start the service called NTLS (see ["service list" on page 1](#) and ["service restart" on page 1](#)). Before such a restart, any connection attempts fail, and "Error on SSL accept" is logged.

[Step 8] Enable the Client to Access a Partition

After creating the network trust link between the client and the appliance, you need to enable the client to access a specific partition on the appliance. You can configure the client to access a partition using an NTL or STC connection, as follows:

NTL client-partition links	Assign the partition to a specific client using the LunaSH client assignpartition command. This allows the client to create NTL connections to the partition to perform cryptographic operations. See "Creating an NTL Link Between a Client and a Partition" below .
STC client-partition links	Enable Secure Trusted Channel (STC) on the client and partition. This disables the NTL connection to the partition, and replaces it with an STC connection. See "Creating an STC Link Between a Client and a Partition" on page 193 .

Creating an NTL Link Between a Client and a Partition

After you establish a network trust link between the client and the appliance, you can assign the Client to a specific Partition on the appliance to grant the client access to the partition. After you assign a client to a partition, the client can establish NTL links to the partition, allowing you to do the following:

- see the partition as a slot in LunaCM,
- use the partition with your cryptographic applications.



Note: You must be connected to the HSM Server and logged in as “admin”.

Assigning a Client to a Partition

Use LunaSH **client assignpartition** command to assign a registered client to an HSM Partition. You might need to use your client IP address as your client name, if you registered your client using an IP address.

This task is performed by the HSM SO, if you are not using STC. If you are configuring a PPSO partition, this is the final task you need to complete before handing off the partition to the partition owner.

To assign a client to a partition

1. Launch LunaSH and log in as the HSM SO.
2. Enter the following command to assign a client to a partition:

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

For example:

```
lunash:> client assignPartition -client ntl_client -partition ntl_partition
'client assignPartition' successful.
Command Result : 0 (Success)
```

3. Enter the following command to verify that the HSM Partition is assigned to the client.

client show -client <clientname>

For example:

```
lunash:> client show -client ntl_client
ClientID:      ntl_client
Hostname:      Luna_Client
HTL Required:  no
OTT Expiry:    n/a
Partitions:    ntl_partition
```

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

client hostip map -client <client_name> -ip <client_IP_address>

For example:

```
lunash:> client hostip map -client ntl_client -ip 192.20.11.21
Command Result : 0 (Success)
```

```
lunash:> client hostip show
```

Client Name	Host Name	Host IP
ntl_client	ntl_client	192.20.11.21

Command Result : 0 (Success)

5. If you are configuring a PPSO partition, hand off possession of the partition to its new owner by providing the contact information (IP address and partition name) and any necessary instructions. The receiving person will become the partition SO and begin configuring the partition for its application.

Verifying Your Setup

Before beginning to use a Client application with your newly configured partition, you can verify that the foregoing setup has been properly performed.

This task is performed by the partition owner, from the SafeNet HSM client workstation used to deploy the partition.

1. On your Client computer, open a command-line console.
2. Go to the software directory (c:\Program Files\SafeNet\LunaClient for Windows, or /usr/safenet/lunaclient for Linux, Solaris or AIX, or /opt/safenet/lunaclient for HP-UX), and type `vtl verify`.
3. The response should be similar to:

```
Slot      Serial #      Label
====      =====
1         2279315 Partition1
```


If you get an error message, then some part of the configuration has not been properly completed. Retrace the procedure.

At this point, the client and HSM are configured and registered with each other. You can now begin to use the SafeNet Network HSM with your application. You can use the `"partition list"` command for a list of HSM Partitions on the HSM, and the `"client list"` command for a list of the clients assigned to an HSM Partition.

4. Setup is complete. We suggest that you browse the *Administration Guide* to develop a deeper understanding of the options and capabilities of your SafeNet Network HSM partition, and of the housekeeping tasks and utilities that you might need.

Client Connection Limits

See ["Connections to the Appliance - Limits"](#) on page 39, for a discussion of the limits for client connections to a SafeNet Network HSM appliance and HSM.

Applications and Integrations

If you have any of dozens of third-party applications, we might already have performed system integration with it, and published an Integration Guide for the application or API that you wish to use. Contact SafeNet Customer Support for the latest list of current integrations, or to request that one be developed.

Creating an STC Link Between a Client and a Partition



Note: Secure Trusted Channel requires firmware 6.22.0 or later.

If you require a higher level of security for your network links than is offered by NTL, such as in cloud environments, or in situations where message integrity is paramount, you can use Secure Trusted Channel (STC) to provide very secure client-partition links. STC offers the following features to ensure the security and integrity of your client-partition communications:

- Privacy of all communicated data through the use of symmetric encryption, so that only the end-points can read any sensitive data.
- Integrity of the communicated data through the use of message authentication codes, so that no eavesdropper could add, delete, modify or replay any command or response.
- Bi-directional authentication of both the HSM and the end-point, so that only authorized entities can establish an STC connection, and there can be no man-in-the-middle attack.

See ["Secure Trusted Channel \(STC\) Network Links"](#) on page 1 in the *Administration Guide* for more information.



Note: STC and NTL can co-exist on the same SafeNet Network HSM appliance, allowing you to configure some partitions to use STC, while other partitions use NTL. The client can also support both STC and NTLS links. However, all links from a specific client to a specific SafeNet Network HSM appliance can be either NTL or STC, but not both.

To use STC, you must enable the following policies:

- HSM policy 39: Allow Secure Trusted Channel. This policy enables STC on the HSM, so that you can configure the

HSM such that some partitions to use STC, while other partitions use NTLS. This policy can only be set by the HSM SO.

- Partition policy 37: Force Secure Trusted Channel. This policy forces the partition to use STC, and requires that HSM policy 39 is also set. For legacy partitions, this policy can only be set by the HSM SO. For partitions with SO, this policy can only be set by the partition SO.

The procedure for creating an STC link between a client and a partition differs depending on whether the partition is a legacy partition or a partition with SO, as follows:

Legacy partitions	See "Creating an STC Link to a Legacy Partition" below
Partitions with SO	See "Creating an STC Link to a Partition With SO" on page 199

Creating an STC Link to a Legacy Partition

The procedure for creating an STC link to a legacy partition consists of the following major steps:

1. Enable the STC policy on the HSM and partition.
2. Export the partition identity public key to a file on the appliance.
3. Create the client token and identity.
4. Exchange the partition and client identity public keys.
5. Register the client identity public key to the partition.
6. Register the partition identity public key with the client.
7. Enable and verify the STC link.

Step 1: Enable the STC policy on the HSM and partition

This step is performed by the HSM SO. For more information, including detailed procedures, examples, and a description of the impact of setting the policies, see ["Enabling or Disabling STC on the HSM" on page 1](#), ["Enabling or Disabling STC on a Partition" on page 1](#) and ["Establishing and Configuring the STC Admin Channel on a SafeNet Network HSM Appliance" on page 1](#) in the *Administration Guide*.

1. Launch LunaSH and log in as the HSM SO.
2. Enter the following command to ensure that policy **39: Allow Secure Trusted Channel** is enabled on the HSM:

```
hsm showpolicies
```

If it is not enabled, enter the following command to enable the policy:

```
hsm changePolicy -policy 39 -value 1
```

3. (Optional) Enable the STC admin channel to provide STC on all links (NTLS and STC) on the portion of the link from the appliance to the HSM, as described in ["Establishing and Configuring the STC Admin Channel on a SafeNet Network HSM Appliance" on page 1](#) in the *Administration Guide*.
4. Enter the following command to ensure that policy **37: Force Secure Trusted Channel** is enabled on the partition:

```
partition showpolicies -partition <partition_name>
```

If it is not enabled, enter the following command to enable the policy:

```
partition changepolicy -partition <partition_name> -policy 37 -value 1
```

Step 2: Export the partition identity public key to a file on the appliance

This step is performed by the HSM SO. Exporting the partition identity public key creates the partition identity if it does not already exist. The public key is exported to a file named <partition_serial_number>.pid on the appliance.

1. Enter the following command to export the partition's public key to a file:

stc partition export -partition <partition_name>

For example:

```
lunash:>stc partition export -partition legacy_stc
Successfully exported partition identity for partition legacy_stc to file 359693009023.pid
Command Result : 0 (Success)
```

Step 3: Create the client token and identity

This step is performed by the root user on the SafeNet HSM client workstation, using LunaCM.

1. Open a SafeNet HSM client session:
 - a. Open a command prompt or terminal window.
 - b. Launch LunaCM:

Windows	C:\Program Files\SafeNet\LunaClient\bin\lunacm
Linux/AIX	/usr/safenet/lunaclient/data/bin/lunacm
Solaris/HP-UX	/opt/safenet/lunaclient/data/bin/lunacm

2. Initialize the STC client software token, or insert the STC client hardware token you have prepared for this client:
 - If you are using an STC client software token, enter the following command to initialize the STC client token.

stc tokeninit -label <token_label>

For example:

```
lunacm:> stc tokeninit -label mySTCclientToken
Successfully initialized the client token.
```

- If you are using an STC client hardware token (SafeNet eToken 7300), insert the token into an available USB port. Before you can use a hardware token, the token must be initialized using the SafeNet Authentication Client on a Windows workstation, as described in ["Using a Hard Token to Store the STC Client Identity" on page 1](#) in the *Administration Guide*.

In addition, you must also install the SafeNet Authentication Client software (8.3 or higher) on the client workstation and add the following line to the **Secure Trusted Channel** section of the **crystoki.ini** (Windows) or **Chrystoki.conf** (UNIX/Linux) file, to specify the path to the SafeNet Authentication Client eToken library:

Windows	ClientTokenLib=C:\Windows\System32\Token.dll
Linux/UNIX	ClientTokenLib=<path_to_libeToken.so> For example, on CentOS, the path is /usr/lib/libeToken.so

3. Enter the following command to create a client identity on the token. The STC client identity public key is automatically exported to the <luna_client_root_dir>/data/client_identities directory:

stc identitycreate -label <client_identity>

For example:

```
lunacm:> stc identitycreate -label mySTCclientID
```

```
Client identity successfully created and exported to file /usr/safenet/lunaclient/data/client_identities/mySTCclientID
```

4. Exit LunaCM.

Step 4: Exchange the partition and client identity public keys

The STC identity public keys are exchanged as follows:

- the client identity public key is copied from the SafeNet HSM client **data/client_identities** directory to the SafeNet Network HSM appliance.
- the partition identity public key is copied from the appliance to the **data/partition_identities** directory on the SafeNet HSM client workstation.

Copying the public keys to or from the SafeNet Network HSM appliance is performed by the SafeNet Network HSM appliance administrator, using **scp** (UNIX/Linux) or **pscp** (Windows).

Copying the public keys to or from the SafeNet HSM client workstation is performed by the root user on the SafeNet HSM client workstation.

The following procedure assumes that you are able to perform both roles, that is, you can log in to the SafeNet HSM client workstation as root, and you possess the SafeNet Network HSM appliance admin password so that you can use scp/pscp to transfer files directly between the SafeNet HSM client workstation and the SafeNet Network HSM appliance.

If your IT and security policies require separation of roles, the keys can be exchanged manually, for example, using email with fingerprint verification, so that the root user on the SafeNet HSM client workstation is responsible for:

- providing the client identity public key to the SafeNet Network HSM appliance administrator.
- copying the partition identity public key to the **data/partition_identities** directory on the SafeNet HSM client workstation.

The SafeNet Network HSM appliance administrator is responsible for:

- using scp/pscp from a separate workstation to copy the client identity public key to the SafeNet Network HSM appliance.
- using scp/pscp from a separate workstation to copy the partition identity public key from the SafeNet Network HSM appliance and then providing it to the root user on the SafeNet HSM client workstation.

- Log in to the SafeNet HSM client workstation as the root user.
- Go to the SafeNet HSM client **data/client_identities** directory:

Windows	cd C:\Program Files\SafeNet\LunaClient\data\client_identities
Linux/AIX	cd /usr/safenet/lunaclient/data/client_identities
Solaris/HP-UX	cd /opt/safenet/lunaclient/data/client_identities

- Export the client identity public key to the HSM appliance, using **pscp** (Windows) or **scp** (Linux/UNIX). You require the SafeNet Network HSM appliance admin password to complete this step:



Note: You must **scp** to the admin account on the HSM appliance, or the client public key will not register correctly. The file arriving at the appliance is automatically placed in the appropriate directory. Do not specify a target directory.

Windows	<p>Syntax: <code>pscp [options] <source_filename> <user>@<host>[:<target_filename>]</code></p> <p>Example: To copy the client identity public key (mySTCclientID) to the myLunaSA appliance, keeping the same name:</p> <pre>pscp mySTCclientID admin@myLunaSA: admin@myLunaSA's password: ***** mySTCclientID 1 kB 1.1 kB/s ETA: 00:00:00 100%</pre>
Linux/UNIX	<p>Syntax: <code>scp [options] <source_filename> <user>@<host>[:<target_filename>]</code></p> <p>Example: To copy the client identity public key (mySTCclientID) to the SafeNet Network HSM appliance with IP 192.168.0.123, keeping the same name:</p> <pre>scp mySTCclientID admin@192.168.0.123: admin@192.168.0.123's password: ***** mySTCclientID 1 kB 1.1 kB/s ETA: 00:00:00 100%</pre>

4. Go to the SafeNet HSM client **data/partition_identities** directory:

Windows	<code>cd C:\Program Files\SafeNet\LunaClient\data\partition_identities</code>
Linux/AIX	<code>cd /usr/safenet/lunaclient/data/partition_identities</code>
Solaris/HP-UX	<code>cd /opt/safenet/lunaclient/data/partition_identities</code>

5. Use **pscp** (Windows) or **scp** (Linux/UNIX) to import the partition public key from the SafeNet Network HSM appliance to the **data/partition_identities** directory on the SafeNet HSM client workstation. See ["Using the scp and pscp Utilities" on page 1](#) for details. You require the SafeNet Network HSM appliance admin password to complete this step:

Windows	<p>Syntax: <code>pscp [options] <user>@<host>:<source_filename> <target_filename></code></p> <p>Example: To copy the partition identity public key (359693009023.pid) from host myHSM to the current (.) directory, keeping the same name:</p> <pre>pscp admin@myHSM:359693009023.pid . admin@myHSM's password: 359693009023.pid 1 kB 1.1 kB/s ETA: 00:00:00 100%</pre>
Linux/UNIX	<p>Syntax: <code>scp [options] <user>@<host>:<source_filename> <target_filename></code></p> <p>Example: To copy the partition identity public key (359693009023.pid) from host IP 192.168.0.123 to the current (.) directory, keeping the same name:</p> <pre>scp admin@192.168.0.123:359693009023.pid . admin@192.168.0.123's password: 359693009023.pid 1 kB 1.1 kB/s ETA: 00:00:00 100%</pre>

Step 5: Register the client identity public key to the partition



Note: Each client identity registered to a partition uses 2332 bytes of storage on the partition. Before registering a client identity to a partition, ensure that there is adequate free space.

This step is performed by the HSM SO. You can register multiple clients to a partition.

1. Launch LunaSH and log in as the HSM SO.
2. Enter the following command to register the client identity public key to the partition:

stc client register -partition <partition_name> -label <client_label> -file <client_public_key>

For example:

```
stc client register -partition mySTCpar -label myClient -file mySTCclientID
```

Step 6: Register the partition identity public key to the client

This step is performed by the root user on the SafeNet HSM client workstation.

1. Log in to the SafeNet HSM client workstation as the root user.
2. Open a SafeNet HSM client session:
 - a. Open a command prompt or terminal window.
 - b. Launch LunaCM:

Windows	C:\Program Files\SafeNet\LunaClient\bin\lunacm
Linux/AIX	/usr/safenet/lunaclient/data/bin/lunacm
Solaris/HP-UX	/opt/safenet/lunaclient/data/bin/lunacm

3. Enter the following command to register the partition identity public key to the client token:

stc partitionregister -file <partition_identity> [-label <partition_label>]

For example:

```
lunacm:> stc partitionregister -file /usr/safenet/lunaclient/data/partition_iden-
tities/359693009023.pid -label mySA_mySTCpartition
```

Step 7: Enable and verify the STC link



CAUTION: When you enable STC on the client, you must specify the SafeNet Network HSM appliance that hosts the partition you want to link to. This forces the client to use STC for all links to the specified SafeNet Network HSM appliance. Any existing NTLS links to the specified SafeNet Network HSM appliance will be terminated.

This step is performed by the root user on the SafeNet HSM client workstation.

1. Log in to the SafeNet HSM client workstation as the root user.
2. Open a SafeNet HSM client session:
 - a. Open a command prompt or terminal window.
 - b. Launch LunaCM:

Windows	C:\Program Files\SafeNet\LunaClient\bin\lunacm
Linux/AIX	/usr/safenet/lunaclient/data/bin/lunacm
Solaris/HP-UX	/opt/safenet/lunaclient/data/bin/lunacm

3. Enter the following command to determine the server ID of the SafeNet Network HSM appliance that hosts the partition:

clientconfig listservers

For example:

```
lunacm:> clientconfig listservers
```

Server ID	Server	Channel	HTL Required
0	192.168.0.123	STC	No
1	192.168.0.59	NTLS	No

4. Enter the following command to enable the STC link:

stc enable -id <server_id>

For example:

```
stc enable -id 0
```

You are about to enable STC to server mySA.
This will initiate an automatic restart of this application. All sessions
logged in through the application will be closed.

Are you sure you wish to continue?
Type 'proceed' to continue, or 'quit' to quit now -> proceed

Successfully enabled STC to connect to server mySA.

At this point, LunaCM restarts. If successful, the partition is listed in the list of available HSMs. You can use the **stc identityshow** command to list the partitions registered to the client token.

5. Enter the following command to verify the link. This command displays the status of the STC link for the current slot:

stc status

For example:

```
lunacm:> stc status
Enabled:      Yes
Status:      Connected
Channel ID:   2
Cipher Name:  AES 256 Bit with Cipher Block Chaining
HMAC Name:    HMAC with SHA 512 Bit
```

Creating an STC Link to a Partition With SO

Creating an STC link to a partition with SO is performed entirely by the root user on the SafeNet HSM client workstation, using LunaCM. The procedure consists of the following major steps:

1. Ensure that you have satisfied the prerequisite conditions.
2. Create the client token and identity.
3. Register the partition identity public key with the client.
4. Enable and verify the STC link.
5. Initialize the partition.



CAUTION: STC allows you to claim the partition as the holder of the partition public key, and creates a one-time temporary STC link to allow you to register the client to the partition. You



must complete all of the steps in this procedure in a single LunaCM session. If you do not, the partition is locked, and will not be accessible. The only workaround is for the HSM SO to delete the partition, create a new partition, and provide you with new partition public key so that you can try again.

Step 1: Ensure that you have satisfied the prerequisite conditions

Before attempting to create an STC link to a partition with SO, ensure that you have satisfied the following prerequisites:

1. You have the STC partition identity public key for the partition. Before using the partition identity public key, it is recommended that you confirm its authenticity by verifying its hash. You can verify the partition identity public key hash after you register the partition identity public key to the client token, as outlined in the following procedure. The HSM SO can use the LunaSH command **stc partition show -partition** <partition_name> to display the partition identity public key hash and provide it to you with the partition identity public key.
2. Confirm with the HSM SO that policy **39: Allow Secure Trusted Channel** is enabled on the HSM.



Note: This procedure automatically registers the client identity to the partition. Each client identity registered to a partition uses 2332 bytes of storage on the partition. Before enabling the STC link, ensure that there is adequate free space on the partition.

Step 2: Create the client token and identity



Note: This step is not required if you have already created a client token and identity. Verify using **stc identityshow**.

1. Open a SafeNet HSM client session:
 - a. Open a command prompt or terminal window.
 - b. Launch LunaCM:

Windows	C:\Program Files\SafeNet\LunaClient\bin\lunacm
Linux/AIX	/usr/safenet/lunaclient/data/bin/lunacm
Solaris/HP-UX	/opt/safenet/lunaclient/data/bin/lunacm

2. Initialize the STC client software token, or insert the STC client hardware token (SafeNet eToken 7300) you have prepared for this client:
 - If you are using an STC client software token, enter the following command to initialize the STC client token.
stc tokeninit -label <token_label>
 For example:

```
lunacm:> stc tokeninit -label mySTCclientToken
```

 Successfully initialized the client token.
 - If you are using an STC client hardware token (SafeNet eToken 7300), insert the token into an available USB port. Before you can use a hardware token, the token must be initialized using the SafeNet Authentication Client on a Windows workstation, as described in ["Using a Hard Token to Store the STC Client Identity" on](#)

[page 1](#) in the *Administration Guide*.

In addition, you must also install the SafeNet Authentication Client software (8.3 or higher) on the client workstation and add the following line to the **Secure Trusted Channel** section of the **crystoki.ini** (Windows) or **Chrystoki.conf** (UNIX/Linux) file, to specify the path to the SafeNet Authentication Client eToken library:

Windows	ClientTokenLib=C:\Windows\System32\libToken.dll
Linux/UNIX	ClientTokenLib=<path_to_libToken.so> For example, on CentOS, the path is /usr/lib/libToken.so

- Enter the following command to create a client identity on the token. The STC client identity public key is automatically exported to the `<luna_client_root_dir>/data/client_identities` directory:

stc identitycreate -label <client_identity>

For example:

```
lunacm:> stc identitycreate -label mySTCclientID
Client identity successfully created and exported to file /usr/
r/safenet/lunaclient/data/client_identities/mySTCclientID
```

Step 3: Register the partition identity public key to the client

- Enter the following command to register the partition identity public key to the client token:

stc partitionregister -file <partition_identity> [-label <partition_label>]

For example:

```
lunacm:> stc partitionregister -file /usr/safenet/lunaclient/partition_iden-
tities/359693009023.pid -label mySA_mySTCpartition
```

- If you were provided with the partition identity public key hash, enter the following command to verify that the hashes match:

stc identityshow

For example:

```
lunacm:> stc ids

Client Identity Name:      myclient
Public Key SHA1 Hash:     5f3395af2ae01ac25c1a27dc25

Partition Name  Partition Serial Number  Partition Public Key SHA1 Hash
par_app3       124338921974             23159590be9b57fd0c9d8a84beed04d4279c01c
par_app47      152943202231             de9f2c7fd25e1b3afad3e85a0bd17d9b100db4b3
par_app12      150253010085             2fd4e1c67a2d28fced849ee1bb76e7391b93eb12
```

If the hashes do not match, enter the following command to deregister the partition identity public key, and contact your HSM SO.

stc partitionderegister -serial <partition_serial_number>

Step 4: Enable and verify the STC link

CAUTION: When you enable STC on the client, you must specify the SafeNet Network HSM appliance that hosts the partition you want to link to. This forces the client to use STC for all links to the specified SafeNet Network HSM appliance. Any existing NTLS links to the specified SafeNet Network HSM appliance will be terminated.

1. Enter the following command to determine the server ID of the SafeNet Network HSM appliance that hosts the partition:

clientconfig listservers

For example:

```
lunacm:> clientconfig listservers
```

Server ID	Server	Channel	HTL Required
0	192.168.0.123	STC	No
1	192.168.0.59	NTLS	No

2. Enter the following command to enable the STC link:

stc enable -id <server_id>

For example:

```
lunacm:> stc enable -id 0
```

You are about to enable STC to server mySA.
This will initiate an automatic restart of this application. All sessions
logged in through the application will be closed.

Are you sure you wish to continue?
Type 'proceed' to continue, or 'quit' to quit now -> proceed

Successfully enabled STC to connect to server mySA.

At this point, LunaCM restarts. If successful, the partition is listed in the list of available HSMs. The slot for the partition is easily identified because it does not have a label, since it is not yet initialized. In the following example, the uninitialized PPSO partition is in slot 1:

```
Available HSMs:
Slot Id -> 0
Label -> stc_legacy
Serial Number -> 359693009024
Model -> K6 Base
Firmware Version -> 6.22.0
Configuration -> Luna User Partition, No SO (PW) Signing With Cloning Mode
Slot Description -> Net Token Slot

Slot Id -> 1
Label ->
Serial Number -> 359693009027
Model -> K6 Base
Firmware Version -> 6.22.0
Configuration -> Luna User Partition, No SO (PW) Signing With Cloning Mode
Slot Description -> Net Token Slot
```

3. Enter the following command to set the current slot to the slot containing the new partition:

slot set -slot <slot>

For example:

```
lunacm:> slot set -slot 1
```

4. Enter the following command to verify the link:

stc status

For example:

```
lunacm:> stc status
Enabled:      Yes
Status:       Connected
Channel ID:   2
Cipher Name:  AES 256 Bit with Cipher Block Chaining
HMAC Name:    HMAC with SHA 512 Bit
```

Step 5: Initialize the partition

When you initialize the partition, the following actions are performed automatically:

- the client identity public key is registered to the partition.
 - partition policy **37: Force Secure Trusted Channel** is enabled on the partition.
1. Set the current slot to the slot containing the uninitialized (unlabelled) partition.
 2. Enter the following command to initialize the partition. On a password-authenticated HSM, you are prompted to specify the partition SO password and domain you want to use for the partition. On a PED-authenticated HSM, you are prompted to attend to the PED to imprint (or provide) the partition SO PED key and domain PED key:

partition initialize -label <partition_label>

For example:

```
lunacm:> par init -label stc_ppso

You are about to initialize the partition.
All contents of the partition will be destroyed.
Are you sure you wish to continue?
Type 'proceed' to continue, or 'quit' to quit now ->proceed

Enter password for Partition SO: *****
Re-enter password for Partition SO: *****

Option -domain was not specified. It is required.
Enter the domain name: *****
Re-enter the domain name: *****

Command Result : No Error
```

The slot now shows the label, indicating that it is initialized:

```
lunacm:> slot list

Slot Id ->          0
Label ->            stc_legacy
Serial Number ->    359693009024
Model ->            K6 Base
Firmware Version -> 6.22.0
Configuration ->    Luna User Partition, No SO (PW) Signing With Cloning Mode
Slot Description -> Net Token Slot
```

```
Slot Id -> 1
Label -> stc_ppso
Serial Number -> 359693009027
Model -> K6 Base
Firmware Version -> 6.22.0
Configuration -> Luna User Partition, No SO (PW) Signing With Cloning Mode
Slot Description -> Net Token Slot
```

You can now create the Crypto Officer and Crypto User roles on the partition. See "[\[Step 9\] Configure PPSO Application Partitions](#)" on page 205.

[Step 9] Configure PPSO Application Partitions

This chapter describes how the partition owner (partition SO) configures a PPSO partition after receiving it from the HSM SO. The configuration tasks you need to perform depend on whether the partition is password-authenticated or PED-authenticated as follows:

Authentication	Tasks
Password	<ol style="list-style-type: none"> 1. "Initialize the Partition SO and Crypto Officer Roles on a PW-Auth PPSO Partition" below 2. "Initialize the Crypto User Role on a PW-Auth PPSO Partition " on page 207
PED	<ol style="list-style-type: none"> 1. "Initialize the Partition SO and Crypto Officer Roles on a PED-Auth PPSO Partition" on page 208 2. "Initialize the Crypto User Role on a PED-Auth PPSO Partition " on page 210 3. "Activate a PED-Auth PPSO Partition for the Crypto Officer Role" on page 211 or "Activate a PED-Auth PPSO Partition for the Crypto User Role" on page 213

Initialize the Partition SO and Crypto Officer Roles on a PW-Auth PPSO Partition

These instructions assume a Password-authenticated SafeNet HSM that has been initialized, and an application partition has been created, capable of having its own Security Officer.

Step 1: Initialize the Partition SO role

This step is performed by the root user on the SafeNet HSM client workstation. If you are using STC to provide the client-partition link, do not perform this procedure, since you already initialized the partition when configuring the STC link. See ["Creating an STC Link Between a Client and a Partition" on page 193](#) for more information.

1. Set the active slot to the created, uninitialized, application partition.

Type **slot set -slot <slot number>**

```
lunacm:> slot set -slot 0
```

```
Current Slot Id:    0      (Luna User Slot 6.22.0 (Password) Signing With Cloning Mode)
```

```
Command Result : No Error
```

```
lunacm:>
```

2. Initialize the application partition, to create the partition's Security Officer (SO).

Type **partition init -label <a label>**

```
lunacm:> par init -label ppsopar
```

```
You are about to initialize the partition.
All partition objects will be destroyed.
```

```
Are you sure you wish to continue?
```

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

```
Command Result : No Error
```

```
lunacm:>
```

Step 2: Initialize the Crypto Officer role

1. The SO of the application partition can now assign the first operational role within the new partition.

Type **role login -name Partition SO**

```
lunacm:> role login -name Partition SO
```

```
Command Result : No Error
```

```
lunacm:>
```

2. Type **role init -name Crypto Officer**

```
lunacm:> role init -name Crypto Officer
```

```
Command Result : No Error
```

```
lunacm:>
```

3. The application partition SO can create the Crypto Officer, but only the Crypto Officer can create the Crypto User. Therefore, the SO must log out to allow the Crypto Officer to log in.

Type **role logout**

```
lunacm:> role logout
```

```
Command Result : No Error
```

```
lunacm:>
```

The next sequence of configuration actions is performed by the Crypto Officer, just created for the application partition. See ["Initialize the Crypto User Role on a PW-Auth PPSO Partition " on the next page.](#)

Initialize the Crypto User Role on a PW-Auth PPSO Partition

These instructions assume

- a Password-authenticated SafeNet HSM has been initialized,
- an application partition has been created,
- a Crypto Officer has been created for the partition, and
- the Crypto Officer password has been conveyed to the person responsible for the Crypto Officer role. See ["Initialize the Partition SO and Crypto Officer Roles on a PW-Auth PPSO Partition" on page 205.](#)

As Crypto Officer, you can do the following:

- Create a Crypto User (limited access user) for the application partition
- Create, delete, change and manipulate cryptographic objects on the application partition, either for your own use or for use by the Crypto User.

To initialize the Crypto User role

1. Set the active slot to the desired application partition, where the Crypto Officer was just created.

Type **slot set -slot <slot number>**

```
lunacm:> slot set -slot 0
```

```
Current Slot Id: 0 (Luna User Slot 6.22.0 (PW) Signing With Cloning Mode)
```

```
Command Result : No Error
```

```
lunacm:>
```

2. Log in as the Crypto Officer.

Type **role login -name Crypto Officer**

```
lunacm:> role login -name Crypto Officer -password $3cr3t
```

```
Command Result : No Error
```

```
lunacm:>
```

3. Create the Crypto User.

Type **role init -name Crypto User**

```
lunacm:> role init -name Crypto User -password Other$ecret
```

```
Command Result : No Error
```

```
lunacm:>
```

The Crypto User can now log in to use applications to perform cryptographic operations using keys and objects created in the partition by the Crypto Officer.

Initialize the Partition SO and Crypto Officer Roles on a PED-Auth PPSO Partition

These instructions assume a PED-authenticated SafeNet HSM that has been initialized, and an application partition has been created, capable of having its own Security Officer.

You will need:

- An HSM that has firmware 6.22.0, or later, and the Per-Partition SO capability installed.
- SafeNet PED and PED Keys with labels. These instructions assume that your SafeNet PED is available locally, but has a working Remote PED connection to the SafeNet Network HSM.
- These instructions assume that you have already made your decisions whether to use all-new, blank PED Keys, or to re-use any existing, imprinted PED Keys for any of the steps.

Step 1: Initialize the Partition SO role

This step is performed by the root user on the SafeNet HSM client workstation. If you are using STC to provide the client-partition link, do not perform this procedure, since you already initialized the partition when configuring the STC link. See ["Creating an STC Link Between a Client and a Partition" on page 193](#) for more information, and skip ahead in this page to ["Step 2: Initialize the Crypto Officer role" on the next page](#).

1. Set the active slot to the created, uninitialized, application partition.

Type **slot set -slot** <slot number>

```
lunacm:> slot set -slot 0
```

```
Current Slot Id:      0      (Luna User Slot 6.22.0 (PED) Signing With Cloning Mode)
```

```
Command Result : No Error
```

```
lunacm:>
```

2. Initialize the application partition, to create the partition's Security Officer (SO).

Type **partition init -label** <a label>

```
lunacm:> par init -label ppsopar
```

```
You are about to initialize the partition.
All partition objects will be destroyed.
```

```
Are you sure you wish to continue?
```

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

```
Please attend to the PED.
```

Respond to SafeNet PED prompts...


```
Command Result : No Error
```

```
lunacm:>
```

Step 2: Initialize the Crypto Officer role

1. The SO of the application partition can now assign the first operational role within the new partition.

Type **role login -name Partition SO**

```
lunacm:> role login -name Partition SO
```

```
Please attend to the PED.
```

```
Command Result : No Error
```

```
lunacm:>
```

2. Type **role init -name Crypto Officer**

```
lunacm:> role init -name Crypto Officer
```

```
Please attend to the PED.
```

Respond to SafeNet PED prompts...

```
Command Result : No Error
```

```
lunacm:>
```

3. The application partition SO can create the Crypto Officer, but only the Crypto Officer can create the Crypto User. Therefore, the SO must log out to allow the Crypto Officer to log in.

Type **role logout**

```
lunacm:> role logout
```

```
Command Result : No Error
```

```
lunacm:>
```

At this point, the Crypto Officer, or an application using the CO's challenge secret/password can perform cryptographic operations in the partition, as soon as the Crypto Officer logs in with **role login -name Crypto Officer**. However, the Crypto Officer can create, modify and delete crypto objects within the partition, in addition to merely using existing crypto objects (sign/verify). You can also create a limited-capability role called Crypto User that can use the objects created by the Crypto Officer, but cannot modify them. The separation of roles is important in some security regimes and operational situations, and where you might be required to satisfy audit criteria for industry or government oversight.

The next sequence of configuration actions is performed by the Crypto Officer, just now created for the application partition. See ["Initialize the Crypto User Role on a PED-Auth PPSO Partition " on the next page.](#)

Initialize the Crypto User Role on a PED-Auth PPSO Partition

These instructions assume

- a PED-authenticated SafeNet HSM has been initialized,
- an application partition has been created,
- a Crypto Officer has been created for the partition, and
- the Crypto Officer PED Key has been conveyed to the person responsible for the Crypto Officer role. See ["Initialize the Partition SO and Crypto Officer Roles on a PED-Auth PPSO Partition" on page 208.](#)

As Crypto Officer, you can do the following:

- Create a Crypto User (limited access user) for the application partition
- Create, delete, change and manipulate cryptographic objects on the application partition, either for your own use or for use by the Crypto User
- Activate the partition for use by applications.

To create a Crypto User for the partition, you will need:

- SafeNet PED and the black Crypto Officer PED Key(s) assigned to you by the SO, as well as blank PED Key(s) with labels for the Crypto User that you are about to create. These instructions assume that your SafeNet PED is locally connected. These instructions assume that you have already made your decisions whether to use all-new, blank PED Keys, or to re-use any existing, imprinted PED Keys for any of the steps.

To create the Crypto User role on a PED-authenticated PPSO application partition

1. Set the active slot to the desired application partition, where the Crypto Officer was just created.

Type **slot set -slot <slot number>**

```
lunacm:> slot set -slot 0
```

```
Current Slot Id:      0      (Luna User Slot 6.22.0 (PED) Signing With Cloning Mode)
```

```
Command Result : No Error
```

```
lunacm:>
```

2. Log in as the Crypto Officer.

Type **role login -name Crypto Officer**

```
lunacm:> role login -name Crypto Officer
```

```
Please attend to the PED.
```

Respond to SafeNet PED prompts...

```
Command Result : No Error
```

```
lunacm:>
```

3. Create the Crypto User.

Type **role init -name Crypto User**

```
lunacm:> role init -name Crypto User
```

```
        Please attend to the PED.
```

Respond to SafeNet PED prompts...

```
Command Result : No Error
```

```
lunacm:>
```

The Crypto User can now log in to use applications to perform cryptographic operations using keys and objects created in the partition by the Crypto Officer.

It is possible for all three of Partition SO, Crypto Officer, and Crypto User to perform their functions against a SafeNet Network HSM partition, from the same SafeNet HSM Client host computer, simply taking turns at the keyboard and the SafeNet PED. It is also possible to work from different computers, as long as any such computer is a registered user of the partition - that is, a working network trust link (NTL) connection is required for each.

In addition, if those persons and their respective SafeNet HSM Client host computers are **not** co-located, then they must arrange to manage their sharing of the Remote PED. Either

- one person must maintain the single Remote PED setup, and the others must coordinate closely with the PED-keeper when authentication to the HSM is required,
- or
- all three can have their own separate PEDs and PedServer instances, but they must coordinate with the appliance administrator to **hsm ped disconnect** any current Remote PED channel before **hsm ped connect -ip <new-ip> -port <new-port>** to establish a Remote PED session with one of the other PedServers.

Crypto Officer or Crypto User Must Log In and Remain Logged In

At this point, the Crypto User, or an application using the CU's challenge secret/password can perform cryptographic operations in the partition, as soon as the Crypto User logs in with **role login -name Crypto User**. However, any event that causes that session to close, including action by the application, requires that the CU must log in again (with the gray PED Key), before the application partition can be used again. For an application that maintains an open session, that is not a handicap. For an application that opens a session for each action, performs the cryptographic action, then closes the session, the CU must be constantly logging in and using the PED and PED Key.

To bypass this limitation, use the Activation feature. See ["Activate a PED-Auth PPSO Partition for the Crypto Officer Role"](#) below or ["Activate a PED-Auth PPSO Partition for the Crypto User Role"](#) on page 213.

Activate a PED-Auth PPSO Partition for the Crypto Officer Role

In this section the Partition SO and the Crypto Officer configure the partition to allow Activation (caching of the authentication), and then Activate it.

These instructions assume

- you are running lunacm on a SafeNet HSM Client host computer containing, or connected to, an HSM with a PPSO application partition,
- that partition has a Crypto Officer created,
- that partition is the currently selected slot

As Crypto Officer of an application partition that is configured for Activation, you can log in once and have your credentials cached and ready in cache as your application opens and closes sessions, without need to re-log-in each time.

To activate a PED-authenticated PPSO application partition for the Crypto Officer role

1. Set the active slot to the desired application partition, .

Type **slot set -slot <slot number>**

```
lunacm:> slot set -slot 0
```

```
Current Slot Id:      0      (Luna User Slot 6.22.0 (PED) Signing With Cloning Mode)
```

```
Command Result : No Error
```

```
lunacm:>
```

2. Log in as the Partition Security Officer.

Type **role login -name Partition SO**

```
lunacm:> role login -name Crypto Officer
```

```
Please attend to the PED.
```

Respond to SafeNet PED prompts...

```
Command Result : No Error
```

```
lunacm:>
```

3. Switch on the activation policy for the partition.

Type **partition changePolicy -slot <slot number> -policy <policy number> -value <policy value>**

```
lunacm:> partition changePolicy -slot 0 -policy 22 -value 1
```

```
Command Result : No Error
```

```
lunacm:>
```

4. Log in as the Partition Crypto Officer.

Type **role login -name Crypto Officer**

```
lunacm:> role login -name Crypto Officer
```

Please attend to the PED.

Respond to SafeNet PED prompts...

```
Command Result : No Error
```

```
lunacm:>
```

Once the partition activation policy is set, the act of logging in by the Crypto Officer role is sufficient to cache the CO black PED Key credential. Now, only the partition challenge secret / password is required to be presented by your application whenever it requires access. The CO credential remains cached until the HSM loses power, or you explicitly log out as CO. The credential is re-cached the next time the CO logs in.



Note: You can stop the automatic caching of the CO credential by having the partition SO switch off the activation policy (22); however doing so also ends activation of the Crypto User role, if that was in effect.

When the CO and CU roles were created, we said you could log in and start using the partition for cryptographic operations by your application(s). Now, with activation in place, you can log in once and put your CO black PED Key or your CU gray PED Key away in a safe place, and the cached credentials will continue to allow your application(s) to open and close sessions and perform their operations within those sessions.

For SafeNet Network HSM and for SafeNet PCIe HSM, you can also set partition policy 23 on (-value 1), for Autoactivation, which goes one step further and preserves the cached credentials through power outages up to 2 hours in duration. Autoactivation does not exist for SafeNet USB HSM; therefore policy 23 cannot be switched on.

Activate a PED-Auth PPSO Partition for the Crypto User Role

In this section the Partition SO and the Crypto User configure the partition to allow Activation (caching of the authentication), and then Activate it.

These instructions assume

- you are running lunacm on a SafeNet HSM Client host computer containing, or connected to, an HSM with a PPSO application partition,
- that partition has a Crypto User created,
- that partition is the currently selected slot
- you have not already performed these actions for Crypto Officer

As Crypto User of an application partition that is configured for Activation, you can log in once and have your credentials cached, and ready in cache as your application opens and closes sessions, without need to re-log-in each time. If the Partition SO already set the Activation policy on behalf of the Crypto Officer, then it applies for both the CO and the CU roles and you can skip to step 4.

To activate a PED-authenticated PPSO application partition for the Crypto User role

1. Set the active slot to the desired application partition, .

Type **slot set -slot <slot number>**

```
lunacm:> slot set -slot 0
```

```
Current Slot Id:      0      (Luna User Slot 6.22.0 (PED) Signing With Cloning Mode)
```

```
Command Result : No Error
```

```
lunacm:>
```

2. Log in as the Partition Security Officer.

Type **role login -name Partition SO**

```
lunacm:> role login -name Crypto Officer
```

```
Please attend to the PED.
```

Respond to SafeNet PED prompts...

```
Command Result : No Error
```

```
lunacm:>
```

3. Switch on the activation policy for the partition.

Type **partition changePolicy -slot <slot number> -policy <policy number> -value <policy value>**

```
lunacm:> partition changePolicy -slot 0 -policy 22 -value 1
```

```
Command Result : No Error
```

```
lunacm:>
```

4. Log in as the Partition Crypto User.

Type **role login -name Crypto User**

```
lunacm:> role login -name Crypto User
```

```
Please attend to the PED.
```

Respond to SafeNet PED prompts...

If the PED prompts for black PED Key, for the Crypto User login, substitute the gray-labeled PED Key, as appropriate.

```
Command Result : No Error
```

lunacm:>

Once the partition activation policy is set, the act of logging in by the Crypto User role is sufficient to cache the CU gray PED Key credential. Now, only the partition challenge secret / password is required to be presented by your application whenever it requires access. The CU credential remains cached until the HSM loses power, or you explicitly log out as CU. The credential is re-cached the next time the CU logs in.



Note: You can stop the automatic caching of the CU credential by having the partition SO switch off the activation policy (22); however doing so also ends activation of the Crypto Officer role, if that was in effect.

When the CO and CU roles were created, we said you could log in and start using the partition for cryptographic operations by your application(s). Now, with activation in place, you can log in once and put your CO black PED Key or your CU gray PED Key away in a safe place, and the cached credentials will continue to allow your application(s) to open and close sessions and perform their operations within those sessions.

For SafeNet Network HSM and for SafeNet PCIe HSM, you can also set partition policy 23 on (-value 1), for Autoactivation, which goes one step further and preserves the cached credentials through power outages up to 2 hours in duration. Autoactivation does not exist for SafeNet USB HSM; therefore policy 23 cannot be switched on.

[Step 10] Set the Partition Policies for PPSO Partitions

At this point, you should have initialized the partition and created the Crypto Officer role and, optionally, the Crypto User role. Before deploying the partitions, review and set the policies that constrain the use of the HSM Partition by clients, as described in the following sections:

- ["Displaying the Current Partition Policy Settings" below](#)
- ["Changing the Partition Policy Settings" on the next page](#)
- ["RSA Blinding Mode" on page 219](#)



Note: This section applies to application partitions that are owned and administered by the HSM SO. If the application partition was created with its own Partition SO, then you cannot use LunaSH to administer the partition. All administration of a PPSO partition is carried out by the Partition SO, via LunaCM, from a registered client computer.

Displaying the Current Partition Policy Settings

First, display the policies (default) of the created legacy-style application Partition. In order to run the `partition showPolicies` command, you do not need to be logged into the HSM Partition. However, to change policies of either the HSM or an individual Partition, you must login as HSM SO.

To display the current partition policy settings

1. Open a LunaCM session.
2. Enter the following command to display current partition capability and policy settings. Capabilities are factory settings. Policies are the means of modifying the adjustable capabilities:

partition showpolicies -partition <partition_name>

For example:

```
lunacm:> partition showpolicies
```

```
Partition Capabilities
0: Enable private key cloning : 0
1: Enable private key wrapping : 0
2: Enable private key unwrapping : 1
3: Enable private key masking : 0
4: Enable secret key cloning : 0
5: Enable secret key wrapping : 1
6: Enable secret key unwrapping : 1
7: Enable secret key masking : 0
10: Enable multipurpose keys : 1
```

```
11: Enable changing key attributes : 1
14: Enable PED use without challenge : 1
15: Allow failed challenge responses : 1
16: Enable operation without RSA blinding : 1
17: Enable signing with non-local keys : 1
18: Enable raw RSA operations : 1
19: Max non-volatile storage space : 3
20: Max failed user logins allowed : 10
21: Enable high availability recovery : 1
22: Enable activation : 0
23: Enable auto-activation : 0
25: Minimum pin length (inverted: 255 - min) : 248
26: Maximum pin length : 255
28: Enable Key Management Functions : 1
29: Enable RSA signing without confirmation : 1
30: Enable Remote Authentication : 1
```

Partition Policies

```
0: Allow private key cloning : 0
1: Allow private key wrapping : 0
2: Allow private key unwrapping : 1
3: Allow private key masking : 0
4: Allow secret key cloning : 0
5: Allow secret key wrapping : 1
6: Allow secret key unwrapping : 1
7: Allow secret key masking : 0
10: Allow multipurpose keys : 1
11: Allow changing key attributes : 1
14: Challenge for authentication not needed : 1
15: Ignore failed challenge responses : 1
16: Operate without RSA blinding : 1
17: Allow signing with non-local keys : 1
18: Allow raw RSA operations : 1
19: Max non-volatile storage space : 3
20: Max failed user logins allowed : 10
21: Allow high availability recovery : 1
22: Allow activation : 0
23: Allow auto-activation : 0
25: Minimum pin length (inverted: 255 - min) : 248
26: Maximum pin length : 255
28: Allow Key Management Functions : 1
29: Perform RSA signing without confirmation : 1
30: Allow Remote Authentication : 0
Command Result : No Error
```

Changing the Partition Policy Settings

Having viewed the Policy settings, you can now modify a Partition Policy for a given Partition, if required.

To change a partition policy

1. Open a LunaCM session.
2. Enter the following command to change a Partition Policy:
partition changepolicy -policy <policy_id> -value <policy_value>

RSA Blinding Mode

Blinding is a technique that introduces random elements into the signature process to prevent timing attacks on the RSA private key. Use of this technique may be required by certain security policies, but it does reduce performance.

The Partition Security Officer can turn this feature on or off.

If RSA blinding is enabled in Capabilities and allowed in Policies, the partition will always run in RSA blinding mode; performance will be lower than SafeNet published performance figures. This is because the deliberate introduction of random elements causes the average signature to take longer to complete.

For maximum performance, you can switch RSA blinding mode off, at the cost of slight additional risk of so-called timing attacks on your keys. It is your decision whether your network and other security measures are sufficiently rigorous that blinding is not needed.

SafeNet HSMs are normally shipped with the Capability set to allow switching blinding on or off, and with the Policy set to **not** use blinding, by default.

Optional Configuration Tasks

After completing the base configuration, you can also perform any of the following optional configuration tasks:

Configure the SafeNet Network HSM appliance to use a Network Time Protocol (NTP) server

You can synchronize a SafeNet Network HSM appliance with a network time protocol (NTP) server. NTP provides a reliable, consistent, and accurate timing mechanism for the appliance using Coordinated Universal Time (UTC), and is the recommended option for providing an accurate date and time for the appliance. SafeNet Network HSM also provides secure NTP. See ["Timestamping – NTP and Time Drift" on page 61](#) in the *SafeNet Network HSM Appliance Administration Guide*.

Configure multiple HSMs to operate in high-availability (HA) mode

High Availability (HA) mode allows you to automatically replicate the data on a HSM/partition over two or more physical HSMs to provide redundancy and load balancing. Applications using an HA HSM/partition do not access it directly. Instead, the HA software creates a virtual slot for the partition and manages which physical HSM is actually used when responding to an application request. See ["High-Availability \(HA\) Configuration and Operation" on page 1](#) in the *Administration Guide*.

Configure SNMP

You can use the SafeNet SNMP MIB to monitor the performance of your HSMs. See ["SNMP Monitoring" on page 1](#) in the *Administration Guide*.

Configure a remote PED

If you are configuring a PED-authenticated HSM, you can configure it to use a remote PED, which allows you to authenticate to the HSM from a remote location. See ["Remote PED" on page 1](#) in the *Administration Guide*.

[Optional] Configure for RADIUS Authentication

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

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

RADIUS Configuration Summary

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

On the RADIUS Server Side

- identify the client systems from which this server will accept requests and return service (this is recorded in the RADIUS server's configuration file)
- identify the users who will be covered by the service

On the RADIUS Client Side (Your SafeNet Network HSM)

- enable RADIUS
- add a RADIUS server, specifying its IP address, and providing the access secret for that server
- check the status of SafeNet Network HSM appliance users
- add desired SafeNet Network HSM appliance users to the RADIUS list, enabling RADIUS authentication for those users
- verify that RADIUS is enabled for any user on your SafeNet Network HSM that needs to use RADIUS

Configuring RADIUS with Your SafeNet Appliance

Follow these steps on the RADIUS Server:

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

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

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

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

```
client 172.20.17.174 {
    ipaddr      = 172.20.17.174
    secret      = testing123
    nas         = other
    shortname    = sa174
}
client 172.20.22.106 {
    ipaddr      = 172.20.22.106
    secret      = testing321
    nas         = other
    shortname    = sa22106
}
```

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

```
/etc/raddb/users:
```

```
sauser162      Cleartext-Password := "userpw654"
sauser171      Cleartext-Password := "userpw987"
sauser172      Cleartext-Password := "userpw789"
sauser173      Cleartext-Password := "userpw456"
sauser174      Cleartext-Password := "userpw321"
```

```
nagios      Cleartext-Password := "nagiospw"
audit      Cleartext-Password := "userpin"
someguy     Cleartext-Password := "userpw"
sauser106   Cleartext-Password := "userpw123"
```

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

Follow these steps on the SafeNet Network HSM appliance:

Note: Without RADIUS, use the command **user add user somename** to add an appliance administrative user on SafeNet Network HSM.



However, **with** RADIUS, use the command **user radiusAdd -u somename** to both create the user on the appliance and add that user to the RADIUS list.

You cannot use **user radiusAdd** to convert an existing user from non-RADIUS to RADIUS. If a named user already exists, with a name you need to employ, then you must **user delete** that user, before creating it again with **user radiusAdd** command.

1. On the SafeNet Network HSM appliance, enable RADIUS.

```
[1722022106] lunash:>sysconf radius enable
```

Command Result : 0 (Success)

2. Add the server (by hostname or IP address), specifying the port to use, and the timeout value in seconds.

```
[1722022106] lunash:>sysconf radius add -s 172.20.15.182 -p 1812 -t 60
```

Enter the server secret:

Re-enter the server secret:

Command Result : 0 (Success)

3. Verify that the desired server has been added.

```
[1722022106] lunash:>sysconf radius show
```

RADIUS for SSH is enabled with the following deployed servers:

server:port	timeout
-----	-----
172.20.15.182:1812	60

Command Result : 0 (Success)

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

```
[1722022106] lunash:>user list
```

Users	Roles	Status	RADIUS
-----	-----	-----	-----
admin	admin	enabled	no

audit	audit	enabled	no
monitor	monitor	disabled	no
operator	operator	disabled	no

Command Result : 0 (Success)

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

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

Creating mailbox file: File exists

Stopping sshd: [OK]

Starting sshd: [OK]

Command Result : 0 (Success)

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

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

User someguy was successfully modified.

Command Result : 0 (Success)

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

```
[1722022106] lunash:>user list
```

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

Command Result : 0 (Success)

```
[1722022106] lunash:>
```