

SafeNet Network HSM 6.3

Configuration Guide

Document Information

Product Version	6.3
Document Part Number	007-011136-015
Release Date	14 July 2017

Revision History

Revision	Date	Reason
A	14 July 2017	Initial release.

Trademarks, Copyrights, and Third-Party Software

Copyright 2001-2017 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 Configuration Guide	9
Customer release notes		9
Gemalto Rebranding		10
Audience		10
Document conventions		10
Notes		10
Cautions		11
Warnings		11
Command syntax and typeface conventions		11
Support Contacts		12
1	[Step 1] Planning Your Configuration	13
Appliance Roles		13
Named Administrative Users and Their Assigned Roles		14
Defined Ability Sets and Custom Roles for Named Users		15
Implications of Backup and Restore of User Profiles		16
Security of Shell User Accounts		16
HSM Roles and Secrets		16
Crypto Officer & Crypto User		17
How the Roles are Invoked		20
Bad Login Attempts		20
Domain Planning		20
Characteristics of Cloning Domains		21
PED-authenticated HSM Planning		22
SafeNet PED Planning		23
What each PED prompt means		24
HSM Initialization and the Blue SO PED Key		25
HSM Cloning Domain and the Red Domain PED Key		26
Partition Owner/User and the black PED Key		26
Remote PED Orange PED Key (RPK)		27
Auditor		27
Secure Recovery Purple PED Key (SRK)		27
Other Considerations		28
Password-authenticated HSM Planning		28
HSM Initialization		28
HSM Cloning Domain		29
Application Partition Owner or Crypto-Officer/Crypto-User		29
Application Partition Cloning Domain		29
Auditor		29
Effect of PPSO on SafeNet Network HSM		30
IPv6 Support and Limitations		31
IPv6 in the Context of the SafeNet Network HSM		32

Limitations When Using IPv6 on the SafeNet Network HSM	33
Configure the IP Address and Network Parameters	34
2 [Step 2] Configure Your Network Settings	35
Gather appliance network setting information	35
Client Requirements	35
Recommended Network Characteristics	36
Bandwidth and Latency Recommendation	36
About Latency and Testing	36
Power-up the HSM Appliance	37
Power On Instructions for the SafeNet Network HSM Appliance	37
Power Off	39
Resuming appliance power	39
Open a Connection	39
First Login and Changing Password	40
Set the System Date and Time and SSH Certificate	42
Timezone Codes	43
Create a new SSH Certificate	44
Configure the IP Address and Network Parameters	45
Gathering Appliance Network Information	46
Configuring the Network Parameters	47
Make Your Network Connection	49
Generate a New HSM Server Certificate	51
Binding Your NTLS or SSH Traffic to a Device	53
Binding Your NTLS Traffic	53
Binding Your SSH Traffic	54
3 [Step 3] Initialize the HSM	56
Password-Authenticated versus PED-Authenticated HSMs	56
Which kind do I have?	56
What if I make a mistake about the type of authentication I present?	56
High-Level Configuration Steps	57
About Initializing a Password-Authenticated HSM	58
Initializing a Password Authenticated HSM	58
Initializing a Password Authenticated HSM	59
About Initializing a PED-Authenticated HSM	62
Recover the SRK	62
Re-split the SRK	64
Other Uses of the SRK	64
Initializing a PED-Authenticated HSM	65
Preparing to Initialize a SafeNet Network HSM [PED-version]	65
Why Initialize?	67
Start a Serial Terminal or SSH session	67
Initialize the HSM	67
Initialization - some additional options and description	74
4 [Step 4] Set the HSM Policies	80
Set HSM Policies (Password Authentication)	80
Set HSM Policies - PED (Trusted Path) Authentication	82

5 [Step 5] Create Application Partitions	86
Choose Partition Type	86
Legacy-style Partitions	86
Per-Partition SO (PPSO) Partitions	86
About Configuring Legacy Partitions	86
Prepare to Create a Legacy Partition (Password Authenticated)	88
About HSM Partitions on the Initialized HSM	88
Create (Initialize) a Password Authenticated Legacy-style Application Partition	89
Partition creation audit log entry	91
Next steps	91
Prepare to Create a Partition (PED Authenticated)	91
About HSM Partitions on the Initialized HSM	91
Create a PED Authenticated Legacy-style Application Partition (f/w pre-6.22.0)	94
About Application Partitions on the Initialized HSM	94
Partition creation audit log entry	100
Create a PED Authenticated Legacy-style Application Partition (f/w 6.22.0 or newer)	101
Partition creation audit log entry	106
Record the Partition Client Password (PED-Auth HSMs)	107
About Configuring an Application Partition with Its Own SO	108
Next step	110
HSM SO Configures PED-authenticated SafeNet Network HSM Partition with SO	110
Preliminary	111
Create the PPSO Partition	113
HSM SO Configures SafeNet Network HSM Password-authenticated Partition with SO	114
Create the PPSO Partition	115
6 [Step 6] Set the Partition Policies for Legacy Partitions	118
Displaying the Current Partition Policy Settings	118
Changing the Partition Policy Settings	120
Policy setting example, SafeNet HSM with Password Authentication	120
Policy setting example, SafeNet HSM with PED Authentication	121
RSA Blinding Mode	121
7 [Step 7] Create a Trusted Link and Register Client and Appliance With Each Other ...	122
Pre-requisites	122
Example	123
Next	124
8 [Step 8] Configure PPSO Application Partitions	125
Initialize the Partition SO and Crypto Officer Roles on a PW-Auth PPSO Partition	125
Initialize the Crypto User Role on a PW-Auth PPSO Partition	127
Initialize the Partition SO and Crypto Officer Roles on a PED-Auth PPSO Partition	128
Initialize the Crypto User Role on a PED-Auth PPSO Partition	130
Crypto Officer or Crypto User Must Log In and Remain Logged In	131
Activate a PED-Auth PPSO Partition for the Crypto Officer Role	131
Activate a PED-Auth PPSO Partition for the Crypto User Role	133
9 [Step 9] Set the Partition Policies for PPSO Partitions	137

Displaying the Current Partition Policy Settings	137
Changing the Partition Policy Settings	138
RSA Blinding Mode	139
10 Optional Configuration Tasks	140
11 Confirm the HSM's Authenticity	141
[Optional] Configure for RADIUS Authentication	143
RADIUS Configuration Summary	143
Configuring RADIUS with Your SafeNet Appliance	143

PREFACE

About the Configuration Guide

This document provides step-by-step instructions for configuring your SafeNet HSM hardware, before you begin using it with your application(s). The instructions are for a basic configuration. Additional configuration options are described in ["Optional Configuration Tasks" on page 140](#).

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

1. ["\[Step 1\] Planning Your Configuration" on page 13](#)
2. ["\[Step 2\] Configure Your Network Settings" on page 35](#)
3. ["\[Step 3\] Initialize the HSM " on page 56](#)
4. ["\[Step 4\] Set the HSM Policies" on page 80](#)
5. ["\[Step 5\] Create Application Partitions" on page 86](#)
6. ["\[Step 6\] Set the Partition Policies for Legacy Partitions" on page 118](#)
7. ["\[Step 7\] Create a Trusted Link and Register Client and Appliance With Each Other" on page 122](#)
8. ["\[Step 8\] Configure PPSO Application Partitions" on page 125](#)
9. ["\[Step 9\] Set the Partition Policies for PPSO Partitions" on page 137](#)

Also review ["Optional Configuration Tasks" on page 140](#) for more configuration options.

Also review ["Confirm the HSM's Authenticity" on page 141](#) for information on confirming that clients are connected to a genuine SafeNet Luna HSM.

This preface also includes the following information about this document:

- ["Customer release notes" below](#)
- ["Gemalto Rebranding" on the next page](#)
- ["Audience" on the next page](#)
- ["Document conventions" on the next page](#)

For information regarding the document status and revision history, see ["Document Information" on page 2](#).

Customer release notes

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

- http://www.securedbysafenet.com/releasenotes/luna/cm_luna_hsm_6-3.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 dir /p.) • Button names (Click Save As.) • Check box and radio button names (Select the Print Duplex check box.) • Dialog box titles (On the Protect Document dialog box, click Yes.) • Field names (User Name: Enter the name of the user.) • Menu names (On the File menu, click Save.) (Click Menu > Go To > Folders.) • User input (In the Date box, type April 1.)
<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>
[optional] [<optional>]	<p>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.</p>
{ a b c } {<a> <c>}	<p>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.</p>

Format	Convention
[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	
Phone (Subject to change. An up-to-date list is maintained on the Technical Support Customer Portal)	Global	+1 410-931-7520
	Australia	1800.020.183
	India	000.800.100.4290
	Netherlands	0800.022.2996
	New Zealand	0800.440.359
	Portugal	800.863.499
	Singapore	800.1302.029
	Spain	900.938.717
	Sweden	020.791.028
	Switzerland	0800.564.849
	United Kingdom	0800.056.3158
United States	(800) 545-6608	
Web	https://safenet.gemalto.com	
Technical Support Customer Portal	https://supportportal.gemalto.com Existing customers with a Technical Support Customer Portal account can log in to manage incidents, get the latest software upgrades, and access the Knowledge Base. To create a new account, click the Register link at the top of the page. You will need your Customer Identifier number.	

[Step 1] Planning Your Configuration

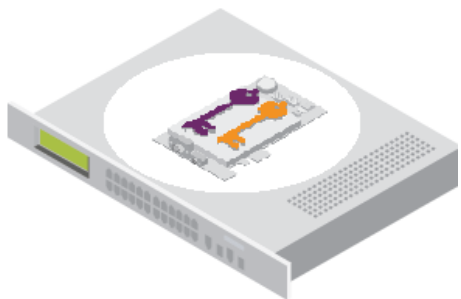
Before initializing your HSM, we suggest taking a moment to consider the following available features and options. Some would be inconvenient to change after your HSM is in service:

- ["Appliance Roles" below](#)
- ["HSM Roles and Secrets" on page 16](#)
- ["Crypto Officer & Crypto User" on page 17](#)
- ["Domain Planning" on page 20](#)
- ["SafeNet PED Considerations" on page 1](#)
- ["PED-authenticated HSM Planning" on page 22](#)
- ["Password-authenticated HSM Planning" on page 28](#)
- ["IPv6 Support and Limitations" on page 31](#)

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. Such roles are

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 Luna Shell 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'
 - a non-administrative role that configures and maintains the audit logs, called 'audit'
- roles that access the HSM, described in "[HSM Roles and Secrets](#)" on page 16

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 Luna Shell (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.

Someone logged into the appliance as 'audit' can see and use the commands used to configure audit logging on the appliance and maintain and verify the resulting logs.

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"
- one 'audit' user, with role "audit", disabled until you enable, default password "PASSWORD"

Those four "built-in" accounts can be neither created nor destroyed, but 'admin' can enable or disable the other three 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.
- multiple audit-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.

User accounts granted the "audit" role can take no actions on the appliance or HSM other than those governing the maintenance of audit logs.

The commands available to the administrative roles are listed in ["User Accounts and Their Privileges" on page 1](#).

For a full description of the audit user's capabilities, see ["Audit Logging" on page 1](#) in the *Administration Guide*.

Why Create Extra Administrative Users?

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

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

```
Apr 13 14:17:15 172 -lunash: Command: syslog tail : john : 192.20.10.133/3107
Command Result : 0 (Success)
```

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

You might find other uses. Please let us know.

Defined Ability Sets and Custom Roles for Named Users

In addition to the pre-defined users and roles, where specific, known combinations and exclusions of actions are conferred (described above), it is possible to define additional Custom Roles with precision. The Custom Roles feature endows each named role with exactly-and-only the specific list of commands that the role is allowed to access and use, and no more. In other words, a Custom Role is as useful as you make it, and as restricted or as safe as you make it.

The lists defining Custom Roles are simple text files with one command per line, as follows:

- The file is created in any text editor that can ensure that each line ends in a UNIX-style linefeed (lf) character.
- The definition file is saved and named in a way that is sensible and practical in your situation, and includes each appliance or HSM command the role is allowed to use.
- The role definition is then uploaded to an administrative user on a SafeNet Network appliance.
- The role definition is imported into an existing named role (not one of the default system roles) with the ["user role import" on page 1](#) command.
- The role with its definition is then assigned to a named user (not one of the default system users) with the ["user role add" on page 1](#) command.
- If a command is on the definition list, it can be used by any named user to which the Custom Role is applied.
- If a command is not included in the list, the user cannot access or use it.

A role can be removed from a named user with the ["user role clear" on page 1](#) command.

Implications of Backup and Restore of User Profiles

The commands "[sysconf config backup](#)" on page 1 and "[sysconf config restore](#)" on page 1 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', 'monitor', and 'audit' 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".



Note: Use of older PuTTY versions, and related tools, can result in the appliance refusing to accept a connection. This can happen if a security update imposes restrictions on connections with older versions. To ensure compatibility, always use the versions of executable files included with the current client installer.

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 20.

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 20](#).

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 - hasps0)
- 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.

IPv6 Support and Limitations

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

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

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

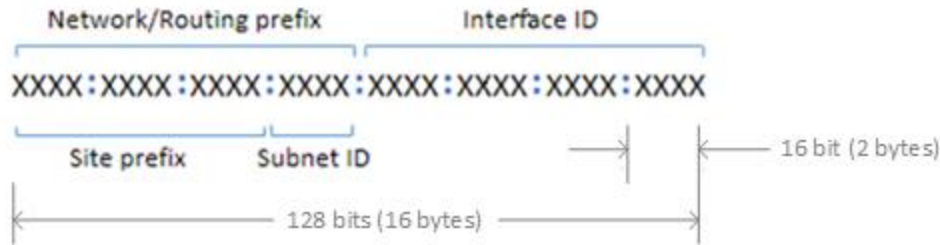
In supporting IPv6, not everything in IPv4 was affected; some subsystems in the internet layer like routing protocols remain the same. The major internet layer upgrades to support IPv6 include:

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

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

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

Global Unicast Address format



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

IPv6 in the Context of the SafeNet Network HSM

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

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

IPv6 Address Configuration Options

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

Static	Use the command " network interface static " on page 1 in the <i>LunaSH Command Reference Guide</i> .
SLAAC	Use the command " network interface slaac " on page 1 in the <i>LunaSH Command Reference Guide</i> Note: You must have a SLAAC-enabled router in your network that is reachable by the HSM appliance to configure a network interface and obtain an IPv6 address using SLAAC protocol.
DHCPv6	Use the command " network interface dhcp " on page 1 in the <i>LunaSH Command Reference Guide</i>

IPv6 Network Gateway

IPv6 devices must use an IPv6 gateway.

This is how you recognize it from the output of the lunash command "[network show](#)" on page 1.

```
Kernel IPv6 routing table
Destination                Next Hop                Flags Metric Ref  U
2018:1:2:3::/64           ::                     UA    256  0
fe80::/64                 ::                     U     256  0
::/0                       fe80::c800:5ff:fedc:8  UGDA 1024  0
::1/128                   ::                     U     0    0
2018:1:2:3:215:b2ff:abe9:2565/128  ::                     U     0    0
fe80::215:b2ff:abe9:2565/128  ::                     U     0    0
ff00::/8                  ::                     U     256  6
```

Generally, the next hop from your network appliance is the gateway.

IPv6 Subnet Mask (Network Mask)

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

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

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

The proper term in IPv6 context is "prefix length". This is how you recognize it from the output of the lunash command "network show" on page 1.

```
Kernel IPv6 routing table
Destination                               Next Hop                                Flags Metric Ref  U
2018:1:2:3::/64                          ::                                     UA      256    0
fe80::/64                                 ::                                     U       256    0
::/0                                       fe80::c800:5ff:fedc:8                UGDA   1024    0
::1/128                                   ::                                     U        0     0
2018:1:2:3:215:b2ff:abe9:2565/128        ::                                     U        0     0
fe80::215:b2ff:abe9:2565/128             ::                                     U        0     0
ff00::/8                                  ::                                     U       256    6
```

Limitations When Using IPv6 on the SafeNet Network HSM

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

Client and SafeNet Network HSM must use the same IP version

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

Simultaneous NTLS connections to IPv4 and IPv6 clients are not supported

You can bind the NTLS service using either IPv4 or IPv6. Therefore, all clients connected to the SafeNet Network HSM at one time must use the same type of addressing.

Single global IPv6 address per network interface

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

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

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

Notes:

1. "RA" stands for Router Advertisement, the critical NDP message used in IPv6 auto-configuration.

2. The above table assumes that a functioning DHCPv6 server is on the network.
3. The configurations shown on this table apply to appliances and not clients.

Example:

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

```
4: eth2: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq state UP qlen 1000
    link/ether 00:15:b2:a8:fd:44 brd ff:ff:ff:ff:ff:ff
    inet6 2018:1:2:3::dcd5/128 scope global dynamic
        valid_lft 1036733sec preferred_lft 691133sec
    inet6 2018:1:2:3:215:b2ff:fea8:fd44/64 scope global noprefixroute dynamic
        valid_lft 2591923sec preferred_lft 604723sec
    inet6 fe80::215:b2ff:fea8:fd44/64 scope link
        valid_lft forever preferred_lft forever
```

Features unsupported for use with IPv6 networks

The following features are currently unsupported on IPv6 networks:

- Secure Trusted Channel
- Host Trust Link
- One-step NTLS (**clientconfig deploy** command)
- Port Bonding
- Server-initiated (peer-to-peer) Remote PED
- Network Time Protocol
- Remote System Logging
- Remote Backup Service (RBS)
- SNMP Monitoring
- IPv6 is not supported for use with UNIX Clients

Configure the IP Address and Network Parameters

To proceed with configuring the IP address and other network parameters for the SafeNet Network HSM, go to ["Configure the IP Address and Network Parameters" on page 45](#).

[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. You should always use the utility files provided with the client.



Note: Use of older PuTTY versions, and related tools, can result in the appliance refusing to accept a connection. This can happen if a security update imposes restrictions on connections with older versions. To ensure compatibility, always use the versions of executable files included with the current client installer.

Go to "[Recommended Network Characteristics](#)" below

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].

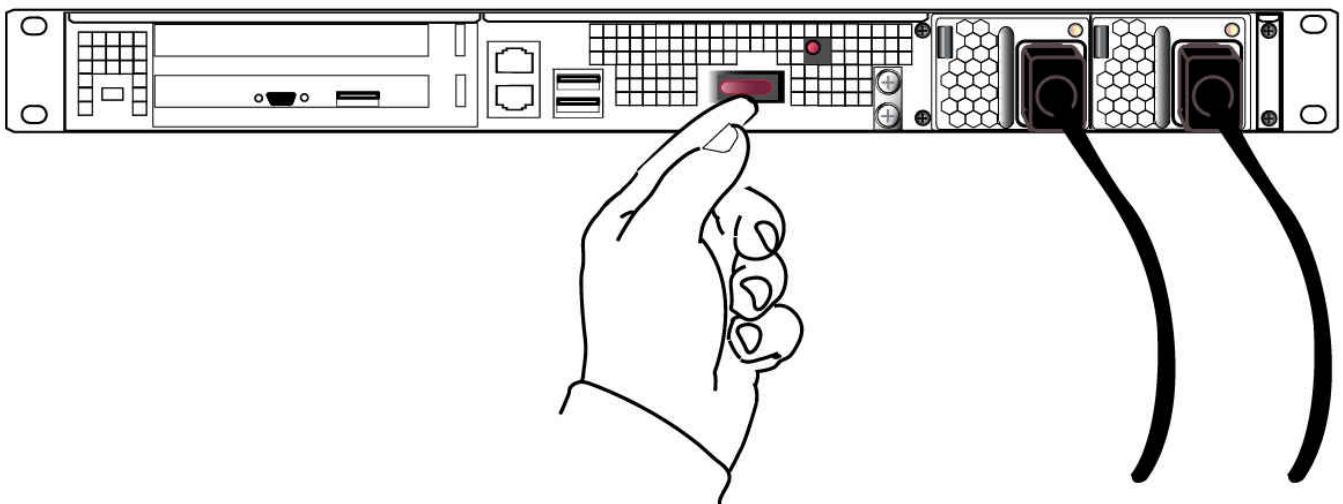
The following instructions require the HSM appliance to be connected and running.

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 ([See "Front-panel Display"](#)) 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.

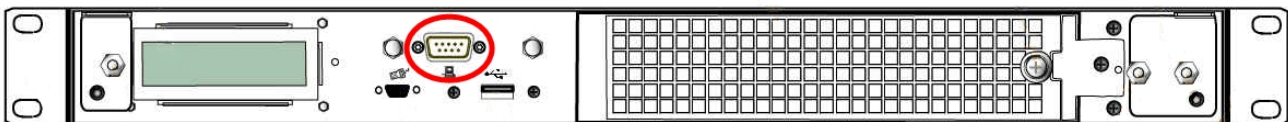
In most cases, it is assumed that automatic resumption from power outage would never be needed, because [adhering to best practices for mission-critical equipment] you would install the appliance with its two power supplies connected to two completely separate, independent power sources, at least one 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 192.20.10.180
```

```
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](#)".

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 1 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.

1. 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.

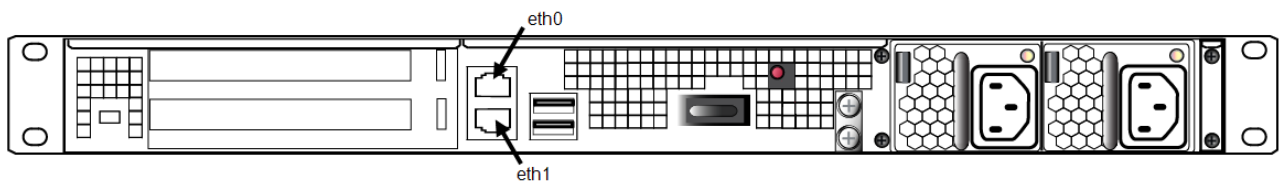
Command Result : 0 (Success)





```

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

Configure the IP Address and Network Parameters

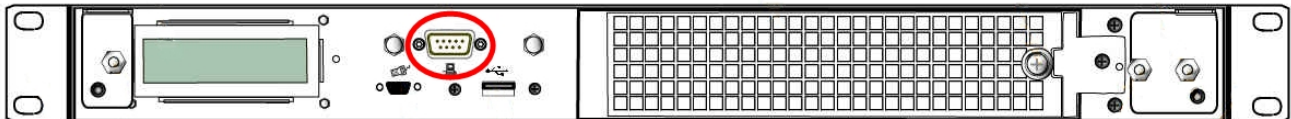
The network device interfaces (eth0 and eth1) are located on the rear of the appliance, as illustrated below:



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

Serial port

Use the serial port to connect a serial device to the SafeNet Network HSM for access to LunaSH to perform initial network configuration. This will prevent SSH admin console disconnection due to changing the appliance IP address. Once you have configured an interface, you can connect the appliance to the network and access LunaSH to complete the network configuration. The serial port is located on the front of the appliance, as illustrated below:



Appliance network configuration

The following network parameters are configured at the appliance level:

- Appliance hostname. A hostname is optional, unless you are using DNS.

Ethernet LAN device configuration

The SafeNet Network HSM is equipped with two individually-configurable Ethernet LAN network devices. You can configure the following network settings for each device:

- IPv4 or IPv6 address. You can configure the addresses using static or DHCP addressing. If you are using IPv6 addressing, you can also use Stateless Autoconfiguration (SLAAC) to have a SLAAC-enabled router in your network automatically configure an IPv6 address on a device.
- Network gateway. IPv4 devices must use an IPv4 gateway. IPv6 devices must use an IPv6 gateway.
- Network mask. IPv4 devices must use dotted-decimal format (for example, 255.255.255.0). IPv6 devices can use full or shorthand syntax.
- Static network route.
- DNS configuration. Although you configure DNS at the device level, the settings you configure for a device are available to all devices on the appliance if the configured device is connected to the network. To ensure DNS access, it is recommended that you configure each device. You can configure the following settings:
 - DNS nameservers. You can add up to three DNS nameservers.
 - DNS search domains.

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

Port bonding: Bond two ports into a single virtual redundant interface

The SafeNet Network HSM supports port bonding, which allows you to bond eth0 and eth1 into a single port, bond0. In a bonded interface, both ports are bound to a virtual interface with a single IP address, with one port active and one port standby. See "[SafeNet Network HSM Appliance Port Bonding](#)" on page 1 for configuration instructions.



Note: This feature is not currently supported for use with IPv6 networks.

NTLS binding: Bind NTLS traffic to a specific device

You can bind the NTLS traffic (used to securely transport cryptographic messages exchanged between a client and the HSM across the network) to a specific Ethernet device (eth0, eth1, bond0, all) on the appliance. This allows you to divide the traffic going to the appliance into cryptographic (destined for the HSM) and administrative (LunaSH) streams, for enhanced security and performance. See "[Binding Your NTLS or SSH Traffic to a Device](#)" on page 53 for more information.

SSH binding: Bind SSH traffic to a specific device, hostname, or IP address

You can optionally bind/restrict the SSH traffic (used to securely transport administrative messages across the network) to a specific Ethernet device (eth0, eth1, bond0, all) on the appliance, to the appliance hostname, or to a specific IP address. This allows you to divide the traffic going to the appliance into cryptographic (destined for the HSM) and administrative (LunaSH) streams, for enhanced security and performance. By default, SSH traffic is unrestricted. See "[Binding Your NTLS or SSH Traffic to a Device](#)" on page 53 for more information.

Gathering Appliance Network Information

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

HSM Appliance Network Parameters

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

- DNS Name Server IP address(es) (per port)
- Search Domain name(s) (per port)
- Device subnet mask (per port)

DNS Entries

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

Other Considerations

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

Configuring the Network Parameters

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



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

To configure the appliance and port network parameters:

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

1. Configure the IP address, network mask, and gateway (optional) on at least one of the Ethernet LAN ports, using the **network interface** command. You can configure the ports to use an IPv4 or IPv6 address. A mix of IPv4 and IPv6 ports is supported.



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

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

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

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

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



Note: Some services are currently unsupported for use with IPv6 networks. See ["IPv6 Support and Limitations" on page 31](#) for more information.

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

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

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

- Optional: If you wish to use the Port Bonding feature described above to configure the bond0 interface, use the **network interface bonding config** and **network interface bonding enable** commands. See ["SafeNet Network HSM Appliance Port Bonding" on page 1](#) for more information.
- Optional: If desired, set the appliance hostname and domain name using the **network hostname** command. You can specify a simple hostname or a Fully Qualified Domain Name (FQDN) using the format <hostname.domainname>. If you supply a hostname that includes a space, all text after the space is ignored. For example, if you typed **network hostname my hsm** the system would assign a hostname of "my". Therefore, if you want "my hsm", use "my_hsm", "my-hsm", or similar.

```
lunash:> network hostname <hostname>
```

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

- Optional: If you wish to use the NTLS or SSH binding features described above to restrict NTLS or SSH messages to an interface (eth0, eth1, bond0, all), use the **ntls bind** or **sysconf ssh** commands. See ["Binding Your NTLS or SSH Traffic to a Device" on page 53](#) for more information.
- Optional: If desired, add a domain name server to the network configuration for the appliance using the **network dns add nameserver** command. The name server is added to the appliance DNS table. You can add up to three different DNS name servers to the appliance DNS table. There is one DNS table that applies to all network devices (ports) on the appliance.



Note: The domain name server settings apply to static network configurations only. If you are using DHCP, the DNS name servers configured on the DHCP server are used. If you are using IPv6, you must configure the name server as described here.

When you add a DNS server, you add it to a specific network device on the appliance (eth0, eth1, bond0). When you add a DNS server to a device, it is added to the DNS table for the appliance and becomes available to all devices on the appliance, provided the device you added it to is connected to the network. For example, if you add a DNS server to eth0, all devices will be able to access the DNS server if eth0 is connected to the network. If eth0 is disconnected from the network, access to the DNS server is lost for any devices to which you did not add the DNS server. To ensure that any DNS server you add is available in the event of a network or port failure, it is recommended that you add it to all devices you will use to connect the appliance to the network.


```
lunash:> network dns add nameserver <IP_address> -device <net_device>
```

- Optional: If desired, add a search domain to the network configuration for the appliance using the **network dns add searchdomain** command. Search domains allow you to avoid typing the complete address of frequently-used Internet domains by automatically appending the search domain to an internet address you specify in LunaSH. For example, if you add the search domain **mycompany.com**, entering the command **network ping hsm1** would search for the domain **hsm1.mycompany.com**. If the domain resolves, it would ping the device with that hostname.

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



Note: The search domain settings apply to static network configurations only. If you are using DHCP, the DNS search domains configured on the DHCP server are used. If you are using IPv6, you must configure the DNS search domain as described here.

When you add a DNS search domain, you add it to a specific network device on the appliance (eth0, eth1, bond0). When you add a search domain to a device, it is added to the DNS table for the appliance and becomes available to all devices on the appliance, provided the device you added it to is connected to the network. For example, if you add a search domain to eth0, all devices will use the search domain if eth0 is connected to the network. If eth0 is disconnected from the network, the search domain is not used by any devices to which you did not add the search domain. To ensure that any search domain you add is available in the event of a network or port failure, it is recommended that you add it to all devices you will use to connect the appliance to the network.

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

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**.

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



Note: If you reconfigure your network settings and you already have client connections established, clients will need to restart any open sessions (for example, restart LunaCM to update the list of partitions).

(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

- 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.
- Login as admin.
- 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).

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

Peers:

```
=====
remote          refid          st t when poll reach  delay  offset  jitter
=====
*LOCAL(0)       .LOCL.         10 l  8   64   1    0.000  0.000  0.000
time-c.timefreq .ACTS.         1 u   7   64   1    78.306 -55560. 0.000
=====
```

Associations:

```
=====
ind assid status  conf reach auth condition  last_event cnt
=====
1 21859 963a  yes  yes none sys.peer sys_peer 3
2 21860 9024  yes  yes none reject reachable 2
=====
```

NTP Time:

```
=====
ntp_gettime() returns code 0 (OK)
time d1504c28.95777000 Wed, Apr 14 2014 12:22:00.583, (.583854),
maximum error 7951596 us, estimated error 0 us
ntp_adjtime() returns code 0 (OK)
  modes 0x0 (),
offset 0.000 us, frequency 0.000 ppm, interval 1 s,
maximum error 7951596 us, estimated error 0 us,
status 0x1 (PLL),
time constant 2, precision 1.000 us, tolerance 512 ppm,
=====
```

Command Result : 0 (Success)

```
[myLuna] lunash:>[
```

Note: Alternatively, you might see return code "5 (ERROR)", which 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 ntlis” 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.

Go to ["Binding Your NTLS or SSH Traffic to a Device"](#) below.

Binding Your NTLS or SSH Traffic to a Device

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

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

Binding Your NTLS Traffic

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

- A specific device (eth0 or eth1)
- All devices (eth0 and eth1)
- A bonded device (bond0). See ["SafeNet Network HSM Appliance Port Bonding"](#) on page 1 in the *Appliance Administration Guide* for more information.

Use the LunaSH **ntlis bind** command to bind the service. The device you configure is not used until all of the following conditions are met:

- it has been configured with a valid IP address
- it is active on the network
- the NTLS service is restarted

This allows you to preconfigure the NTLS binding and have it become active only after you have completed your network configuration.



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

To bind your NTLS traffic to a device

Use the **ntlis bind** command: to bind the NTLS traffic to a network device (eth0, eth1, bond0, all). Include the **-ipv6** option to specify an IPv6 address. You can use the **ntlis show** command to see the current binding.



Note: You can bind the NTLS service using either IPv4 or IPv6. Therefore, all clients connected to the SafeNet Network HSM at one time must use the same type of addressing.

Example

```
lunash:>ntls bind eth0
```

NTLS binding set to network device eth0.
You must restart the NTLS service for the new settings to take effect.

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

```
> proceed
Proceeding...
Restarting NTLS service...
Stopping ntlsl: [ OK ]

Starting ntlsl: [ OK ]

Command Result : 0 (Success)
```



Note: The “Stopping ntlsl” operation might fail in the above example, because NTLS is not yet running on a new HSM appliance. Just ignore the message.

```
lunash:>ntls show
```

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

Command Result : 0 (Success)

```
lunash:>ntls bind eth1
```

NTLS binding set to network device eth1.
You must restart the NTLS service for the new settings to take effect.

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

```
> proceed
Proceeding...
Restarting NTLS service...
Stopping ntlsl: [ OK ]

Starting ntlsl: [ OK ]

Command Result : 0 (Success)
```

```
lunash:>ntls show
```

NTLS is configured to bind to eth1, but it is not active at this time.
NTLS will bind to eth1 if it's active and has a valid IP address when NTLS restarts.
NTLS is currently bound to IP Address: "192.20.11.78" (eth0)

Command Result : 0 (Success)

Binding Your SSH Traffic

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

To bind your SSH traffic to a device or IP address

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

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

```
lunash:>sysconf ssh device eth1

Success:  SSH now restricted to ethernet device eth1 (ip address 192.168.255.2).
Restarting ssh service.
Stopping sshd:                                     [ OK ]
Starting sshd:                                     [ OK ]
Command Result : 0 (Success)
```

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

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

Command Result : 0 (Success)
```

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

```
lunash:>sysconf ssh ip 192.20.10.200

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

Command Result : 0 (Success)
```

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:

- ["About Initializing a Password-Authenticated HSM" on page 58.](#)
- ["About Initializing a PED-Authenticated HSM" on page 62.](#)

[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 of the *Product Overview*.

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 80](#)
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 86](#)
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" on the next page.](#)

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 80](#)

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 80](#)

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 65.

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@192.20.10.202'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.
```



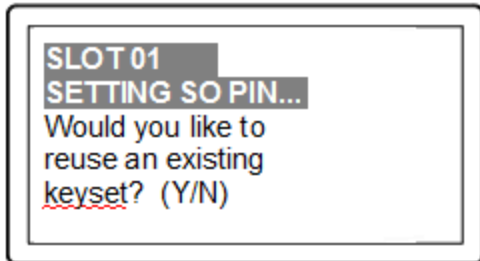
Note: Respond promptly to avoid PED timeout Error. At this time, the PED becomes active and begins prompting you for PED Keys and other responses. For security reasons, this sequence has a time-out, which is the maximum permitted duration, after which an error is generated and the process stops. If you 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 74 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.

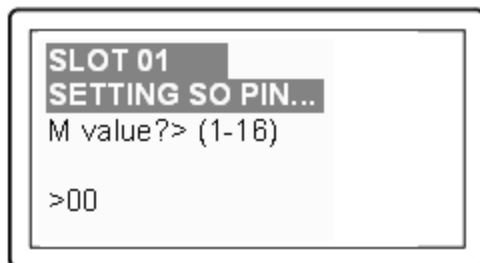
The simplest scenario is your first-ever HSM and new PED Keys. However, you might have previously initialized this HSM and be starting over. Or you might have other HSMs already initialized and need to share the authentication or the domain with your new HSM.

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

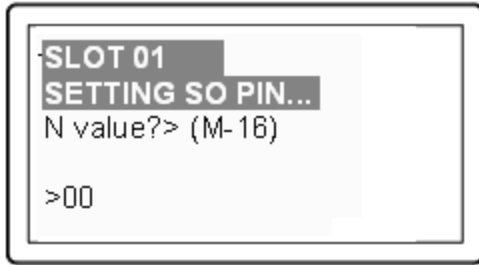


If you say [NO] (on the PED keypad), then you are indicating there is nothing of value on your PED Keys to preserve. On the assumption that you will now be writing onto a new blank PED Key, or onto one that contains old unwanted authentication, SafeNet PED asks you to set MofN values.

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.



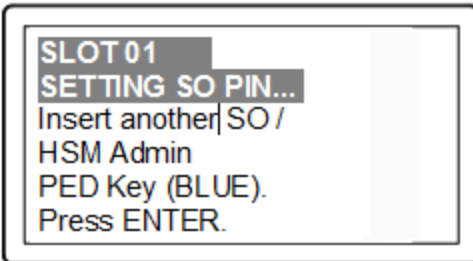
and



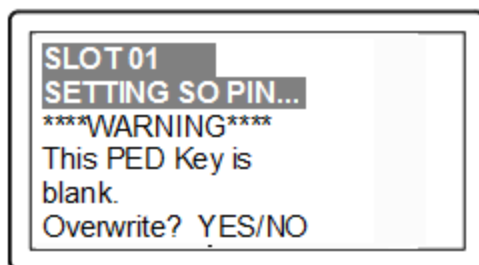
Setting M and N equal to "1" means that the authentication is not to be split, and only a single PED Key will be necessary when the authentication is called for in future.

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.

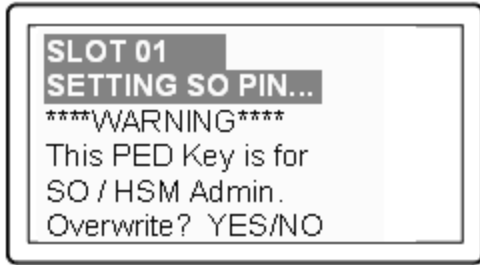
SafeNet PED now asks you to provide the appropriate PED Key - a fresh blank key, or a previously used key that you intend to overwrite, or a previously used key that you intend to preserve and share with this HSM.



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].



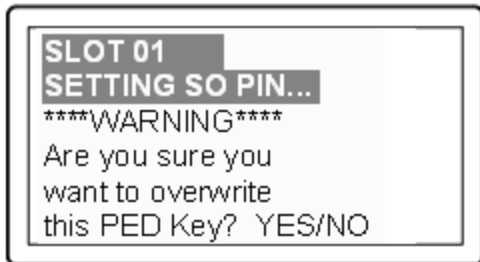
OR



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.

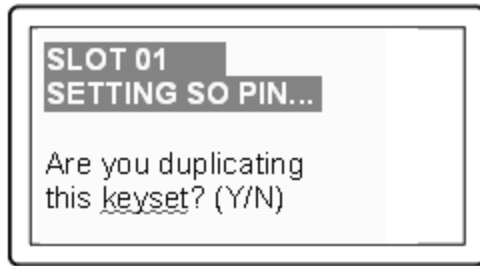


For any situation other than reusing a keyset, SafeNet PED now prompts for you to set a PED PIN. For multi-factor authentication security, the physical PED Key is "something you have". You can choose to associate that with "something you know", in the form of a multi-digit PIN code that must always be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



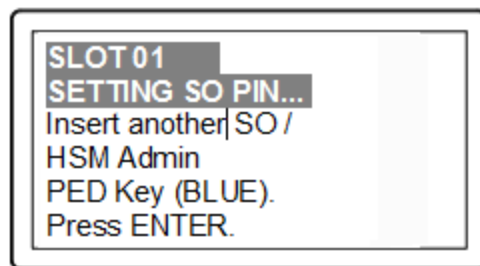
Type a numeric password on the PED keypad, if you wish. Otherwise, just press [Enter] twice to indicate that no PED PIN is desired.

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

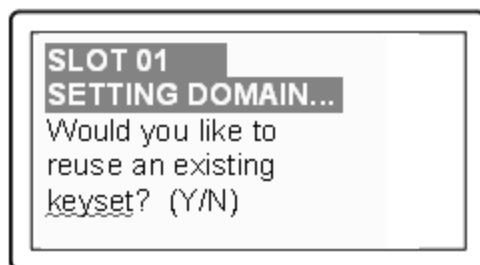


You can respond [YES] and present one or more blank keys, all of which will be imprinted with exact copies of the current PED Key's authentication, or you can say [NO], telling the PED to move on to the next part of the initialization sequence. (You should always have backups of your imprinted PED Keys,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

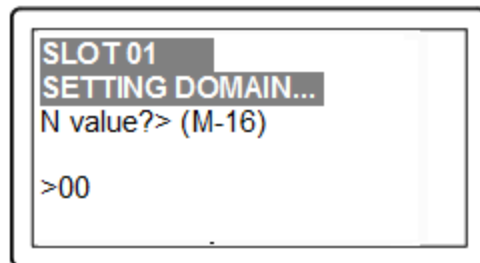
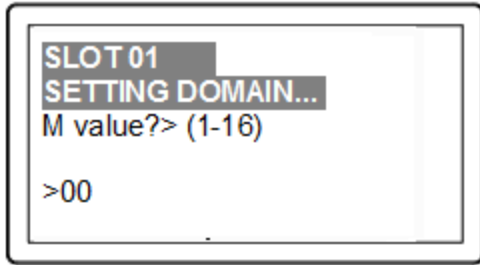


SafeNet PED passes the authentication along to the HSM and then asks the first question toward imprinting a cloning domain:

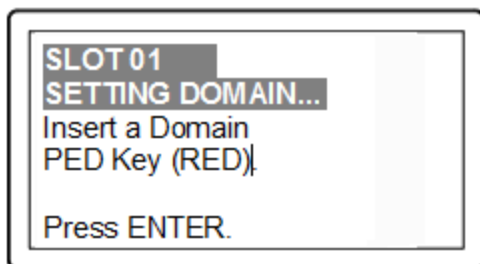


If this is your first SafeNet HSM, or if this HSM will not be cloning objects with other HSMs that are already initialized, then answer [NO]. SafeNet PED prompts for values of M and N.

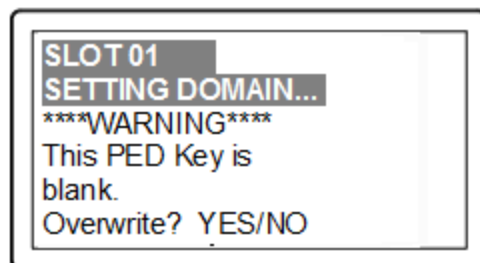
If you have another HSM and wish that HSM and the current HSM to share their cloning Domain, then you must answer [YES]. In that case, SafeNet PED does not prompt for M and N.



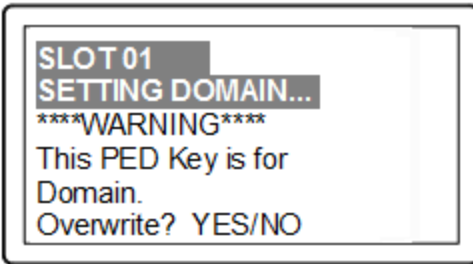
SafeNet PED goes through the same sequence that occurred for the blue SO PED Key, except it is now dealing with a red Domain PED Key.



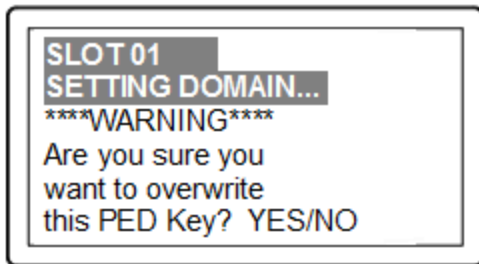
Insert a red HSM Cloning Domain PED key [of course, the unlabeled PED Key is generically black - we suggest that you apply the appropriate color sticker either immediately before or immediately after imprinting the key; before, just to ensure it gets done, or after, as a helpful indicator as to which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



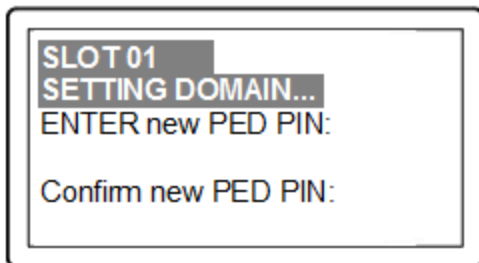
OR



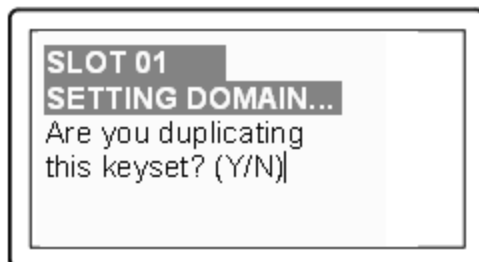
Just as with the blue SO PED Key, the next message is:



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.

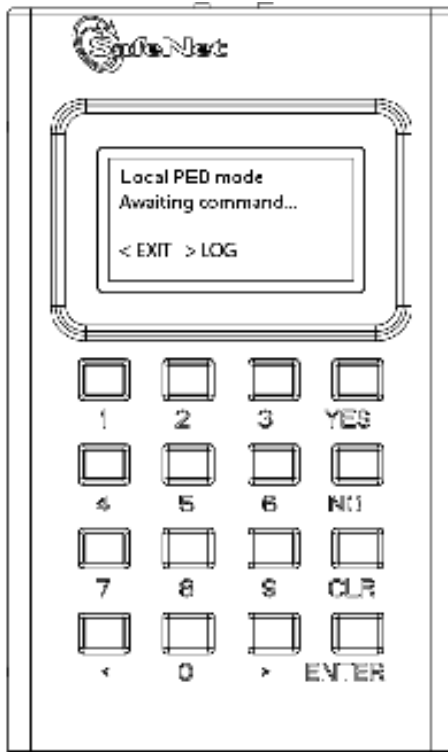
The next step is "[Prepare to Create a Partition \(PED Authenticated\)](#)" on page 91 on the HSM.

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 "[Shared or Group PED Keys](#)" on page 1 in the *Administration Guide*) 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.

Table 1: PED prompt sequences

"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	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)
keyset? (Y/N)		
[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/overwritten) PED Keys to be imprinted with this same secret. If you say "NO", then 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.

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 before the [Enter]).

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 security 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 on-board 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 ["Set HSM Policies - PED \(Trusted Path\) Authentication" on page 82](#)

or

go directly to ["\[Step 5\] Create Application Partitions" on page 86.](#)

[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 82](#)

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 HSM non-volatile storage space	Disallowed 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.

- 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.)

- 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 88](#)

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.

- 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.

- 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.

- 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. To do this, see ["Prepare to Create a Partition \(PED Authenticated\)" on page 91](#)

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 88](#) .

See ["Prepare to Create a Partition \(PED Authenticated\)" on page 91](#).

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 108. 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 35,
- have its HSM SO assigned by "[About Initializing a Password-Authenticated HSM](#)" on page 58.

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:=@ABCDEFGHIJKLMN[OPQRSTUVWXYZ]^_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:=?@ABCDEFGHIJKLMN[OPQRSTUVWXYZ]^_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:;<=>?@ABCDEFGHIJKLMN[OPQRSTUVWXYZ[\]^_`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 108.](#)
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 118 (Optional).

Otherwise, go to "[Assign a Client to an HSM Partition](#)" on page 1 .

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 "[Creating a Network Link Between the Client and the Partition](#)" on page 1)

- have its HSM SO and its Cloning Domain assigned (see ["About Initializing a PED-Authenticated HSM" on page 62](#)).

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).



Note: Use of older PuTTY versions, and related tools, can result in the appliance refusing to accept a connection. This can happen if a security update imposes restrictions on connections with older versions. To ensure compatibility, always use the versions of executable files included with the current client installer.

Login as HSM SO

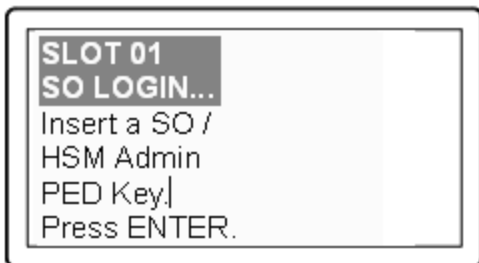
1. To create HSM Partitions, you must login to the HSM as HSM Security Officer or SO. Ensure that the PED is connected to the PED port on your HSM host , and that the PED is powered on and "Awaiting command..."

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](#) of the *Installation Guide* and ["Configuring Remote PED" on page 1](#) of the *Administration Guide*).

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 101

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 110

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:=@ABCDEFGHIJKLMN OPQRSTUVWXYZ[]^_abcdefghijklmnopqrstuvw xyz{|}~
```

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:=?@ABCDEFGHIJKLMN OPQRSTUVWXYZ[]^_abcdefghijklmnopqrstuvw xyz{|}~
```

(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:;<=>?@ABCDEFGHIJKLMN OPQRSTUVWXYZ[\]^_`abcdefghijklmnopqrstuvw xyz{|}~
```

(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'
```

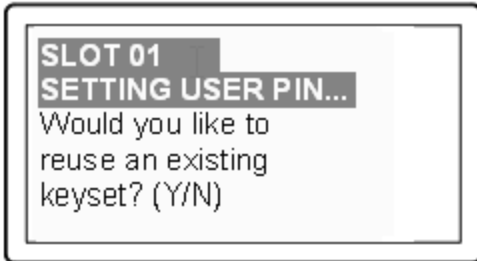
```
> proceed
```

```
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.

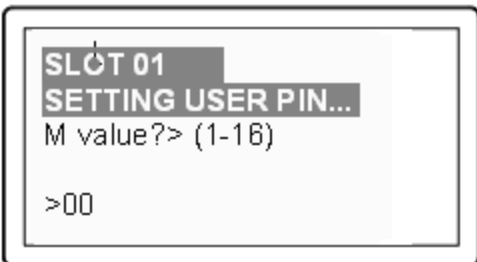
- The PED inquires if you intend to reuse a pre-existing imprinted black PED Key.



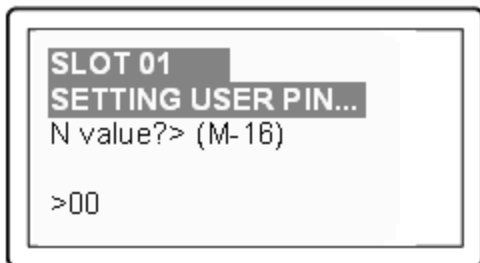
Respond "Yes" if you have a key from another HSM partition with a partition Owner ID already imprinted on it, that you wish to share/reuse. The authentication data on that PED Key will be preserved and used for this partition. Respond "No" if you have a fresh, never-imprinted key, or if you have a key 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 of the *Administration Guide* for more detail)

- The PED requests values for :



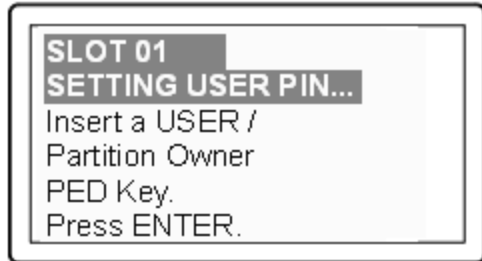
and



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

MofN" on page 1 of the *Administration Guide*).

- 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.

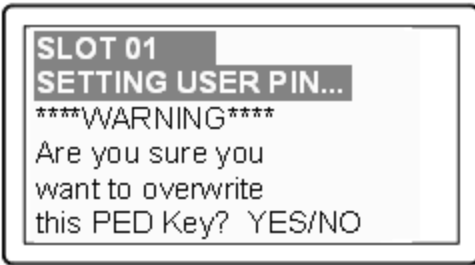


- The PED *might* continue with:



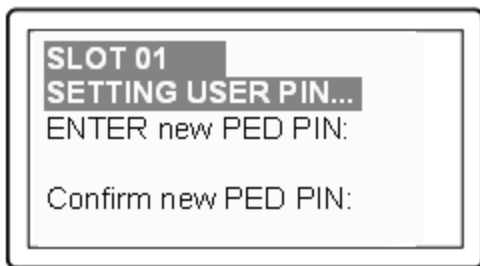
Decide whether this should be a group PED Key (see "[Shared or Group PED Keys](#)" on page 1), press [YES] or [NO] on the PED keypad, and press [Enter].

- 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].

- 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).

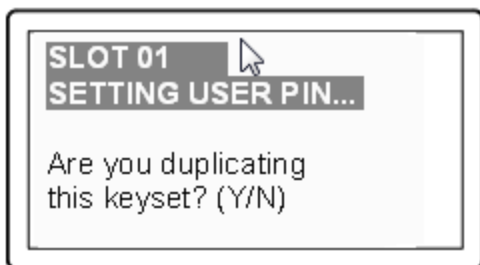


You must press [Enter] to inform the PED that you are finished entering PED PIN digits, or that you have decided not to use a PED PIN (no digits entered).

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.

- You are then prompted



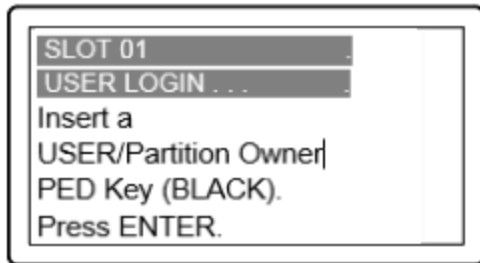
See ["Duplicating PED Keys" on page 1](#).

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:



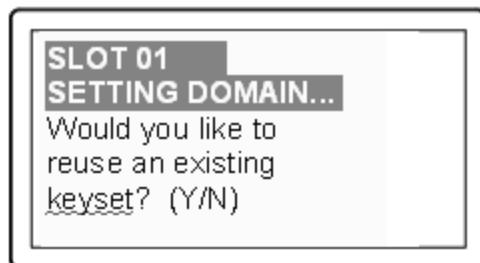
Leave the black key inserted, and press Enter.

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.

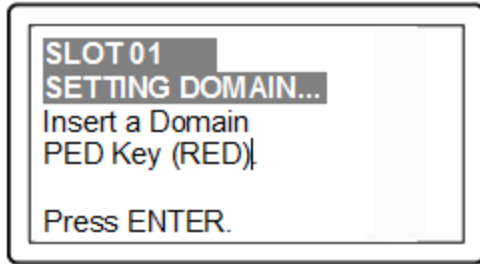
10. The PED inquires if you intend to reuse a previously imprinted red Domain PED Key.



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.

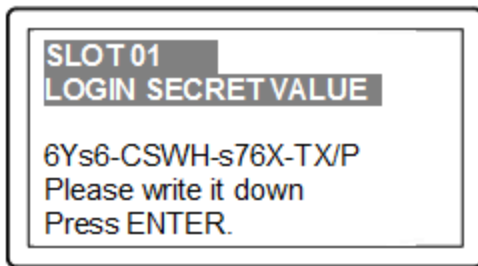
11. As it did for the black key, the PED now requests values for M and N. Again, enter 1 for each unless you wish to invoke MofN splitting of the domain secret.
12. The PED then prompts for a red Domain PED key with the message



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 1.

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:=@ABCDEFGHIJKLMNQRSTUvwxyz[]^_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:=?@ABCDEFGHIJKLMNQRSTUvwxyz[]^_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:

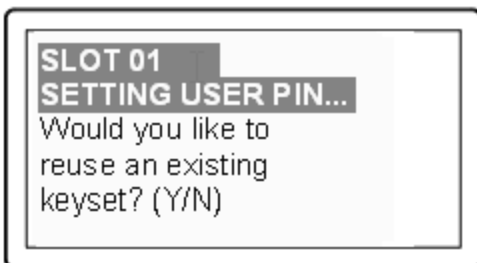
```
lunash:> partition create -partition mylegacypar1
(substitute the name of your choice for "mylegacypar1")
```

```
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.

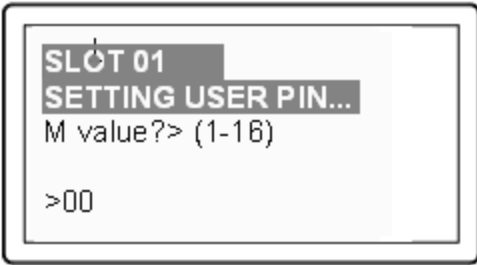


Respond "Yes" if you have a key from another HSM partition with a partition Owner ID already imprinted on it, that you wish to share/reuse.

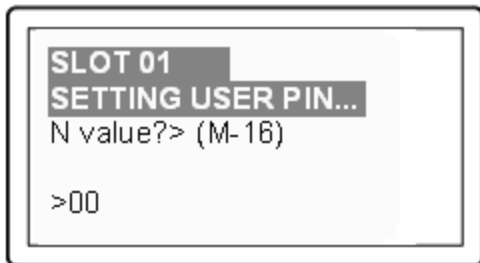
Respond "No" if you have a fresh, never-imprinted key, or if you have a key previously imprinted with an ID that you do not wish to preserve.

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

3. The PED requests values for :

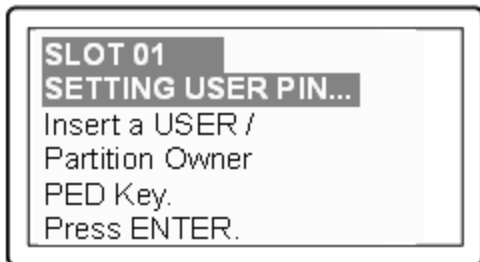


and



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

- 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.



- The PED *might* continue with:



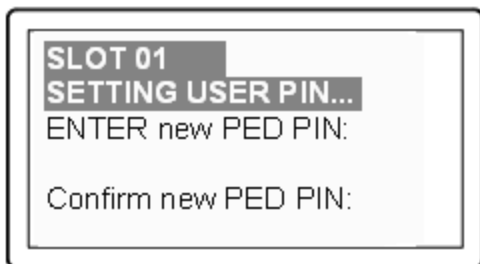
Decide whether this should be a group PED Key (see "What is a Shared or Group PED Key?"), press [YES] or [NO] on the PED keypad, and press [Enter].

- 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].

- 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).

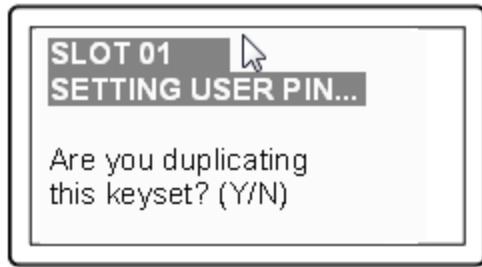


You must press [Enter] to inform the PED that you are finished entering PED PIN digits, or that you have decided not to use a PED PIN (no digits entered).

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.

- You are then prompted

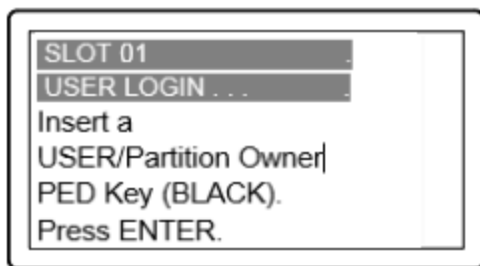


See "What is a duplicate PED Key?".

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.

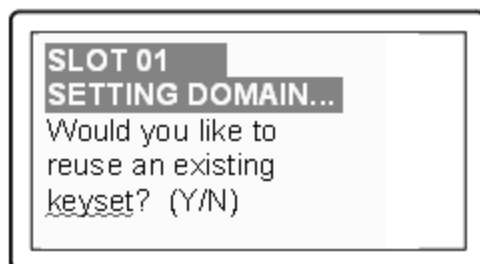
Respond "Yes", if you want the PED to imprint the first black key and then ask for more black PED Keys, until you have imprinted (duplicated) as many as you wish. After each duplicate is made, the PED asks: Would you like to make another duplicate set? Answer "Yes" until you have enough copies, and then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

- 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.

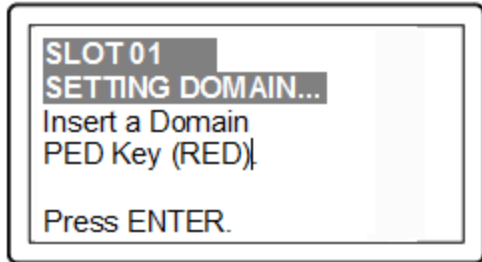
- Next, the partition's cloning domain must be set, The PED inquires if you intend to reuse a previously imprinted red Domain PED Key.



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 118 (Optional).

Otherwise, go to "[Assign a Client to an HSM Partition](#)" on page 1 .

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))
```

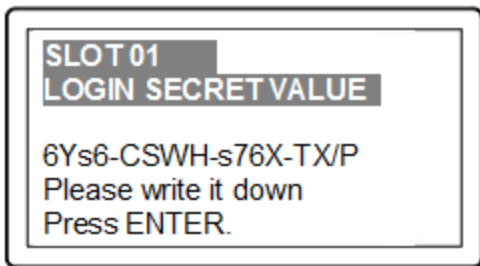
In the example above, the HSM serial number is 150718 and the partition container number is 20. Note that the partition container number is a three-digit number with leading zeros suppressed, so that the actual partition container number is 020. To determine the partition serial number concatenate the 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 118)

Otherwise, see "Creating a Network Link Between the Client and the Partition" on page 1.

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

HSM firmware version	PPSO Capability applied?	Ownership/oversight of partition (type)	Commands visible in lunacm when this HSM partition is the currently selected slot
----------------------	--------------------------	---	---

when you specify "slot" while creating a partition in lunacm, or when you specify "hasps0" 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 in the *Administration Guide*).
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 "](#) below.

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 114](#).

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](#) in the *Administration Guide*.



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:                      192.20.10.217
  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: 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 "[\[Step 6\] Create a Network Trust Link Between the Client and the Appliance](#)" on page 1.

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: 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 "[\[Step 6\] Create a Network Trust Link Between the Client and the Appliance](#)" on page 1.

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 120](#)
- ["RSA Blinding Mode" on page 121](#)



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 Trusted Link and Register Client and Appliance With Each Other

In this section, setup a network trust link (NTL) between a LunaClient and an application partition on a SafeNet Network HSM, then register each with the other, enabling applications on a client computer to access the partition.



Note: This feature is not currently supported for use with IPv6 networks.

Pre-requisites

Before using the "deploy" option, the following pre-requisite conditions must be in place:

On the SafeNet Network HSM side

- The SafeNet Network HSM's server.pem file must be available on the appliance (**sysconf regenCert** command in lunash).
- An application partition must exist on the HSM (use the **partition create** command in lunash - you did this in "[Step 5] Create Application Partitions" on page 86).

On the client side

Two files, pscp and plink (previously part of the Windows installation) are included on all platform installations to make the deploy option possible (see "[clientconfig deploy](#)" on page 1 of the *LunaCM Command Reference Guide*). Those files are 32-bit applications. For Linux 64-bit platforms only, ensure that glibc.i686 is installed.



Note: If you do not wish to install glibc.i686, you must use multi-step NTLS configuration. See "[\[Step 7\] Create a Network Trust Link Between the Client and the Appliance](#)" on page 1 in the *Appliance Administration Guide*.

To create an NTL and allow the client access to a partition:

1. On the client computer, where lunaclient is installed, launch lunacm.
2. In lunacm, run the **clientconfig deploy** command:

```
lunacm:> clientconfig deploy -server <appliance_IP> -client <client_IP/hostname> -partition <partition_name>
[-password <password>] [-user <username>]
```

Example

On the SafeNet Network HSM side

```
[SA192201730] lunash:>hsm init -label mysa30hsm

Please enter a password for the HSM Administrator:
> *****
Please re-enter password to confirm:
> *****
Please enter a cloning domain to use for initializing this HSM:
> *****
Please re-enter cloning domain to confirm:
> *****

CAUTION: Are you sure you wish to initialize this HSM?
Type 'proceed' to initialize the HSM, or 'quit'
to quit now.
> proceed
'hsm init' successful.

Command Result : 0 (Success)
[SA192201730] lunash:>hsm login

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

'hsm login' successful.

Command Result : 0 (Success)
[SA172201730] lunash:>partition create -partition mysa30leg -label mysa30leg

On completion, you will have this number of partitions: 1

Please enter a password for the partition:
> *****
Please re-enter password to confirm:
> *****
Please enter a cloning domain to use when creating this partition:
> *****
Please re-enter cloning domain to confirm:
> *****

Type 'proceed' to create the initialized partition, or
'quit' to quit now.
> proceed
'partition create' successful.

Command Result : 0 (Success)
[SA172201730] lunash:>
```

On the client side

```
lunacm:> clientconfig deploy -server 192.20.17.30 -client MyTestTower -partition mysa30leg -pass-
word pA_s$werd9
Please wait...
```

The server's host key is not cached in the registry. You have no guarantee that the server is the computer you think it is.

The server's rsa2 key fingerprint is:
ssh-rsa 2048 15:86:1d:82:d9:8f:e9:51:90:62:0d:f5:87:e5:89:a3
If you trust this host, enter "y" to add the key to PuTTY's cache and carry on connecting.
If you want to carry on connecting just once, without adding the key to the cache, enter "n".
If you do not trust this host, press Return to abandon the connection.
Store key in cache? (y/n) y
Using username "admin".
Last login: Thu Jun 9 20:39:09 2016 from 10.105.186.208

Luna SA 6.3.0 Command Line Shell - Copyright (c) 2001-2016 SafeNet, Inc. All rights reserved.

New server 192.20.17.30 successfully added to server list.

The following Luna SA Slots/Partitions were found:

Slot	Serial #	Label
====	=====	=====
0	16298193222735	mysa30leg
1	16298193222734	mysapsopar1

Command Result : No Error

lunacm:>

Next

["\[Step 8\] Configure PPSO Application Partitions" on page 125](#)

[Step 8] 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 127
PED	<ol style="list-style-type: none"> 1. "Initialize the Partition SO and Crypto Officer Roles on a PED-Auth PPSO Partition" on page 128 2. "Initialize the Crypto User Role on a PED-Auth PPSO Partition " on page 130 3. "Activate a PED-Auth PPSO Partition for the Crypto Officer Role" on page 131 or "Activate a PED-Auth PPSO Partition for the Crypto User Role" on page 133

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 1](#) 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 125.](#)

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 1](#) 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 128.

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 133.

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 9] 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 139](#)



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 log in 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 1 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*.

Confirm the HSM's Authenticity

Hardware Security Modules have traditionally been deployed in the corporate data center's most secure zone. Establishing trust with the HSM is, in part, achieved by physical access control. In cases of remote client usage (such as cloud cryptography), the client needs a way to verify the authenticity of the device protecting their most valued cryptographic keys.

Public Key Confirmations

Gemalto's SafeNet Luna HSMs include factory-issued device identities certified by a Gemalto authority. The root of this authority is maintained by Gemalto in HSMs locked in a vault with layered physical and logical access controls. These certificates are used as the root of trust for the issuance of "public key confirmations" (PKCs), certificates issued by the HSM attesting to the life cycle of a specific private key. A Luna HSM will issue confirmations only for private keys that were created by the HSM and that can never exist outside of the HSM. A valid confirmation is cryptographic proof that a specific key is inside the identified HSM. The confirmation is also proof that the identified HSM is real.

The key pair within the HSM that signs the confirmation is called a Hardware Origin Key (HOK). It is protected inside the HSM's FIPS 140-2 Level 3 security boundary. Each HOK is unique and there is no way to extract or replace it. The HOK is created in the HSM at the time of manufacture and certified by Gemalto's secure manufacturing authority, which is certified by Gemalto's root authority.

Public key confirmations are automatically generated for RSA key pairs in the HSM. A user can get a confirmation through the PKCS #11 API or the Luna **cmu** tool, and use it to verify that any RSA key is protected and has always been protected by a Luna HSM. A PKC bundle contains the following certificates:

- **MIC**: Manufacturing Integrity Certificate; corresponds to the Manufacturing Integrity Private Key (MIK), signed by the SafeNet Root.
- **HOC**: Hardware Origin Certificate; corresponds to the Hardware Origin Private Key (HOK). Unique to each HSM. Signed by MIK.
- **DAC**: Device Authentication Certificate; corresponds to the Device Authentication Private Key (DAK). Unique to each HSM. Signed by HOK.
- **PKC**: Public Key Confirmation Certificate; certificate for a private key on the HSM. Signed by DAK.

Public key confirmations are delivered as PKCS #7 files containing a certificate chain. The PKCS #7 files can be viewed using tools like OpenSSL and Microsoft's Certificates snap-in for MMC.



Note: While third-party tools are capable of cryptographically validating the certificate signature chain, they may display some certificate errors, since they do not recognize some SafeNet-specific key usage attributes included in the certificates.

Confirming the HSM's Authenticity

The **cmu** also includes a command that tests an HSM's authenticity by creating and verifying a confirmation on a temporary key created in the HSM (see "**cmu verifyhsm**" on page 1 in the *Utilities Guide*). The test includes a proof of possession that asks the HSM to sign a user-entered string as proof the associated private key is present within the target HSM.

The test requires the SafeNet root certificate, provided below:



safenet-root.pem



Note: The current certificate is valid until 2031-12-31, but it may change before this date at Gemalto's discretion. Ensure that you have the most recent version of this documentation.

To confirm the HSM's authenticity:

1. Right-click the link above and save the root certificate to the LunaClient directory.
2. Open a command line and navigate to the LunaClient directory.
3. Use the **cmu** utility to authenticate the HSM. You must specify a challenge string for the HSM to sign, and the root certificate file:

cmu verifyhsm -challenge <string> -rootcert safenet-root.pem

When prompted, specify the partition you wish to use and the Crypto Officer credential for that partition.

```
>cmu verifyhsm -challenge "1234567890" -rootcert safenet-root.pem
Select token
 [0] Token Label: mypartition-1
 [1] Token Label: mypartition-2
Enter choice: 0
Please enter password for token in slot 0 : *****
Reading rootcert from file "safenet-root.pem"... ok.
Generating temporary RSA keypair in HSM... ok.
Extracting PKC bundle from HSM... ok.
Verifying PKC certificate... ok.
Verifying DAC certificate... ok.
Verifying HOC certificate... ok.
Verifying MIC certificate... ok.
Verifying MIC against rootcert... ok.
Signing and verifying challenge... ok.
Verifying HSM serial number... ok.
Overall status: Success.
```

If this test fails, contact the HSM SO.

[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 192.20.17.174 {
    ipaddr      = 192.20.17.174
    secret      = testing123
    nas         = other
    shortname   = sa174
```

```

}
client 192.20.22.106 {
    ipaddr      = 192.20.22.106
    secret      = testing321
    nas         = other
    shortname   = sa22106
}

```

- 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.

- On the SafeNet Network HSM appliance, enable RADIUS.

```
[1722022106] lunash:>sysconf radius enable
```

Command Result : 0 (Success)

- Add the server (by hostname or IP address), specifying the port to use, and the timeout value in seconds.

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

Enter the server secret:

Re-enter the server secret:

Command Result : 0 (Success)

3. Verify that the desired server has been added.

```
[1722022106] lunash:>sysconf radius show
```

RADIUS for SSH is enabled with the following deployed servers:

server:port	timeout
-----	-----
192.20.15.182:1812	60

Command Result : 0 (Success)

4. Check the user list to see which users exist, are enabled on the 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:>