Luna SA

Configuration Guide

THE
DATA
PROTECTION
COMPANY

Document Information

Product Version	5.4.1
Document Part Number	007-011136-007
Release Date	04 July 2014

Revision History

Revision	Date	Reason
A	26 February 2014	Initial release.
B	17 April 2014	Updates to the SFF Backup feature.
C	04 July 2014	Solaris client support.

Trademarks

Disclaimer

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

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

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

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

CONTENTS

PREFACE About the Configuration Guide 6
Customer release notes 6
Audience 6
Document conventions 7
Notes 7
Cautions 7
Warnings 7
Command syntax and typeface conventions 7
Support Contacts 8

CHAPTER 1 Planning Your Configuration 10
Roles 10
Named Administrative Users and Their Assigned Roles 10
Implications of Backup and Restore of User Profiles 11
Security of Shell User Accounts 12
Crypto Officer & Crypto User 12
How the Roles are Invoked 14
Bad Login Attempts 15
Domain Planning 15
Luna PED Planning 16
What each PED prompt means 16
HSM Initialization and the Blue SO PED Key 17
HSM Cloning Domain and the Red Domain PED Key 18
Partition Owner/User and the black PED Key 18
Remote PED Orange PED Key (RPK) 19
Auditor 19
Secure Recovery Purple PED Key (SRK) 20
Other Considerations 20
Luna PED Planning 20
What each PED prompt means 21
HSM Initialization and the Blue SO PED Key 22
HSM Cloning Domain and the Red Domain PED Key 23
Partition Owner/User and the black PED Key 23
Remote PED Orange PED Key (RPK) 24
Auditor 24
Secure Recovery Purple PED Key (SRK) 24
Other Considerations 25

CHAPTER 2 Configure the Luna Appliance for your Network 26
Gather appliance network setting information 26
Client Requirements 26
Recommended Network Characteristics 27
Power-up the HSM Appliance 27

Open a Connection 30
First Login & Changing Password 31
Set System Date and Time 33
Configure IP and Network Parameters 35
Make Your Network Connection 37
Generate a New HSM Server Certificate 39

CHAPTER 3 HSM Initialization 42

Initializing a Password-Authenticated HSM 44
Initializing a Password Authenticated HSM 44
Initializing a PED-Authenticated HSM 46
Recover the SRK 46
Re-split[see 'resplit'] the SRK 48
Other Uses of the SRK 48
Initializing a PED-Authenticated HSM 48
Preparing to Initialize a Luna SA HSM [PED-version] 49
Why Initialize? 50
Start a Serial Terminal or SSH session 51
Initialize the HSM 51
Initialization - some additional options and description 62

CHAPTER 4 HSM Capabilities and Policies 67

Set HSM Policies (Password Authentication) 67
Set HSM Policies - PED (Trusted Path) Authentication 69

CHAPTER 5 Creating a Partition on the HSM 72

Prepare to Create a Partition (Password Authenticated) 72
About HSM Partitions on the Initialized HSM 72
Create the Partition [PW] 73
Partition creation audit log entry 74
Next steps 74
Prepare to Create a Partition (PED Authenticated) 75
About HSM Partitions on the Initialized HSM 75
Create (Initialize) the Partition - PED Authenticated 76
Partition creation audit log entry 84
Record the Partition Client Password (PED-Auth HSMs) 85

CHAPTER 6 Partition Policies 88

Set Partition Policy 89
Policy setting example, Luna HSM with Password Authentication 90
Policy setting example, Luna HSM with PED Authentication 90

CHAPTER 7 Prepare the Client for Network Trust Link 91

Preparing the Client 91
Import a Server Cert 92
Prepare a Network Trust Link - Windows 93
Import HSM Appliance Server Certificate onto Client (Windows) 93
Register the HSM Server Certificate with the Client (Windows) 95

Create a Client Certificate (Windows) 96
Export a Client Cert to an HSM Appliance (Windows) 99
Prepare a Network Trust Link - UNIX/Linux 102
Import HSM Appliance Server Certificate onto Client (UNIX) 102
Register the HSM Server Certificate with the Client (UNIX) 102
Register 103
Create a Client Certificate (UNIX) 103
Export a Client Cert to an HSM Appliance (UNIX) 104
Register the Client Certificate to an HSM Server 105
How Many Clients? 106
Register VM Clients 106
What's the Next Step? 106

CHAPTER 8 Assign a Client to an HSM Partition 107

Assign a Client to a Partition 107
Verify Your Setup 107
Client Connection Limits 108
Applications and Integrations 108

CHAPTER 9 Optional Configuration Tasks 109

PREFACE
About the Configuration Guide

This document provides step-by-step instructions for configuring your Luna 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 109.

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

1. "Planning Your Configuration" on page 10
2. "Configure the Luna Appliance for your Network" on page 26
3. "HSM Initialization" on page 42
4. "HSM Capabilities and Policies" on page 67
5. "Creating a Partition on the HSM" on page 72
6. "Partition Policies" on page 88
7. "Prepare the Client for Network Trust Link" on page 91
8. "Assign a Client to an HSM Partition" on page 107
9. "Optional Configuration Tasks" on page 109

This preface also includes the following information about this document:

- "Customer release notes" on page 6
- "Audience" on page 6
- "Document conventions" on page 7
- "Support Contacts" on page 8

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/crn_luna_hsm_5-4.pdf

Audience

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

All products manufactured and distributed by SafeNet, Inc. are designed to be installed, operated, and maintained by personnel who have the knowledge, training, and qualifications required to safely perform the tasks assigned to them.

The information, processes, and procedures contained in this document are intended for use by trained and qualified personnel only.

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

Document conventions

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

Notes

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

Note: Take note. Contains important or helpful information.

Cautions

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

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

Warnings

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

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

Command syntax and typeface conventions

Format	Convention
bold	The bold attribute is used to indicate the following: • Command-line commands and options (Type dir /p.) • Button names (Click Save As.) • Check box and radio button names (Select the Print Duplex check box.) • Dialog box titles (On the Protect Document dialog box, click Yes.) • Field names (User Name: Enter the name of the user.) • Menu names (On the File menu, click Save.) (Click Menu > Go To > Folders.) • User input (In the Date box, type April 1.)

Format	Convention
italics	In type, the italic attribute is used for emphasis or to indicate a related document. (See the *Installation Guide* for more information.)
<variable>	In command descriptions, angle brackets represent variables. You must substitute a value for command line arguments that are enclosed in angle brackets.
[**optional**] [<optional>]	Represent optional **keywords** or <variables> in a command line description. Optionally enter the keyword or <variable> that is enclosed in square brackets, if it is necessary or desirable to complete the task.

{**a**|**b**|**c**}
{<a>|<b>|<c>}
	Represent required alternate **keywords** or <variables> in a command line description. You must choose one command line argument enclosed within the braces. Choices are separated by vertical (OR) bars.

[**a**|**b**|**c**] [<a>|<b>|<c>]	Represent optional alternate keywords or variables in a command line description. Choose one command line argument enclosed within the braces, if desired. Choices are separated by vertical (OR) bars.

Support Contacts

If you encounter a problem while installing, registering or operating this product, please ensure that you have read the documentation. If you cannot resolve the issue, please contact your supplier or SafeNet support. SafeNet support operates 24 hours a day, 7 days a week. Your level of access to this service is governed by the support plan arrangements made between SafeNet and your organization. Please consult this support plan for further information about your entitlements, including the hours when telephone support is available to you.

Table 1: Technical support contacts

Contact method	Contact	
Address	SafeNet, Inc. 4690 Millennium Drive Belcamp, Maryland 21017 USA	
Phone	United States	(800) 545-6608, (410) 931-7520
	Australia and New Zealand	+1 410-931-7520
	China	(86) 10 8851 9191
	France	0825 341000
	Germany	01803 7246269
	India	+1 410-931-7520
	United Kingdom	0870 7529200, +1 410-931-7520
Web	www.safenet-inc.com	
Support and Downloads	www.safenet-inc.com/support	

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

CHAPTER 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:

- "Roles" on page 10
- "Crypto Officer & Crypto User" on page 12
- "Domain Planning" on page 15
- "Luna PED Considerations" on page 1
- "Luna PED Planning" on page 20

Roles

Luna HSM products offer multiple identities, some mandatory, some optional, that you can invoke in different ways to map to roles and functions in your organization. The following topics offer some aspects that you might wish to consider before committing to an HSM configuration.

Named Administrative Users and Their Assigned Roles

By default, the appliance has

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

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

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

Thus, you could choose to have:

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

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

abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789-._

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

Abilities or Privileges of Created Users

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

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

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

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

Why Create Extra Administrative Users?

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

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

```
Apr 13 14:17:15 172 -lunash: Command: syslog tail : john : 172.20.10.133/3107
Command Result : 0 (Success)
```

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

You might find other uses. Please let us know.

Implications of Backup and Restore of User Profiles

The commands "sysconf config backup" and "sysconf config restore" allow you to store a snapshot of the administrative user database (the names and status of all named Luna Shell users) that can later be restored if desired.

⚠ **CAUTION:**
Restoring from backup restores the database of user profiles that existed before the backup was made. This includes:
- the set of users that existed when the backup was made
- the passwords that users had at the time of the backup
- the enabled/disabled status of users, at the time of the backup.

This means that:
- you will lose any user accounts created since the backup,
- passwords of existing users could be reverted without their knowledge,
- enabled users might be disabled (therefor unable to perform their tasks)
- disabled users might be enabled (therefore re-granted access that was suspended) and
- any user accounts removed since that backup will be restored.

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

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

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

Security of Shell User Accounts

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

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

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 Luna HSM follows the standard Cryptoki model:

- **appliance admin**

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

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

  The appliance "admin" performs network administration and some other functions that do not require the additional authentication. Therefore, by controlling access to passwords (for a Luna HSM with Password Authentication) or to PED Keys (for a Luna 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 Luna 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 Luna HSM with Password Authentication) or the HSM Admin (blue) PED Key (for a Luna HSM with Trusted Path Authentication) can:

  - create and delete Partitions,
  - create and delete Partition Owners (black PED Key holders on a Luna 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 Luna 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 Luna HSM with Trusted Path Authentication) can:

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

Note: Both a Luna HSM with Password Authentication and a Luna 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: **Luna HSM with PED (Trusted Path) Authentication**, splits the Partition access into two layers. The HSM Partition Owner (a concept that exists only for a Luna 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 Luna PED when the Partition is created).

Note: For **Luna 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 Luna Shell (lunash) as admin.

- **Client**

  A Client is a "working" or "production" user of one or more Luna SA HSM Partitions, that connects from a client computer (one that has set up NTLS by exchanging certificates and registering with the Luna SA). 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 Luna SA 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 Luna SA 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 Luna SA 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 Luna PED, similar to the Crypto Officer or Partition Owner Password that is generated on the Luna 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 Luna 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

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.

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 Luna HSMs.

- The HSM SO-space domain can be created at the HSM (therefore unique) at HSM init time, or it can be imported, meaning that it is shared with one-or-more other HSMs.
- The HSM partition domain can be created at the HSM (therefore unique) at partition creation time, or it can be imported, meaning that it is shared with one-or-more other HSM partitions.
- The partition domain can be the same as the HSM SO domain or different.
- The partition domain can be the same as the domain of another partition on the same HSM (for HSMs that support multiple partitions) or different.

For PED authenticated HSMs, the domain secret for the SO space or for a 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 Luna 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 Partitions.

Luna 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.

M of N - 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 M of N by providing the M value and the N value using the PED Keypad, when prompted. You refuse M of N by setting the M value and the N value both to "1". M of N 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 M of N 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 M of N sets, per role, if you chose to invoke the M of N 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 Luna 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 Luna PED (which must be connected, as described in the Luna 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 M of N 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 M of N 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.

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 Luna 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 M of N, 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 Luna 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 M of N, 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 M of N), 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 M of N, 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.

Luna 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.

M of N - 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 M of N by providing the M value and the N value using the PED Keypad, when prompted. You refuse M of N by setting the M value and the N value both to "1". M of N 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 M of N 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 M of N sets, per role, if you chose to invoke the M of N 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 Luna 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 Luna PED (which must be connected, as described in the Luna 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 M of N 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 M of N 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.

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 Luna 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 M of N, 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 Luna 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 M of N, 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 M of N), 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 M of N, 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.

CHAPTER 2

Configure the Luna Appliance for your Network

In this section, gather information and apply appropriate settings to replace factory default values, and have your Luna SA appliance recognized on your network.

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)
- 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 LunaClient Software, and is installed in c:\Program Files\SafeNet\LunaClient\putty.exe.
  The pscp utility is also included in LunaClient Software installer, and is required for this installation.

Go to "Recommended Network Characteristics" on page 27

Recommended Network Characteristics

Determine whether your network is configured optimally for use of Luna 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 Luna 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 Luna 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

Luna appliance client-server communication uses timeouts less than 30 seconds to determine failure scenarios. Thus the appliance does not tolerate network configurations or conditions that introduce a greater delay - problems can result, especially with 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 Luna appliance and a switch, and then reconnect, traffic should resume immediately, but with certain network switch configurations it might take 30 seconds for traffic to resume.

The problem here is at the switch (and not the Luna 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" on page 27 .

Power-up the HSM Appliance

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

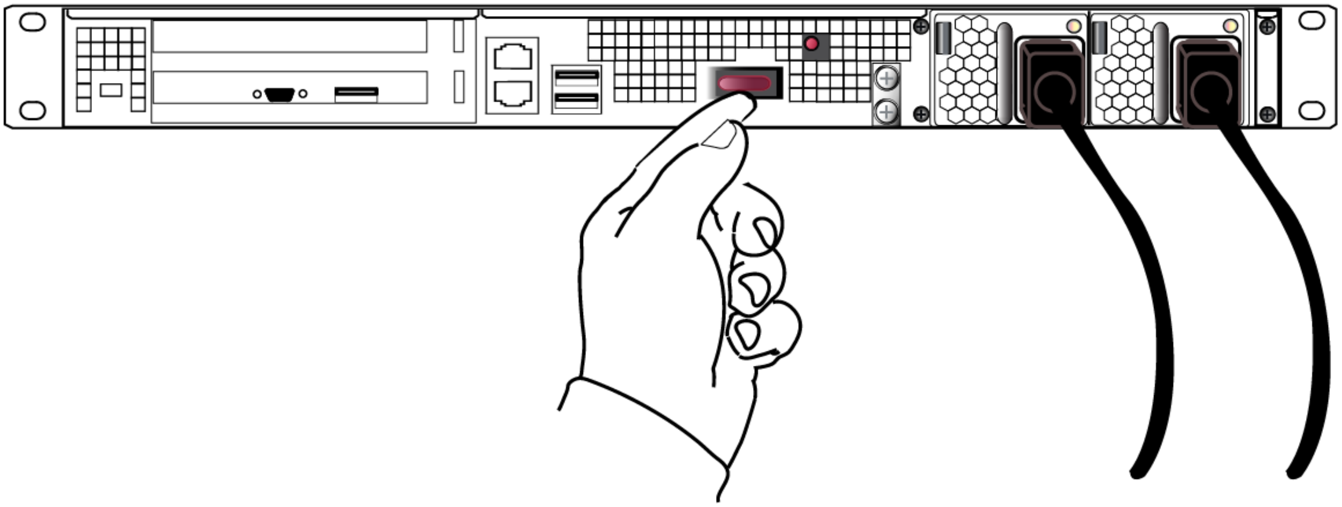
- **power connections** [We suggest that each of the two power supplies be connected to an independent electrical source, and that at least one of those sources should be protected by UPS (uninterruptible power supply) and generator backup.],

- **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 Luna Appliance

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



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

⏻

If the appliance was deliberately powered down, using the START/STOP switch or the "poweroff" command, then it should remain off until you press the START/STOP switch. However, if power was removed while the system was on (either a power failure, or the power cable was disconnected - not good practice), then the system should restart without a button press. This behavior allows unattended resumption of activity after power interruption. [In most cases, it is assumed that this would never be needed, as you would install the appliance with its two power supplies connected to two completely separate, independent power sources, at least one of which would be battery-backed (uninterruptible power supply) and/or generator-backed.]

🖧

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.

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

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

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

Next, see "Open a Connection" on page 30.

Open a Connection

Perform your initial configuration via direct serial connection to the Luna 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 Luna 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 Luna SA 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:&gt; 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 & Changing Password" on page 31.

First Login & Changing Password

Orientation summary

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.

This section describes the complete process of preparing your new HSM Server and one Client system for operation with your application.

- First Time Login and Changing Passwords (below, on this page)
- Verify and Set the Date and Time (next section)
- Configure HSM appliance's IP and Network Parameters (using static or DHCP, etc. - In general, we strongly recommend against using DHCP for HSM appliances.)
- Restart services, so that your configuration changes (previous step) can take effect
- Make Your Network Connection

Login now

When you have connected to the HSM Server, the onboard secure Command Line Interface (with the lunash:> prompt) is independent of the platform (Linux, 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.

```
Luna SA 5.4.0-14 [Build Time: 20131223 11:55]

Authorized Use Only
```

[localhost] ttyS0 login: admin

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

```
Changing password for admin
(current) UNIX password:

You can now choose the new password.

 A valid password should be a mix of upper and lower case letters,
digits, and other characters. You can use an 8 character long
password with characters from at least 3 of these 4 classes.
An upper case letter that begins the password and a digit that
ends it do not count towards the number of character classes used.

Enter new password:
Re-type new password:

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

Luna SA 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

```
[myluna1] 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               st         > Status
 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 System Date and Time" on page 33

Set System Date and Time

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.

Set 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 Luna SA 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 Luna SA 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.

Go to "Configure IP and Network Parameters" on page 35.

Configure IP and Network Parameters

The HSM appliance is pre-configured with network settings left over from our manufacturing process and not recommended for your production network. The following procedure assumes that your network uses DNS. If you are configuring without a DNS server available, some of the commands on this and subsequent pages might be affected. Such commands are highlighted with this “No DNS” icon.

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

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

```
[local_host] lunash:>net show
    Hostname: local_host
    Domain:           <not set>
    IP Address (eth0): HW Address (eth0): 00:15:B2:A2:43:60
    Mask (eth0):       Gateway (eth0):  <not set>

    Name Servers: <not set>
    Search Domain(s): <not set>

Kernel IP routing table
Destination Gateway Genmask Flags Metric Ref Use Iface
```

```
Link status
  eth0: Configured
        Link detected: yes
  eth1: Not configured

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

2. Use `network hostname` to set the hostname of the HSM appliance (use lowercase characters).
   ```
   lunash:> network hostname myluna3
   ```

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

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

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

3. Use `network domain` to set the name of the network domain in which the HSM Server (appliance) is to operate.
   ```
   lunash:> net domain safenet-inc.com
   ```

4. Use ‘`network dns add nameserver`’ to set the Nameserver IP Address (address for the local name server).
   ```
   lunash:> net dns add nameserver 192.168.1.3
   ```
   (substitute an appropriate address for the example; ask your Network Administrator).

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

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

5. Use `net dns add searchdomain` to set the DNS Search Domain (the search list to be used for hostname lookups).
   ```
    lunash:> net dns add searchdomain safenet-inc.com
   ```

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

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

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

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

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

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

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

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

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

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

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

View the new network settings with `network show`.

```
 lunash:> network show
```

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

(Next, go to "Make Your Network Connection" on page 37)

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.

1. Connect the ethernet cable to the upper ethernet port on the HSM appliance back panel and use ssh to open a session on the HSM appliance.
2. Login as admin.

Test Your Network Configuration

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

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

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

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

   Add servers
   lunash:> sysconf ntp addserver <hostname-OR-ipaddress>

   Activate servers
   lunash:> sysconf ntp enable

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

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

Peers:
==============================================================================
remote refid st t when poll reach delay offset jitter
==============================================================================
*LOCAL(0) .LOCL. 10 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: The return code "5 (ERROR)" indicates a gap between your system time and the NTP server's time. You can expect one of two outcomes:

- if the initial time-gap between your appliance and the server is greater than twenty minutes, the appliance gives up and never synchronizes with that server

- if the initial time-gap is less than twenty minutes, the appliance synchronizes with the server, slowly, over several minutes; this ensures that there is no sudden jump in system time which would be unwelcome in your system logging.

(When your connection is working , got to "Generate a New HSM Server Certificate" on page 39".)

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.

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

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

```
lunash:>
```

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 Luna SA 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.

Bind the Network Trust Link Service

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.

2. 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 ntls:                                             [   OK  ]
Starting ntls:                                             [   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 ntls:                                             [   OK  ]
Starting ntls:                                             [   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 ntls” operation might fail in the above example, because NTLS is not yet running on a new HSM appliance. Just ignore the message. The service starts again, whether the stop was needed or not.

If you have been following the instructions in these pages as part of setting up a new HSM appliance then the next step is to initialize the HSM on your Luna SA appliance. Those instructions can be found in the "HSM Configuration" section. Choose one of the following links, according to the type of HSM appliance that you have:

- "Initializing a Password Authenticated HSM" on page 44.
- "Initializing a PED-Authenticated HSM" on page 48.

CHAPTER 3

HSM Initialization

To initialize an HSM is to prepare it for operation, under the control of an HSM Admin.

Choose instructions for the type of HSM that you own:

- "About Initializing a Password Authenticated HSM"
- "About Initializing a PED Authenticated HSM"

Which kind do I have?

Luna SA 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 `hsm displayLicenses` command. You can run that command from the Luna shell (logged in as appliance admin). The hsm displayLicences 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 Luna SA. Look for the term **FIPS3** appearing in that list to indicate that your Luna SA is PED Authenticated (uses the Trusted Path) - otherwise, your HSM is Password Authenticated.

What if I make a mistake?

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 lunash 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 Luna 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 section of this help 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 Luna HSM, you should have passwords already determined according to your organization's security policies. For a PED Authenticated Luna HSM, you should have a Luna PED connected, and an appropriate set of PED Keys available.

If this is your only PED Authenticated Luna 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.

Initializing a Password-Authenticated HSM

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

"Initializing a Password Authenticated HSM" on page 44

Initializing a Password Authenticated HSM

Initialize the HSM , to set up the necessary identities, ownership and authentication at the HSM Server level. 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 *Lunacm Command Reference*. 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, `lunash` 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, within the HSM appliance. For proper security, it should be different than the appliance admin password, and 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.

A domain is created (new) or is imprinted (from an existing domain) when you initialize the HSM.)

Initialize a Password Authenticated HSM

Type the `hsm init` command at the lunash 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 (press <enter> to use the default domain):
> ********
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, lunash displays a “success” message.

You have initialized the HSM and created an HSM Admin 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 Admin (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 67

Initializing a PED-Authenticated HSM

In this section, you initialize the HSM portion of the Luna appliance, and set any policies that you require. In normal operation, you would perform these actions just once, when first commissioning your Luna 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 Luna SA 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 Luna SA 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 Luna HSMs and PED Keys before, please read the sub-section "Managing PED Keys" 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 Luna HSM in Secure Transport Mode, then a preliminary step is required before you can initialize; see "Recover the SRK" on page 46.

Otherwise, go directly to "Initializing a PED-Authenticated HSM" on page 48.

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 Luna 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 Luna SA powered and connected to a Luna PED, and also connected to a computer having the Luna 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 resplit[1] required: no
Hardware tampered:  no
Transport mode: yes

Command Result : No Error
lunash:>
```

Recover the srk with the command

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

Refer to the Luna 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

[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.

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[1] 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 page 48.

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

In this section, you initialize the HSM portion of the Luna appliance, and set any policies that you require. In normal operation, you would perform these actions just once, when first commissioning your Luna 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 Luna SA 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 Luna SA appliance that is not fresh from the factory, or freshly factoryReset,

[1] [see 'resplit']

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 Luna HSMs and PED Keys before, please read the sub-section "Managing PED Keys" 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 Luna SA HSM [PED-version]

The last thing that the production workers do, before placing your Luna SA 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 Luna SA 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 Luna SA 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 Domain (another PED Key), and places the HSM in a state ready to use.

Use the instructions on this page if you have Luna SA with PED (Trusted Path) authentication.

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

Start a Serial Terminal or SSH session

```
bash#: ssh 192.20.10.203
login as: admin
admin@172.20.10.202's password:________
Last login: Fri Dec  2 20:16:54 2011 from 192.17.153.225
Luna SA 5.1.0-22 Command Line Shell - Copyright (c) 2001-2011 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 Luna Shell as the HSM administrator 'admin': lunash:>
4. Run the hsm init command, giving a label for your Luna SA 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.
```

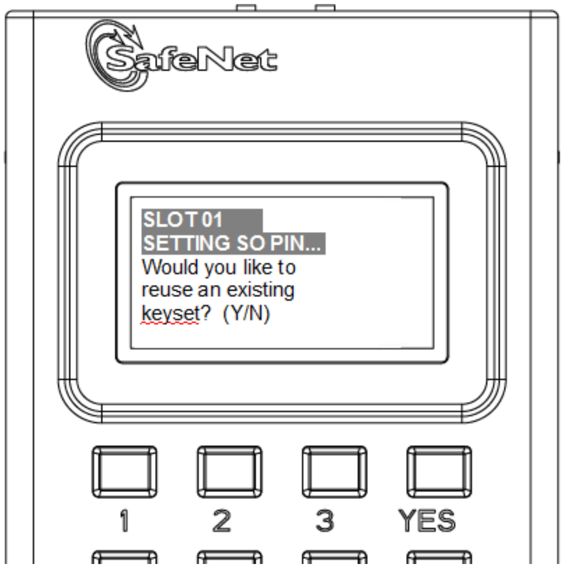
Note: Respond promptly to avoid PED timeout Error. At this time, the PED becomes active and begins prompting you for PED Keys and other responses. For security reasons, this sequence has a time-out, which is the maximum permitted duration, after which an error is generated and the process stops. If you 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 62 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.

Luna 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.

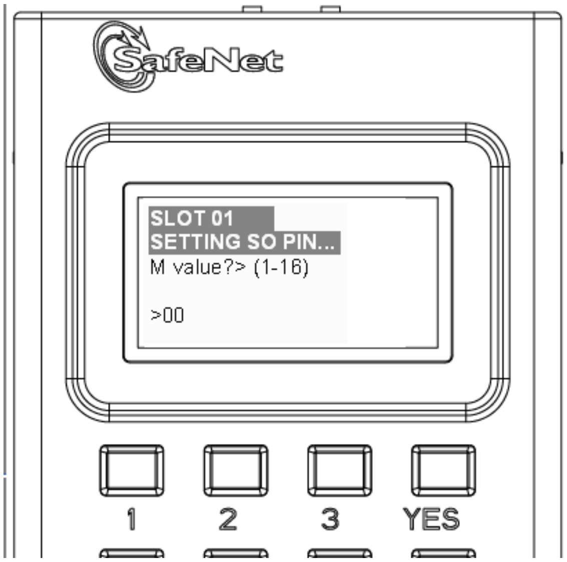
The HSM and PED need to know, prior to imprinting the first SO PED Key.



SLOT 01
SETTING SO PIN...
Would you like to
reuse an existing
keyset? (Y/N)

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, Luna PED asks you to set M of N values.

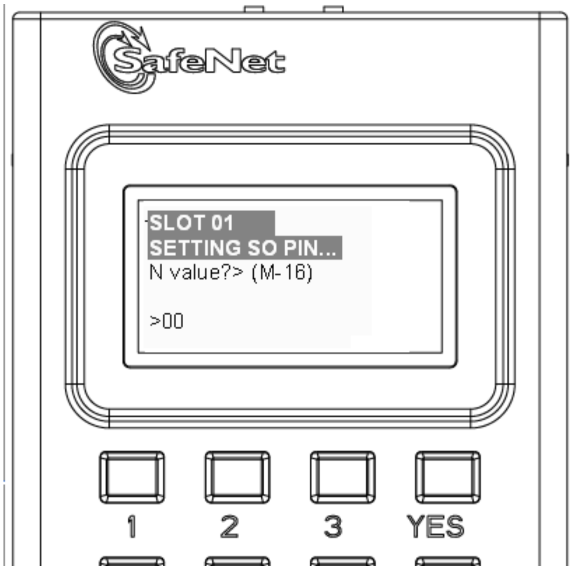
If you say [YES], you indicate that you have a PED Key (or set of PED Keys) from another HSM and you wish your current/new HSM to share the authentication with that other HSM. Authentication will be read from the PED Key that you present and imprinted onto the current HSM.



SLOT 01
SETTING SO PIN...
M value?> (1-16)

>00

and

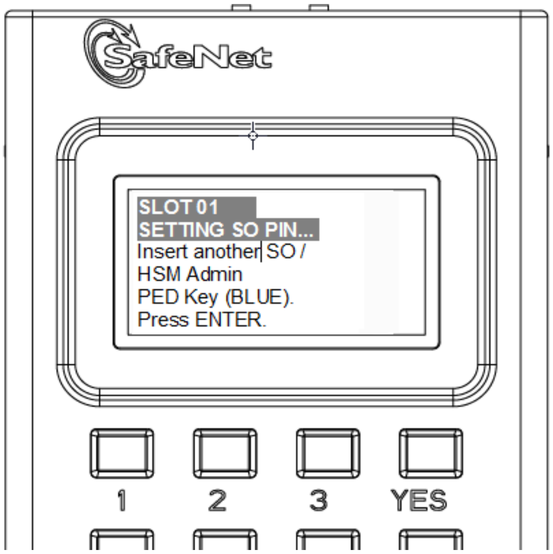


```
SLOT 01
SETTING SO PIN...
N value?> (M-16)

>00
```

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.

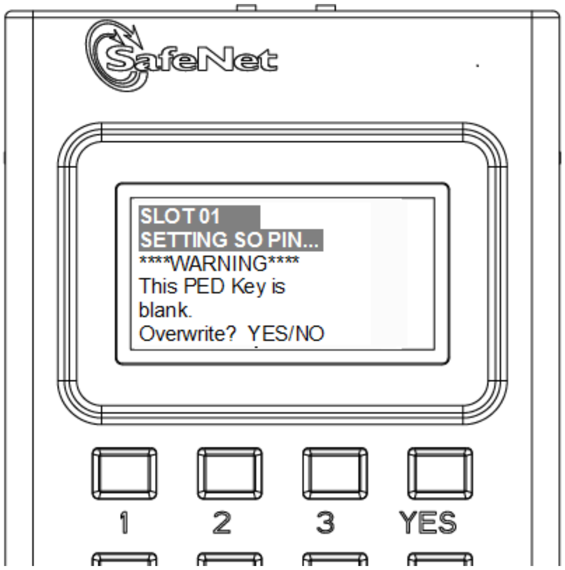
Setting M and N larger than "1" means that the authentication is split into N different "splits", of which quantity M of them must be presented each time you are required to authenticate. M of N allows you to enforce multi-person access control - no single person can access the HSM without cooperation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

Luna 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.



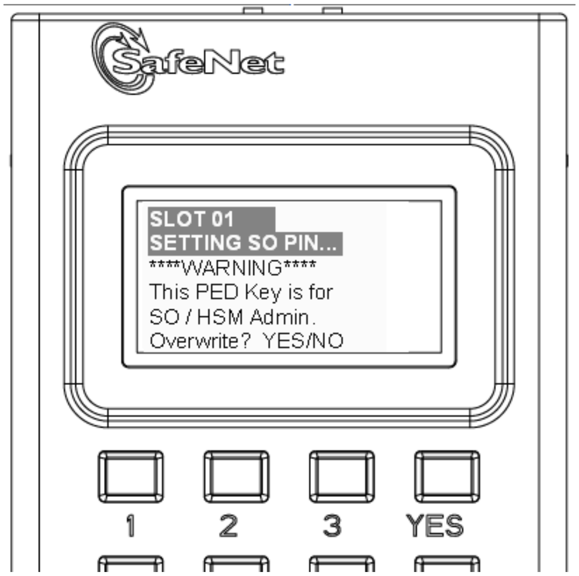
```
SLOT 01
SETTING SO PIN...
Insert another SO /
HSM Admin
PED Key (BLUE).
Press ENTER.
```

Insert a blue HSM Admin / SO PED key [of course, the PED Key is generically black - we suggest that you apply the appropriate color sticker either immediately before or immediately after imprinting] and press [Enter].



```
SLOT 01
SETTING SO PIN...
****WARNING****
This PED Key is
blank.
Overwrite? YES/NO
```

OR

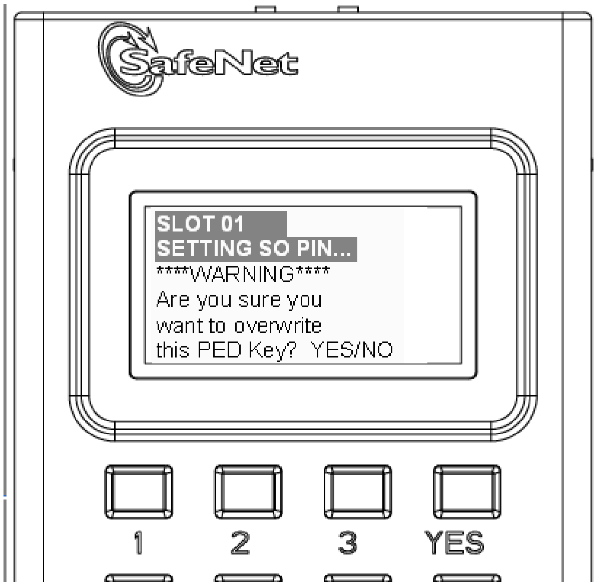


```
SLOT 01
SETTING SO PIN...
****WARNING****
This PED Key is for
SO / HSM Admin.
Overwrite? YES/NO
```

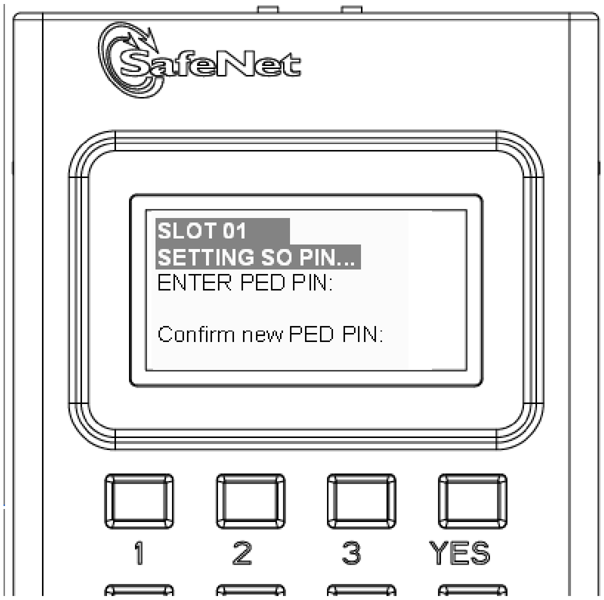
Answer (press the appropriate button on the PED keypad)

- "**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 Luna SA HSM during this initialization).

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


SLOT 01
SETTING SO PIN...
****WARNING****
Are you sure you
want to overwrite
this PED Key? YES/NO

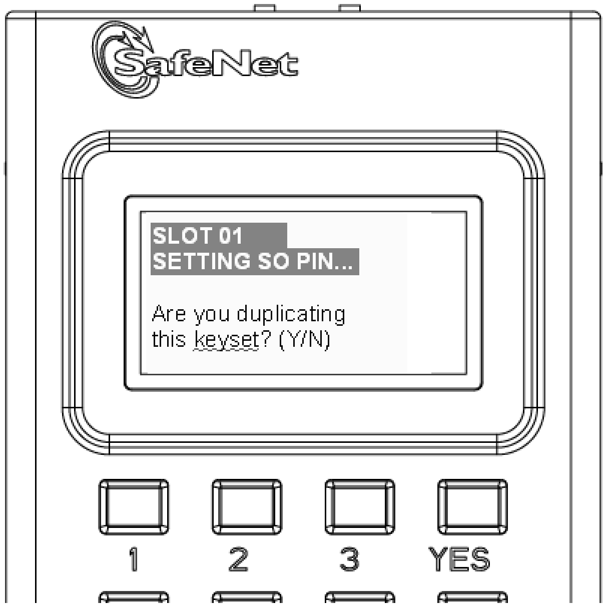
For any situation other than reusing a keyset, Luna PED now prompts for you to set a PED PIN. For multi-factor authentication security, the physical PED Key is "something you have". You can choose to associate that with "something you know", in the form of a multi-digit PIN code that must always be supplied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


SLOT 01
SETTING SO PIN...
ENTER PED PIN:

Confirm new PED PIN:

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

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

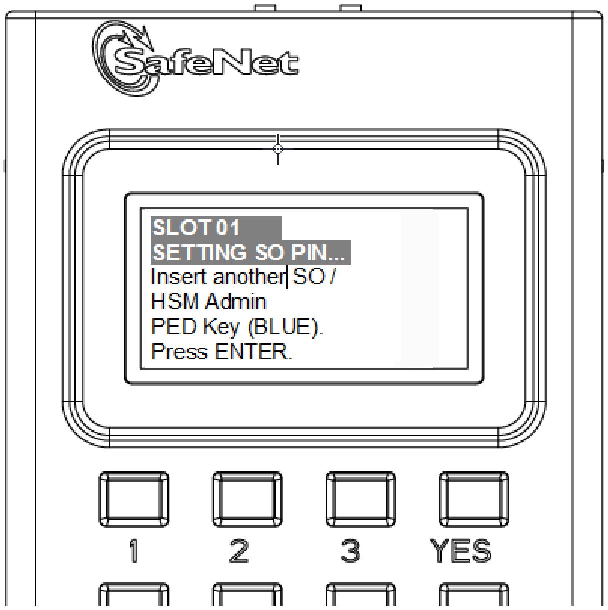


SLOT 01
SETTING SO PIN...

Are you duplicating
this keyset? (Y/N)

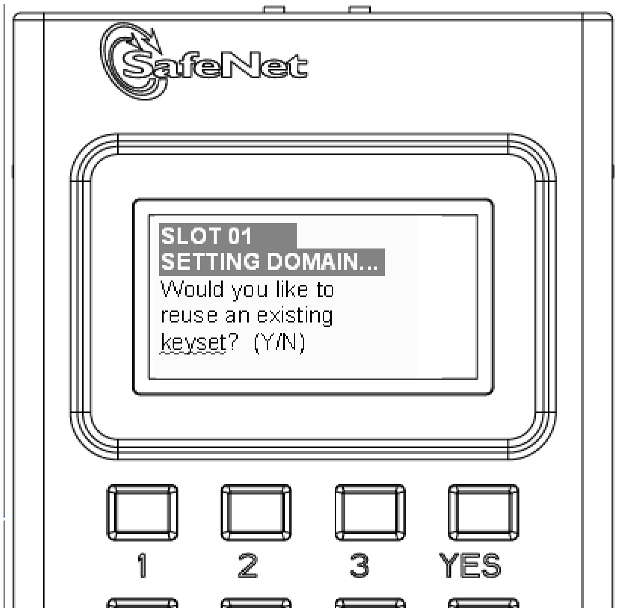
You can respond [YES] and present one or more blank keys, all of which will be imprinted with exact copies of the current PED Key's authentication, or you can say [NO], telling the PED to move on to the next part of the initialization sequence. (You should always have backups of your imprinted PED Keys,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



SLOT 01
SETTING SO PIN...
Insert another SO /
HSM Admin
PED Key (BLUE).
Press ENTER.

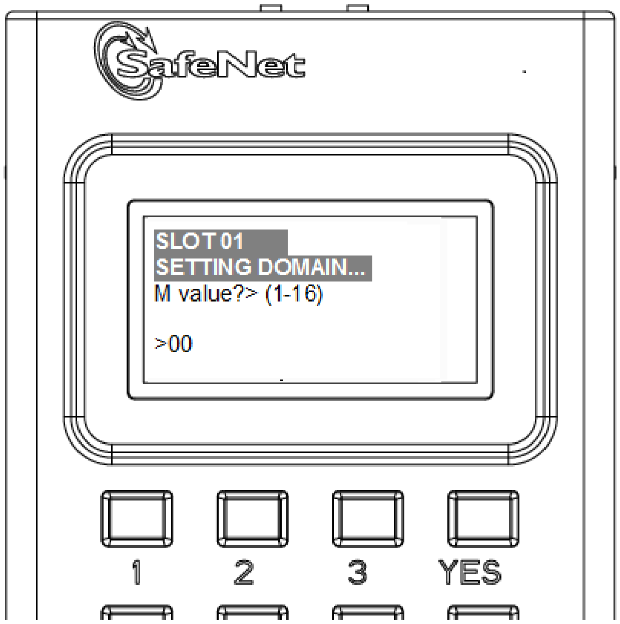
Luna PED passes the authentication along to the HSM and then asks the first question toward imprinting a cloning domain:



SLOT 01
SETTING DOMAIN...
Would you like to
reuse an existing
keyset? (Y/N)

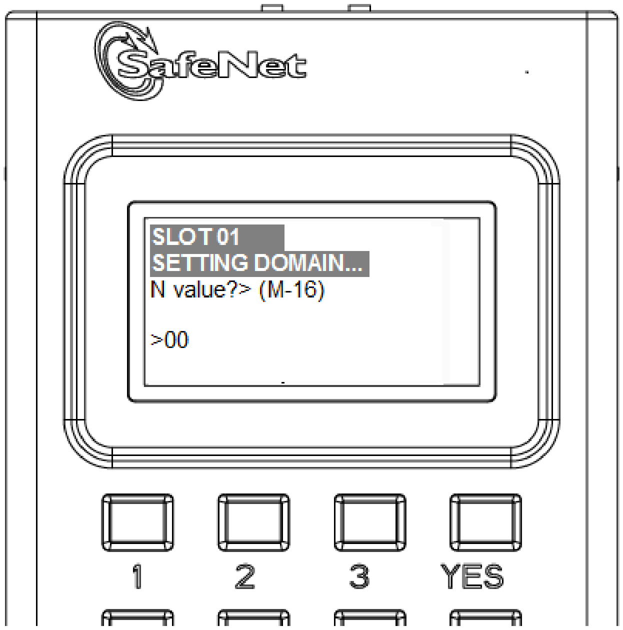
If this is your first Luna HSM, or if this HSM will not be cloning objects with other HSMs that are already initialized, then answer [NO]. Luna PED prompts for values of M and N.

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, Luna PED does not prompt for M and N.



SLOT 01
SETTING DOMAIN...
M value?> (1-16)

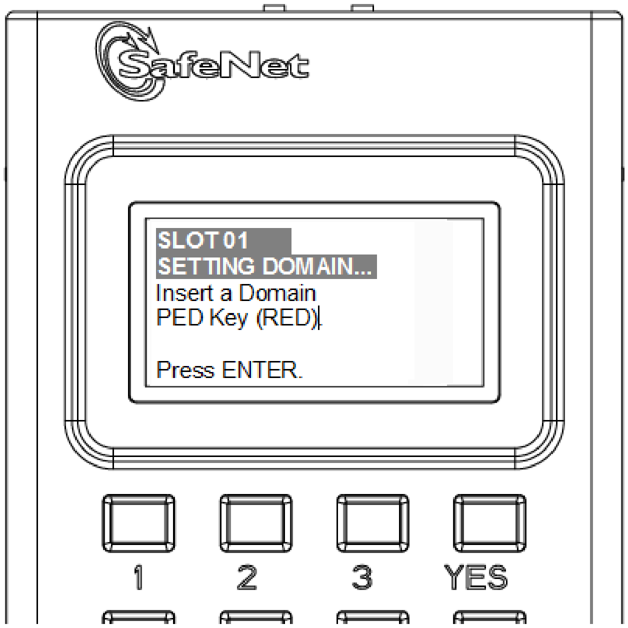
>00



SLOT 01
SETTING DOMAIN...
N value?> (M-16)

>00

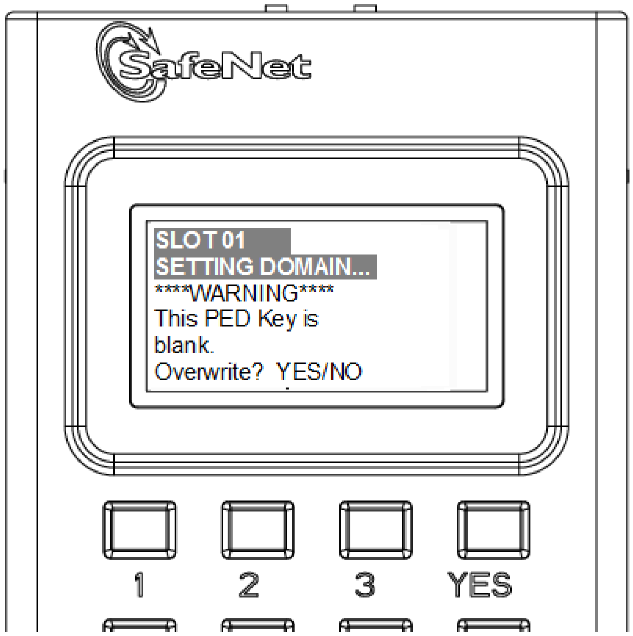
Luna PED goes through the same sequence that occurred for the blue SO PED Key, except it is now dealing with a red Domain PED Key.



SLOT 01
SETTING DOMAIN...
Insert a Domain
PED Key (RED)

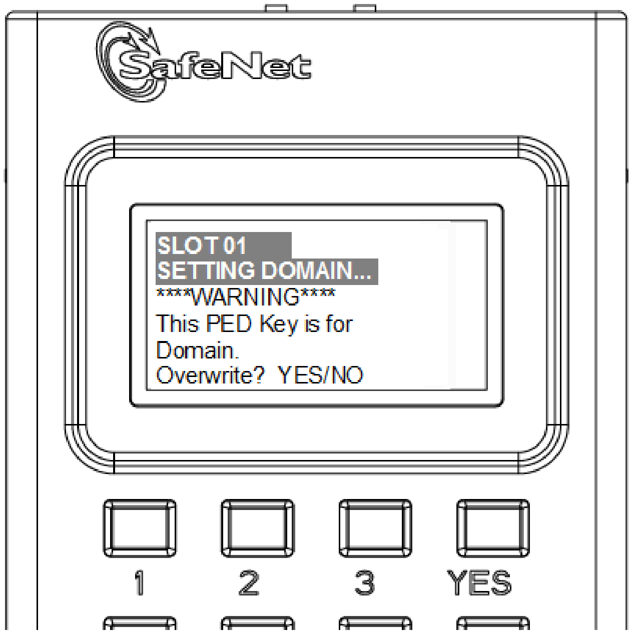
Press ENTER.

Insert a red HSM Cloning Domain PED key [of course, the PED Key is generically black - we suggest that you apply the appropriate color sticker either immediately before or immediately after imprinting] and press [Enter].



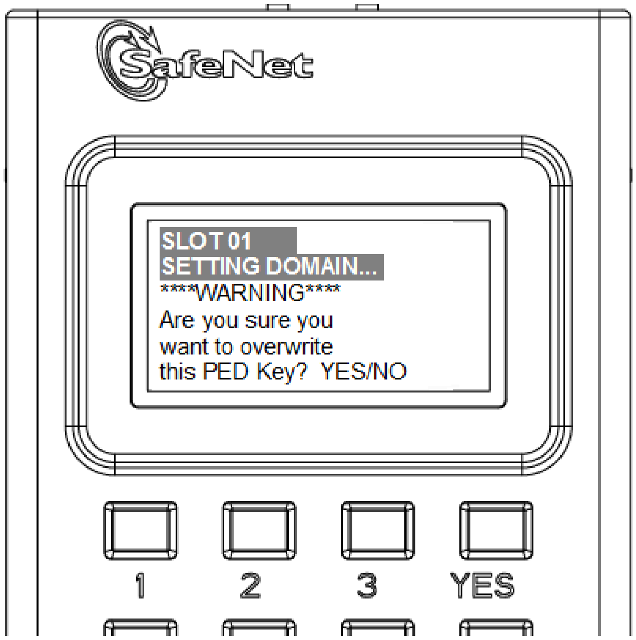
SLOT 01
SETTING DOMAIN...
****WARNING****
This PED Key is
blank.
Overwrite? YES/NO

OR



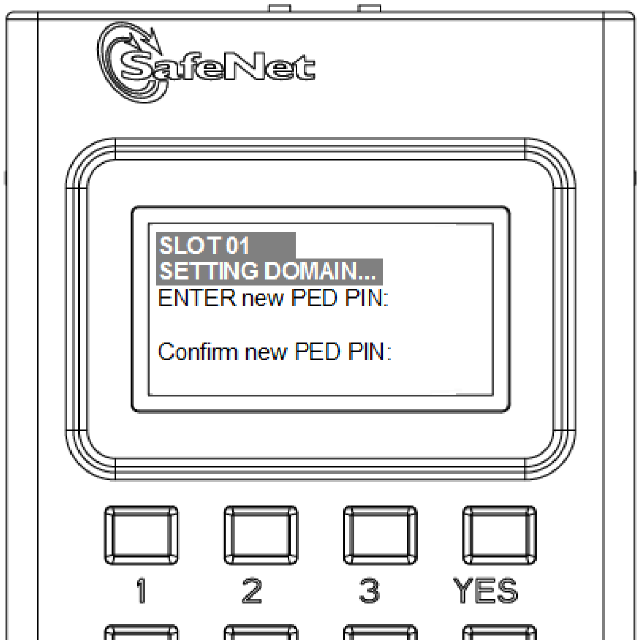
SLOT 01
SETTING DOMAIN...
****WARNING****
This PED Key is for
Domain.
Overwrite? YES/NO

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



SLOT 01
SETTING DOMAIN...
****WARNING****
Are you sure you
want to overwrite
this PED Key? YES/NO

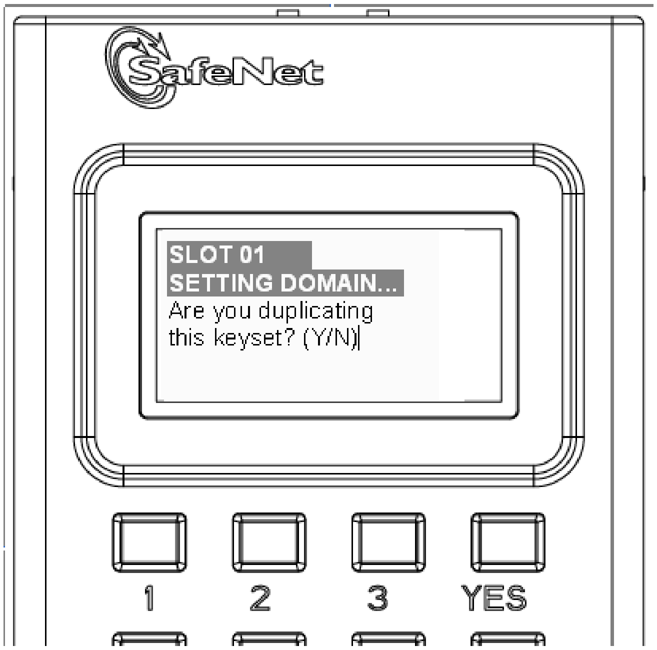
When you confirm that you do wish to overwrite whatever is (or is not) on the currently inserted key, with a Cloning Domain generated by the PED, the PED asks:



SLOT 01
SETTING DOMAIN...
ENTER new PED PIN:

Confirm new PED PIN:

And finally:



SLOT 01
SETTING DOMAIN...
Are you duplicating
this keyset? (Y/N)

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...), Luna 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.

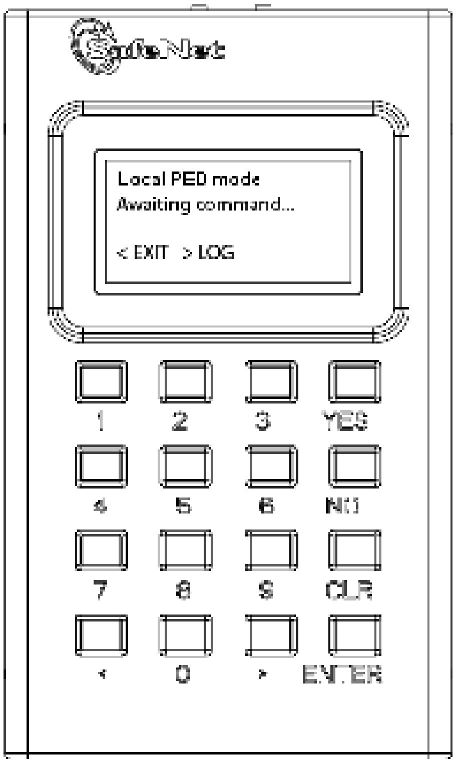
The next step is "Prepare to Create a Partition (PED Authenticated)" on page 75 on the HSM.

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 Luna HSM. So, assume that you have issued the hsm init command. The system told you to attend to the Luna PED, which you already had connected.

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

Insert the Blue PED Key



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

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

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

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

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

"Fresh" PED Keys	Pre-used PED Keys (reuse)	Pre-used PED Keys (overwrite)
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 no PED PIN (thus nothing to remember in future).	Same as in first column.	Same as in first column.
Are you duplicating this keyset? YES/NO	Are you duplicating this keyset? YES/NO	Are you duplicating this keyset? YES/NO
If you respond "YES", you can keep inserting additional blank (or old-to-be-reused) PED Keys to be imprinted with this same secret. If you say "NO", you have just the one key with that secret - don't lose it.	Same as in first column.	Same as in first column.
Login SO / HSM Admin... Insert a SO/ HSM Admin PED Key Press ENTER	Login SO / HSM Admin.. Insert a SO/ HSM Admin PED Key Press ENTER	Login SO / HSM Admin.. Insert a SO/ HSM Admin PED Key Press ENTER
Having created/imprinted the HSM Admin or SO secret, the HSM now requires you to login, in order to go further. This is a verification step.	Same as in first column.	Same as in first column.
SETTING DOMAIN... Would you like to reuse an existing keyset? (Y/N)	SETTING DOMAIN... Would you like to reuse an existing keyset? (Y/N)	SETTING DOMAIN... Would you like to reuse an existing keyset? (Y/N)

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

Table 1: PED prompt sequences

Some additional comments about some of the choices:

Provide a PED PIN (optional)

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

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

Confirm, by entering the same PIN (or nothing if you did not enter a PIN the first time), and pressing [Enter] again. (When you provide a PED PIN – even if it is the null PIN (by just pressing [Enter] with no digits) – Luna 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”, Luna 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”, Luna PED imprints the first blue key and then asks for more blue PED Keys, until you have imprinted (duplicated) as many as you require.

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

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

Creating a Cloning Domain

You create the domain for future cloning of the HSM, or you adopt the domain from a previous token or Luna HSM, so that the current Luna 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 Luna PED goes ahead and imprints a domain, which is matched on the HSM. However, if Luna PED detects that the red PED Key contains data, then Luna 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 Luna Backup HSM, so that the backup HSM will share the domain with the source Luna HSM, and so that the red Domain PED Key remains usable with the Luna 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 Luna HSM, you can :

optionally modify some of the HSM's Policy settings

or

go directly to "Creating HSM Partitions"

CHAPTER 4
HSM Capabilities and Policies

SafeNet Luna 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 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)" on page 67
- "Set HSM Policies - PED (Trusted Path) Authentication" on page 69

Set HSM Policies (Password Authentication)

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

> **Note: Capability vs Policy Interaction**
> Capabilities identify the purchased features of the product and are set at time of manufacture. Policies represent the HSM Admin’s enabling (or restriction) of those features.

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

```
[myluna] lunash:>hsm showPolicies
HSM Label:   myhsm
Serial #:    700022
Firmware:    6.21.0.
The following capabilities describe this HSM, and cannot be altered
except via firmware or capability updates.


Description                                     Value
============                                    =====
Enable PIN-based authentication                 Allowed
Enable PED-based authentication                 Disallowed
Performance level                               15
Enable domestic mechanisms & key sizes          Allowed
Enable masking                                  Allowed
Enable cloning                                  Allowed
Enable special cloning certificate              Disallowed
Enable full (non-backup) functionality          Allowed
Enable ECC mechanisms                           Allowed
Enable non-FIPS algorithms                      Allowed
Enable SO reset of partition PIN                Allowed
Enable network replication                      Allowed
Enable Korean Algorithms                        Disallowed
FIPS evaluated                                  Disallowed
Manufacturing Token                             Disallowed
Enable Remote Authentication                    Allowed
Enable forcing user PIN change                  Allowed
Enable portable masking key                     Allowed
Enable partition groups                         Disallowed
Enable Remote PED usage                         Disallowed
Enable external storage of MTK split            Disallowed
HSM non-volatile storage space                  2097152
Enable HA mode CGX                              Disallowed
Enable Acceleration                             Allowed
Enable unmasking                                Disallowed

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

Description                Value
PIN-based authentication   True

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

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


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

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

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

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

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

FIPS-validated algorithms if your application requires them.

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

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

   ```
   lunash:> hsm login
   ```

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

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

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

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

Example – Change of HSM Policy

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

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

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

If you have been following the instructions on this page as part of setting up a new HSM system, then the next step is to create virtual HSMs or HSM Partitions on the HSM that you just configured. "Prepare to Create a Partition (Password Authenticated)" on page 72

Set HSM Policies - PED (Trusted Path) Authentication

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

Note: Capability vs Policy Interaction
Capabilities identify the purchased features of the product and are set at time of manufacture. Policies represent the HSM Admin’s enabling (or restriction) of those features.

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

```
lunash:> hsm showPolicies
HSM Label:   mysa5hsm
Serial #:    700022
Firmware:    6.2.1
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                          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                        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          2097152
Enable HA mode CGX                              Disallowed
Enable Acceleration                             Allowed
Enable unmasking                                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 by 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 remote PED usage                  On      25      No
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 at FIPS 140-2 level 3, meaning that the PED and PED Keys are required for authentication, and values typed from a keyboard are ignored.

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

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

2. In order to change HSM policies, the HSM Administrator 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 Luna SA tells you so, with an error message, that you can ignore.)
   Control is passed to the PED, which prompts you for the blue PED Key.
   Insert the appropriate PED Key for this HSM, and press [ENT] on the PED keypad.

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

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

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

Example – Change of HSM Policy

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

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

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

While this is not an issue when you have just initialized an HSM, it may be a very important consideration if your HSM system has been in a “live” or “production” environment and the HSM contains useful or important data, keys, certificates.

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

Luna SA 5 does not currently have a secure identity management (SIM) configuration. Certain HSM policy settings exist to enable migration from Luna SA 4.x to Luna SA 5.x, specifically the “Enable masking” and “Enable portable masking key” values.

CHAPTER 5
Creating a Partition on the HSM

Choose the authentication method that applies to your HSM.

See "Prepare to Create a Partition (Password Authenticated)" on page 72.

See "Prepare to Create a Partition (PED Authenticated)" on page 75.

Prepare to Create a 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 Luna appliance for the first time and must now create your first HSM Partition, or
- if you have purchased a Luna 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 Luna 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 Luna appliance should already:

- have its network settings configured by "Configure the Luna Appliance for your Network" on page 26,
- have its HSM Administrator assigned by "Initializing a Password-Authenticated HSM" on page 44.

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 Luna Appliance

If you do not already have a connection open, connect your administration computer to the serial Console port of the Luna 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 Luna 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 Luna 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 the Partition [PW]" on page 73.

Create the Partition [PW]

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.

A partition name can be from 1 to 64 characters in length, and can include any of the following characters :

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

No spaces.

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 (Partition policy controls 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 birthday and other easily identifiable dates.

1. Create and name an HSM Partition. At the lunash prompt, type:

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

2. 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.

3. Write down the HSM 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 Luna HSM.

Repeat the above actions for each HSM Partition that you wish to create (to the limits of your Luna 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 entiries.

Next steps

If you have been following the instructions on these pages as part of setting up a new Luna 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 "Partition Policies" on page 88 (Optional).

Otherwise, go to "Prepare the Client for Network Trust Link" on page 91.

Prepare to Create a Partition (PED Authenticated)

This section is HSM Partition setup for PED (Trusted Path) Authentication. The activities in this section are required in these circumstances.

- if you just prepared an HSM on the HSM appliance for the first time and must now create your first HSM Partition, or
- if you have purchased a Luna SA 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 Luna SA) , 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 appliance ***should already***:

- have its network settings configured (see "Configuring the Luna Appliance Network Settings")
- have its HSM Administrator and its Cloning Domain assigned (see " Initializing a PED-Authenticated HSM" on page 46).

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 HSM Appliance

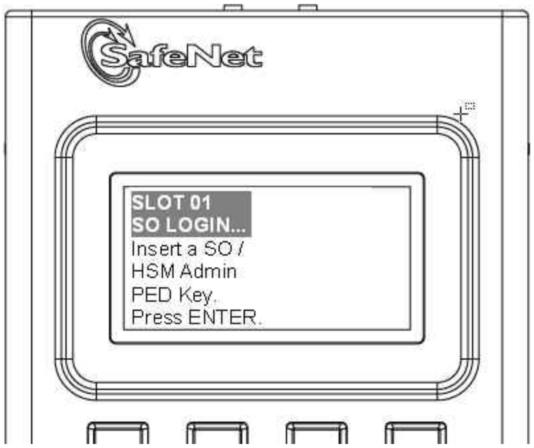
1. If you do not already have a connection open, connect your administration computer to the serial Console port of the HSM appliance, and open a Terminal session, or use ssh to connect via the network (for Windows, we provide PuTTy; for UNIX/Linux, your operating system provides the ssh client, either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

Then, Login as HSM Admin / SO

2. To create HSM Partitions, you must login to the HSM as HSM Admin (also called Security Officer or SO). Ensure that the PED is connected to the PED port on your HSM appliance, and that the PED is powered on and "Awaiting command.."
3. At the `lunash` prompt, type:

```
lunash:> hsm login
```

4. Authenticate as HSM Admin:
   The PED prompts for the blue PED Key



SLOT 01
SO LOGIN...
Insert a SO /
HSM Admin
PED Key.
Press ENTER.

You must 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.

5. Next, see "Create (Initialize) the Partition - PED Authenticated" on page 76 .

WARNING! If you fail three consecutive login attempts as HSM Admin (also called SO), the HSM is zeroized and cannot be used — it must be re-initialized. Re-initializing zeroizes the HSM contents. Zeroizing destroys all key encryption material. Please note that the HSM must actually receive some information before it logs a failed attempt, so if you forget to insert a PED Key, or if you insert the wrong kind (for example, if you insert a black key when a red key is called for), 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 (or SO), perform an ‘`hsm logout`’, then log in again.

Create (Initialize) the Partition - PED Authenticated

Having logged in, 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.)

A partition name can be from 1 to 64 characters in length, and can include any of the following characters :

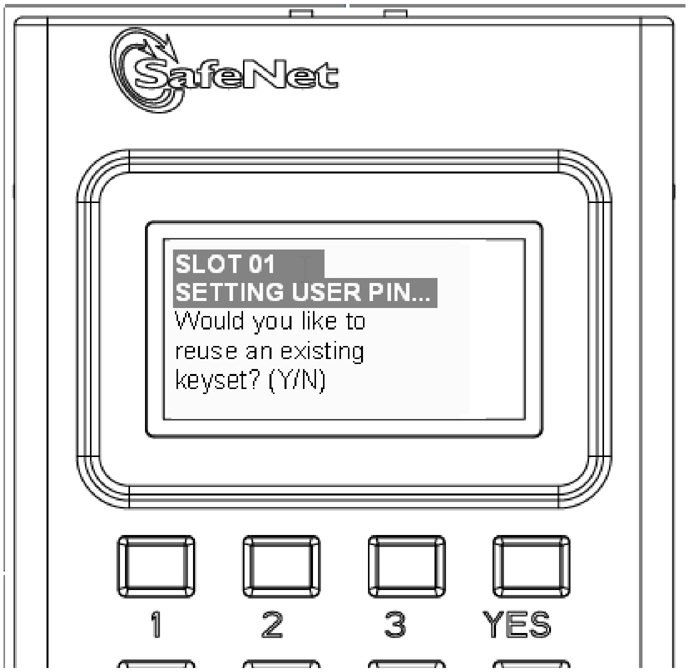
!#$%'()*+,-./0123456789:=@ABCDEFGHIJKLMNOPQRSTUVWXYZ[]^_abcdefghijklmnopqrstuvwxyz{}~

No spaces.

1. Create and name an HSM 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 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.
```

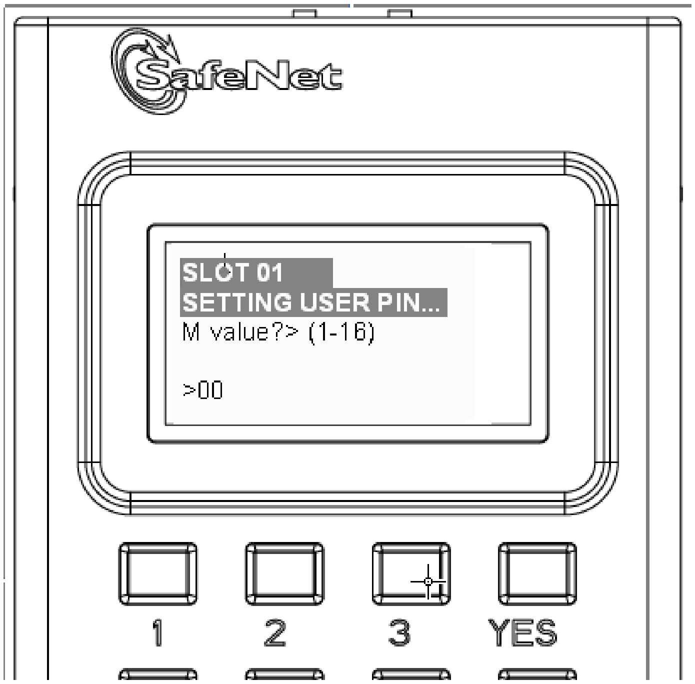
2. The PED inquires if you intend to reuse a pre-existing imprinted black PED Key.



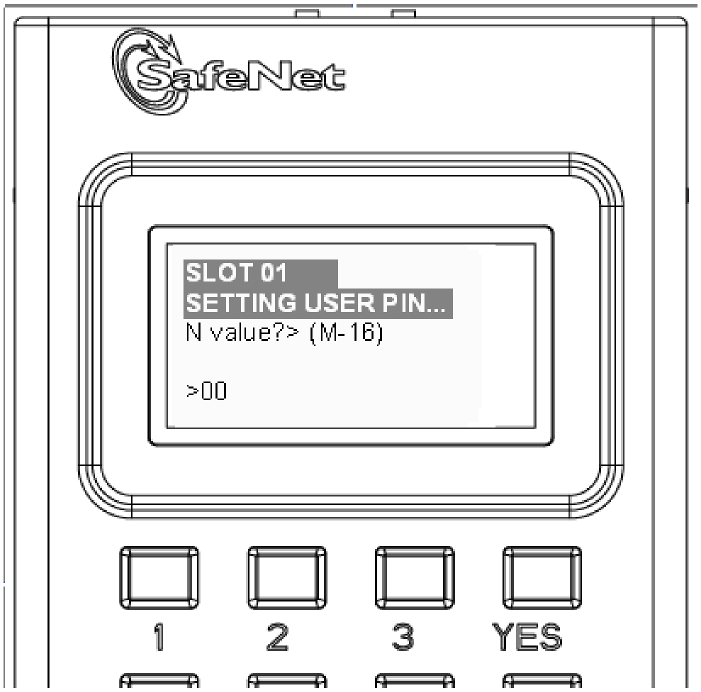
SLOT 01
SETTING USER PIN...
Would you like to
reuse an existing
keyset? (Y/N)

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.

3. The PED requests values for :

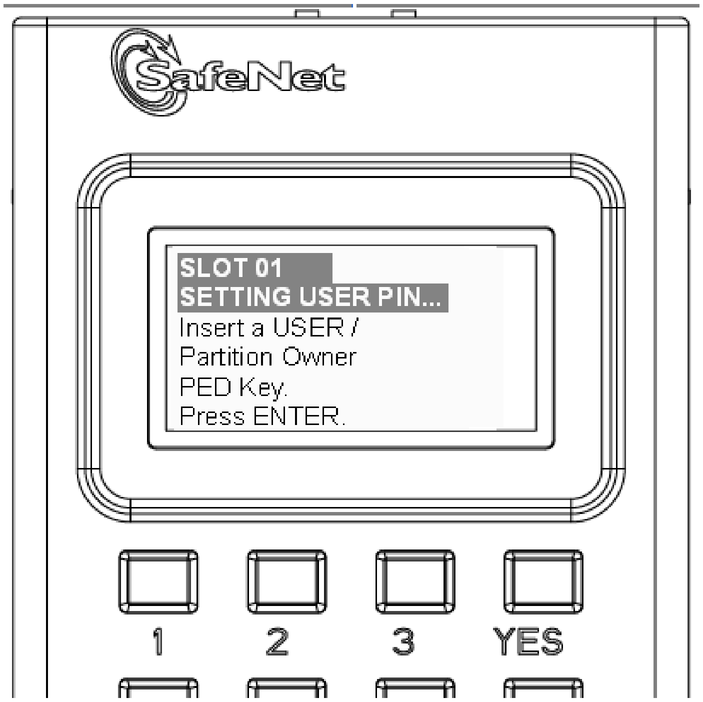


and



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

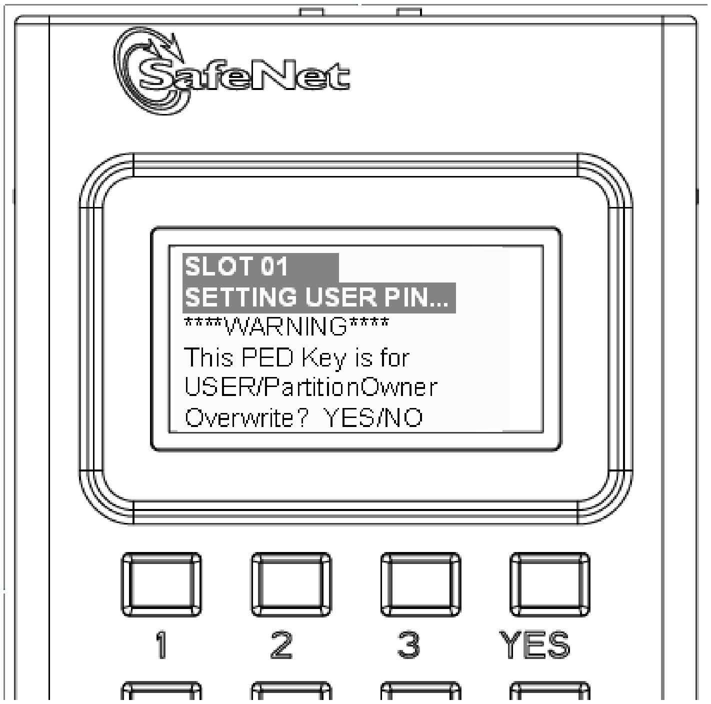
4. The PED then demands the black Owner PED key with the message



SLOT 01
SETTING USER PIN...
Insert a USER /
Partition Owner
PED Key.
Press ENTER.

Insert the black HSM Partition Owner PED key [of course, the PED Key is generically black - we suggest that you apply the appropriate color sticker either immediately before or immediately after imprinting] and press [Enter].. A unique Partition Owner PIN is to be imprinted on both the PED key and the HSM Partition.

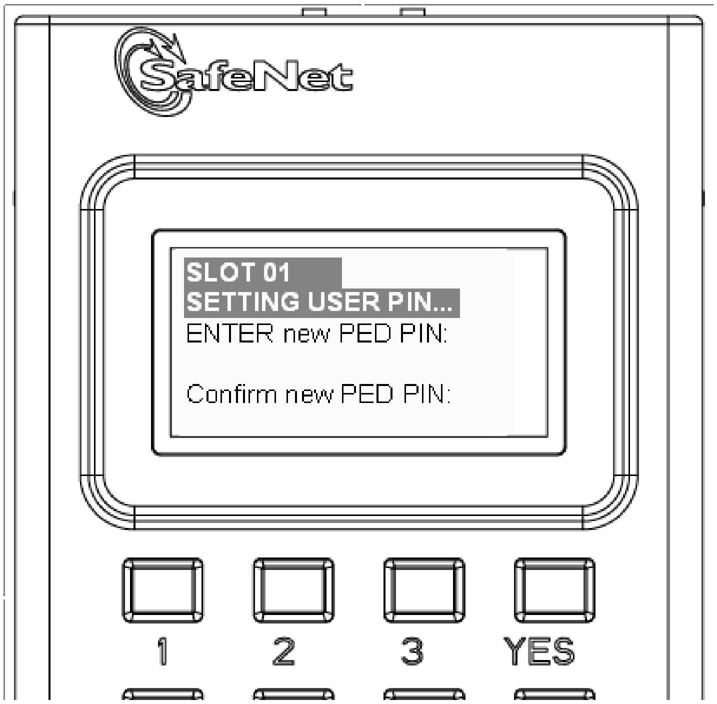
5. The PED *might* continue with:



SLOT 01
SETTING USER PIN...
****WARNING****
This PED Key is for
USER/PartitionOwner
Overwrite? YES/NO

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

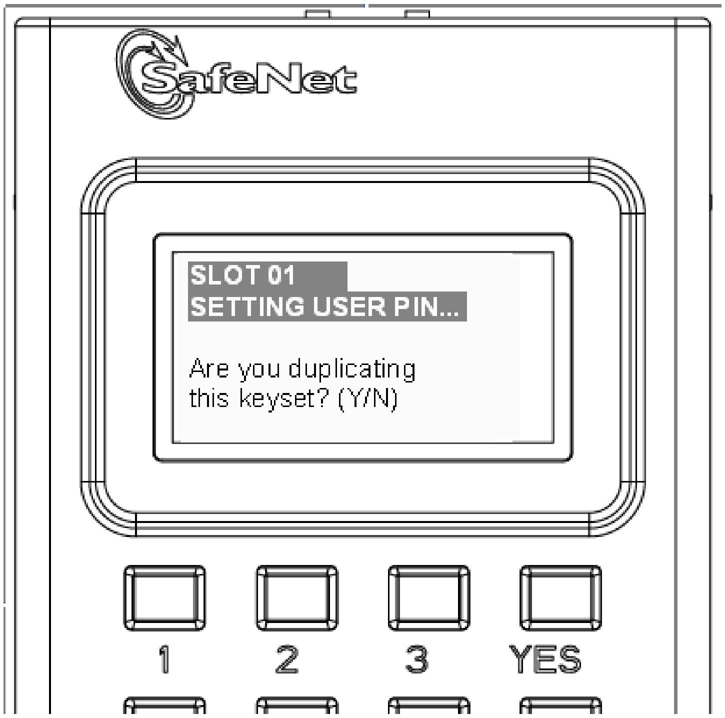
6. Next, you are asked to provide a PED PIN (optional, see "What is a PED PIN?" — can be 4-to-48 digits, or can be *no* digits if a PED PIN is not desired).



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.

Press [ENTER] again.

7. You are then prompted



SLOT 01
SETTING USER PIN...

Are you duplicating
this keyset? (Y/N)

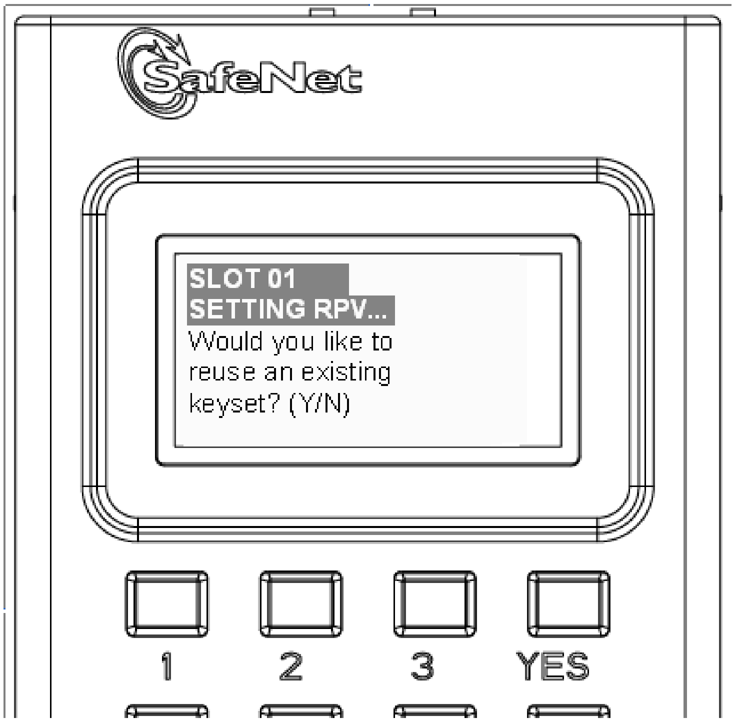
See "What is a duplicate PED Key?".
Respond “No”, if you want the PED to imprint just the one black HSM Admin PED Key and go on to the next step in creation of the HSM Partition.
Respond “Yes”, if you want the PED to imprint the first black key and then ask for more black PED Keys, until you have imprinted (duplicated) as many as you wish.

8. 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 Luna PED.

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

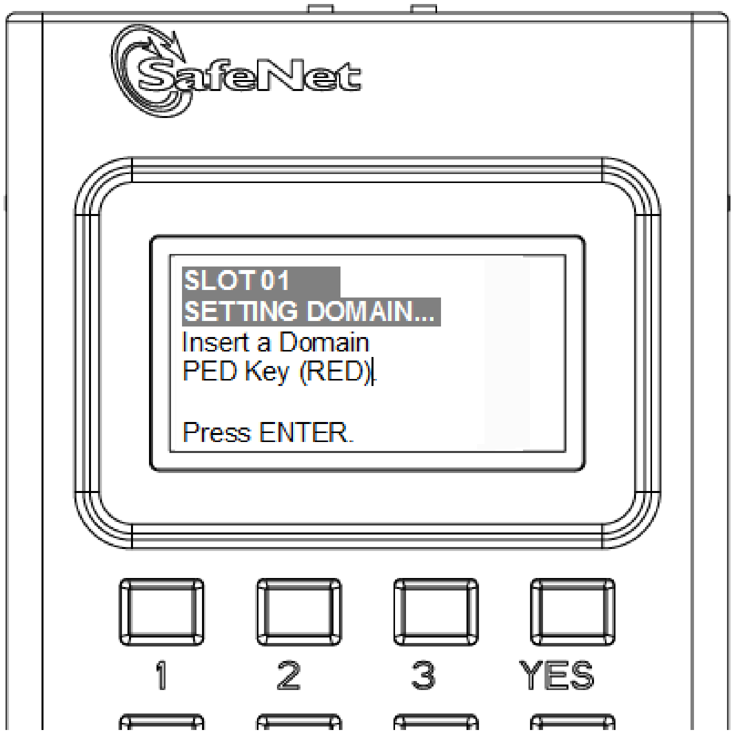


SLOT 01
SETTING RPV...
Would you like to
reuse an existing
keyset? (Y/N)

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.

10. 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 M of N splitting.

11. The PED then prompts for a red Domain PED key with the message



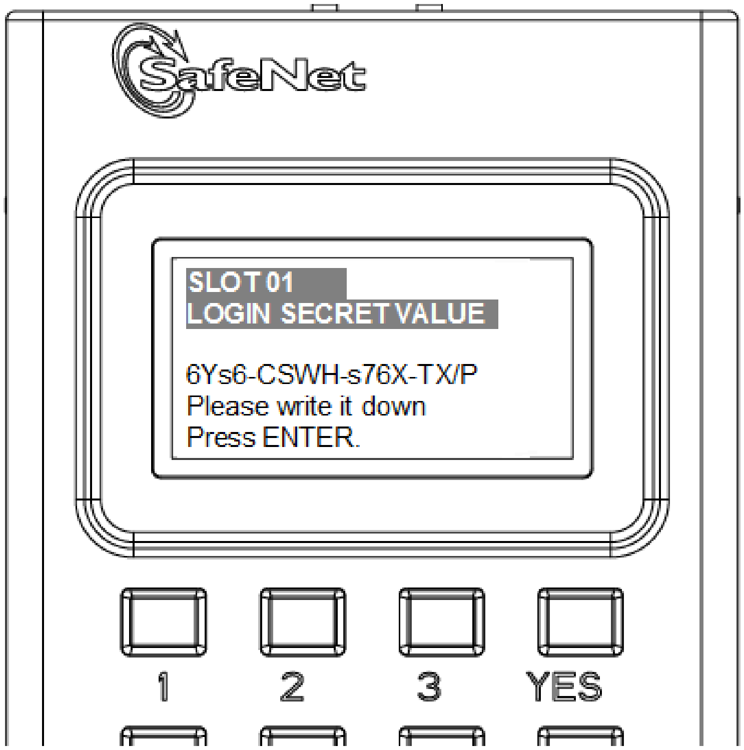
SLOT 01
SETTING DOMAIN...
Insert a Domain
PED Key (RED)

Press ENTER.

Insert the red HSM Partition Domain PED key [of course, the PED Key is generically black - we suggest that you apply the appropriate color sticker either immediately before or immediately after imprinting] and press [Enter]. A unique Partition Owner PIN is to be imprinted on both the PED key and the HSM Partition.

12. The PED goes through the same prompts as for the black PED Key. Respond as appropriate.

13. Luna PED presents the generated partition challenge secret (password), which you must record:



SLOT 01
LOGIN SECRET VALUE

6Ys6-CSWH-s76X-TX/P
Please write it down
Press ENTER.

We suggest that you record the presented string using a text editor - in our experience, the greatest proportion of errors with the partition challenge secret involve misreading of hand-written text. The dashes (hyphens) are displayed only to enhance human readability of the string- they are not part of the 16-character partition challenge secret or partition password.

14. Control returns to luna shell with:

```
'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.

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))
```

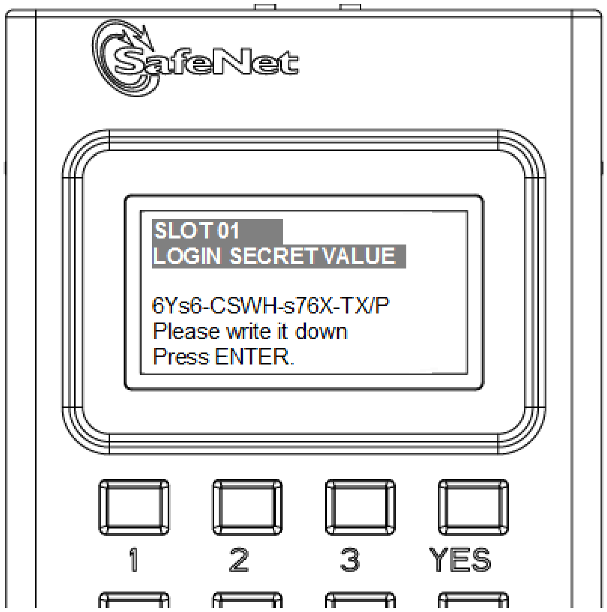
In the example above, the HSM serial number is 150718 and the partition container number is 20. Note that the partition container number is a three-digit number with leading zeros suppressed, so that the actual partition container number is 020. To determine the partition serial number concatenate the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

```
150718020
```

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

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.



```
SLOT 01
LOGIN SECRET VALUE

6Ys6-CSWH-s76X-TX/P
Please write it down
Press ENTER.
```

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 Luna SA.

> **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, Luna PED goes back to "Awaiting command...".

Next you might need to adjust the Partition Policy settings for the new Partition. (Optional see "Partition Policies" on page 88)

Otherwise, see "Prepare the Client for Network Trust Link" on page 91.

CHAPTER 6

Partition Policies

At this point, you should have initialized the HSM and created an HSM Partition. You may need to set the policies that constrain the use of the HSM Partition by clients. Capabilities are factory settings ( ). Policies are the means of modifying the adjustable capabilities.

First, display the policies (default) of the created HSM 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 Administrator.

1. View the Partition policies. At the lunash prompt, type the command

```
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


   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


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

(Next, change any of the policies that you wish to change "Set Partition Policy" on page 89 .)

Set Partition Policy

Having viewed the Policy settings (previous page) you can now modify a Partition Policy for a given Partition, if required.

1. To change a Partition Policy, at the `lunash` prompt type:

   lunash:> partition changePolicy -partition <name of HSM Partition> -policy <policy code> -value <new policy value>

Select an example that is applicable to your Luna appliance's HSM type:

Policy setting example, Luna HSM with Password Authentication

The default minimum password length is 7 characters (which the Luna 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, Luna 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:>
```

Go to "Prepare the Client for Network Trust Link".

CHAPTER 7

Prepare the Client for Network Trust Link

Network Trust Links (NTL) are secure, authenticated network connections between the Luna SA and Clients. NTLs use two-way digital certificate authentication and TLS data encryption to protect sensitive data as it is transmitted between HSM Partitions on the Luna SA and Clients.

On the Luna appliance, port 1792 is used.

NTLs consist of three parts:

- Network Trust Link Service (NTLS) which resides on the Luna SA
- Network Trust Link Agents (NTLA) which are installed on Clients
- The Network Trust Link itself, a secure connection that is created between the NTLS and an authenticated NTLA.

The Luna SA can support up to 800 simultaneous NTL connections. There is some overhead in setting up each link, so if you are using a large number of links, it is best to stagger their starts, to avoid timeout.

The 800-connection capability is important for client applications that are multi-process based, rather than multi-threaded.

Preparing the Client

With the assistance of your local network administrator, you should already have prepared the Client system for network connection. This section is about introducing a Client to the HSM appliance, by creating and exchanging certificates, so that the two systems recognize each other. Therefore the Client needs all the standard network setup required of any networked computer — contact your Network Administrator for assistance. This means:

- Configure all the necessary IP settings (hostname, IP address, DNS, gateway, etc.) as appropriate to your network, and as applicable to your Client's operating system.
- Install an ssh client (the scp copy utility should already have been installed during the HSM software installation).
- Start network services on your Client machine and verify that you have achieved a proper, working network configuration (by means of "ping" and other network utilities).

In order to connect a Client to an HSM Partition on the HSM appliance, you must first create a Network Trust Link (NTL) between them. An NTL consists of:

- the Network Trust Link Agent (NTLA), a software library that resides on the Client
- the Network Trust Link Server (NTLS), the server software that manages Network Trust Links on the HSM appliance and,
- the NTL itself, an encrypted, secure communications channel between the Client's NTLA and the HSM appliance's NTLS.

Network Trust Links use digital certificates to verify the identities of connecting clients. During the initial HSM system configuration (earlier in this chapter), the Administrator generated a unique certificate that identifies the HSM appliance. Similarly, each Client must generate its own certificate that identifies it uniquely (next section). Both the Client and the HSM appliance use these certificates to verify the other's identity before an NTL is created between them.

To create an NTL, the Client and HSM appliance must first exchange certificates. Once the certificates have been exchanged, the Client registers the Luna SA’s certificate in a trust list, and the Luna SA appliance, in turn, registers the Client’s certificate in its list of clients.

When the certificates have been exchanged and registered at each end, the NTL is ready to use. This is described in upcoming pages of this section.

The client software was installed for your operating system during the general installation (refer to the *Luna SA QuickStart Guide*).

You will perform the actions in this section:

- the first time you commission a Luna SA appliance, and you require a client to exchange certificates with the HSM and to be assigned to an HSM Partition, and
- whenever you have a new client that needs access to an HSM Partition.

Import a Server Cert

Choose the version for your client computer's operating system:

See "Import HSM Appliance Server Certificate onto Client (UNIX)" on page 102.

OR

See "Import HSM Appliance Server Certificate onto Client (Windows)" on page 93.

Prepare a Network Trust Link - Windows

In this section, create and exchange certificates from Windows systems, to configure a Network Trust Link with your Luna SA appliance.

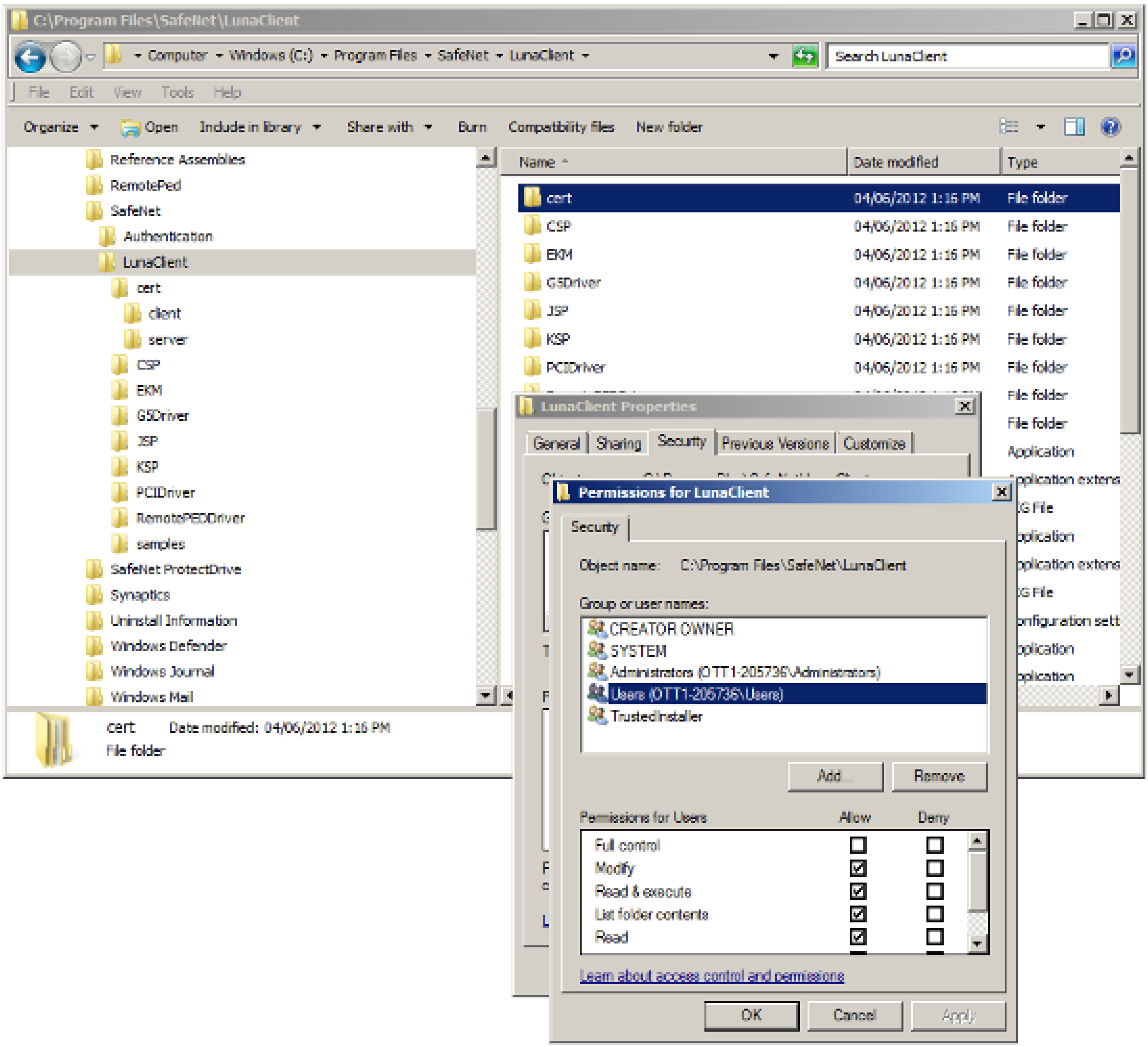
Import HSM Appliance Server Certificate onto Client (Windows)

1. Open a command prompt window on the Client, and change directory to `c:\Program Files\Safenet\LunaClient\`.
2. Securely transfer the `server.pem` file from the Luna SA, using the supplied pscp utility.
   ```
   c:\Program Files\SafeNet\LunaClient\ > pscp admin@myLuna:server.pem .
   admin@myLuna's password:
   server.pem           100%
   |*****************************************************| 928
   00:00
   ```
   Note the dot (.) at the end of the command, denoting “place the resulting file in the current directory”.
3. Verify that the Server Certificate has arrived on the Client:
   ```
   c:\Program Files\SafeNet\LunaClient\ > dir
   server.pem
   ```
4. Move the Server Certificate to the cert/server directory:
   ```
   move server.pem c:\Program Files\SafeNet\LunaClient\cert\server
   ```

You might need to surround the entire filespec (path and filename) within quotation marks if Windows stumbles at the space between Program and Files.

If the operations fail - and you have verified that the commands are typed correctly - then you might lack file permissions in the affected directories. If you lack administrator privileges on your computer, contact your IT department. If you do have the required privileges, then you might need to adjust the permissions for the affected directories (which by default are installed in the protected Windows directory "Program Files").

To adjust the permissions for the directory c:\Program Files\SafeNet\LunaClient\, right-click that directory. In the resulting context menu, select Properties, and in the ensuing dialog select the "Security" tab. Choose the appropriate user or group and adjust as needed. Then repeat the commands in the steps above, which should now work as expected.


C:\Program Files\SafeNet\LunaClient
Computer ▸ Windows (C:) ▸ Program Files ▸ SafeNet ▸ LunaClient
Search LunaClient
File Edit View Tools Help
Organize Open Include in library Share with Burn Compatibility files New folder
Reference Assemblies
RemotePed
SafeNet
Authentication
LunaClient
cert
client
server
CSP
EKM
G5Driver
JSP
KSP
PCIDriver
RemotePEDDriver
samples
SafeNet ProtectDrive
Synaptics
Uninstall Information
Windows Defender
Windows Journal
Windows Mail
cert Date modified: 04/06/2012 1:16 PM
File folder
LunaClient Properties
General Sharing Security Previous Versions Customize
Permissions for LunaClient
Security
Add... Remove
Learn about access control and permissions
OK Cancel Apply

Name	Date modified	Type
cert	04/06/2012 1:16 PM	File folder
CSP	04/06/2012 1:16 PM	File folder
EKM	04/06/2012 1:16 PM	File folder
G5Driver	04/06/2012 1:16 PM	File folder
JSP	04/06/2012 1:16 PM	File folder
KSP	04/06/2012 1:16 PM	File folder
PCIDriver	04/06/2012 1:16 PM	File folder

Object name: C:\Program Files\SafeNet\LunaClient

Group or user names:

- CREATOR OWNER
- SYSTEM
- Administrators (OTT1-205736\Administrators)
- Users (OTT1-205736\Users)
- TrustedInstaller

Permissions for Users	Allow	Deny
Full control	☐	☐
Modify	☑	☐
Read & execute	☑	☐
List folder contents	☑	☐
Read	☑	☐

The appearance might vary slightly for different Windows versions. If the permissions change does not propagate to sub-directories, then you might need to repeat the process for the "cert" sub-directory and for the "client" and "server" sub-directories.

Example

Securely transfer the server.pem file from the Luna SA, using the supplied pscp utility.

```
c:\Program Files\SafeNet\LunaClient\ > pscp admin@192.168.0.123:server.pem .
admin@192.168.0.123's password:
server.pem              100%
|*****************************************************| 928
00:00
```

Any time the IP or hostname of the HSM appliance has changed (such as moving from a pre-production environment), the client(s) that have previously connected via SSH will detect a mismatch in the HSM appliance's server certification information and warn you of potential security breach. In this case you will need to remove that server's certificate information from the client's known host file found in:

```
/<user home dir>/.ssh/known_hosts2
```

If this is happening in a production environment, this could potentially be a security breach needing investigation.

Similarly, when you first open a scp or ssh link, you must accept the certificate.
You can check the fingerprint of the certificate with:

```
lunash:> sysconf fingerprint -ssh
```

Next, see "Register the HSM Server Certificate with the Client (Windows)" on page 95.

Register the HSM Server Certificate with the Client (Windows)

Use vtl, the supplied client-side tool for managing HSM client/server setup. The vtl command is not interactive. It is called from the command line or a shell prompt, it completes its current task, and it exits back to the shell.

Invoke the `vtl addServer` command so that the client can create a secure connection with the HSM (the server).

The vtl executable is located at `c:\Program Files\SafeNet\LunaClient` unless you have changed the default installation.

Register

```
C:\Program Files\SafeNet\LunaClient > vtl addServer -n <LunaSA hostname-or-IPaddress> -c <serverCert-file>
```

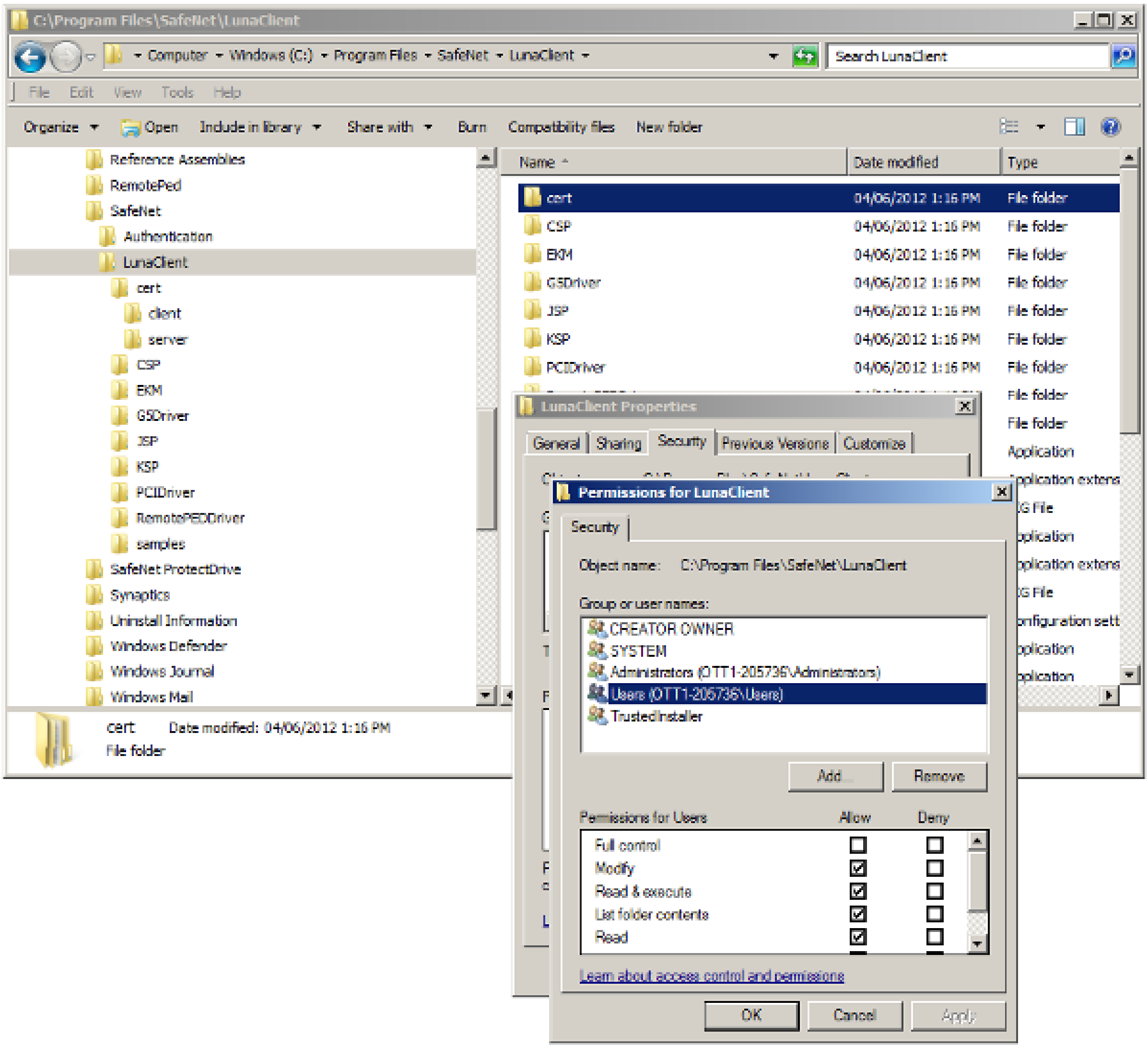
Example

```
  c:\Program Files\SafeNet\LunaClient\ > vtl addServer -n myLuna3 -c server.pem
```

You might need to surround the entire filespec (path and filename) within quotation marks if Windows stumbles at the space between Program and Files.

If the operations fail - and you have verified that the commands are typed correctly - then you might lack file permissions in the affected directories. If you lack administrator privileges on your computer, contact your IT department. If you do have the required privileges, then you might need to adjust the permissions for the affected directories (which by default are installed in the protected Windows directory "Program Files").

To adjust the permissions for the directory c:\Program Files\SafeNet\LunaClient\, right-click that directory. In the resulting context menu, select Properties, and in the ensuing dialog select the "Security" tab. Choose the appropriate user or group and adjust as needed. Then repeat the commands in the steps above, which should now work as expected.


C:\Program Files\SafeNet\LunaClient
Computer ▸ Windows (C:) ▸ Program Files ▸ SafeNet ▸ LunaClient ▸
Search LunaClient
File Edit View Tools Help
Organize Open Include in library Share with Burn Compatibility files New folder
Reference Assemblies
RemotePed
SafeNet
Authentication
LunaClient
cert
client
server
CSP
EKM
GSDriver
JSP
KSP
PCIDriver
RemotePEDDriver
samples
SafeNet ProtectDrive
Synaptics
Uninstall Information
Windows Defender
Windows Journal
Windows Mail
Name
Date modified
Type
LunaClient Properties
General Sharing Security Previous Versions Customize
Permissions for LunaClient
Security
Add... Remove
Learn about access control and permissions
OK Cancel Apply

Name	Date modified	Type
cert	04/06/2012 1:16 PM	File folder
CSP	04/06/2012 1:16 PM	File folder
EKM	04/06/2012 1:16 PM	File folder
GSDriver	04/06/2012 1:16 PM	File folder
JSP	04/06/2012 1:16 PM	File folder
KSP	04/06/2012 1:16 PM	File folder
PCIDriver	04/06/2012 1:16 PM	File folder

cert Date modified: 04/06/2012 1:16 PM
File folder

Object name: C:\Program Files\SafeNet\LunaClient

Group or user names:

- CREATOR OWNER
- SYSTEM
- Administrators (OTT1-205736\Administrators)
- Users (OTT1-205736\Users)
- TrustedInstaller

Permissions for Users	Allow	Deny
Full control	□	□
Modify	☑	□
Read & execute	☑	□
List folder contents	☑	□
Read	☑	□

The appearance might vary slightly for different Windows versions. If the permissions change does not propagate to sub-directories, then you might need to repeat the process for the "cert" sub-directory and for the "client" and "server" sub-directories.

If you are working without DNS, then give the server IP number, rather than its name, as in:

c:\Program Files\SafeNet\LunaClient\ >vtl addServer -n <sa-ip-address> -c server.pem

When you have completed this step, see "Create a Client Certificate (Windows)" on page 96.

Create a Client Certificate (Windows)

Begin by creating a certificate and private key for the client, using the vtl command-line interface.

Note: Before you run the `vtl createCert` command, run `hostname` to view the hostname of your client computer. Then, when you run the `vtl createCert -n <clientHostname>` command (example below), be sure to input the hostname *exactly* as reported (uppercase/lowercase). If you create a certificate using a hostname parameter that is not an exact case-match for the client's hostname, you may be unable to create an NTLS link.

```
c:\Program Files\SafeNet\LunaClient\ >vtl createCert -n <clientHostname>
```

Example

```
c:\Program Files\SafeNet\LunaClient > vtl createCert -n myClient1

c:\Program Files\SafeNet\LunaClient\cert\client > dir
vtl
myClient1.pem
myClient1Key.pem
```

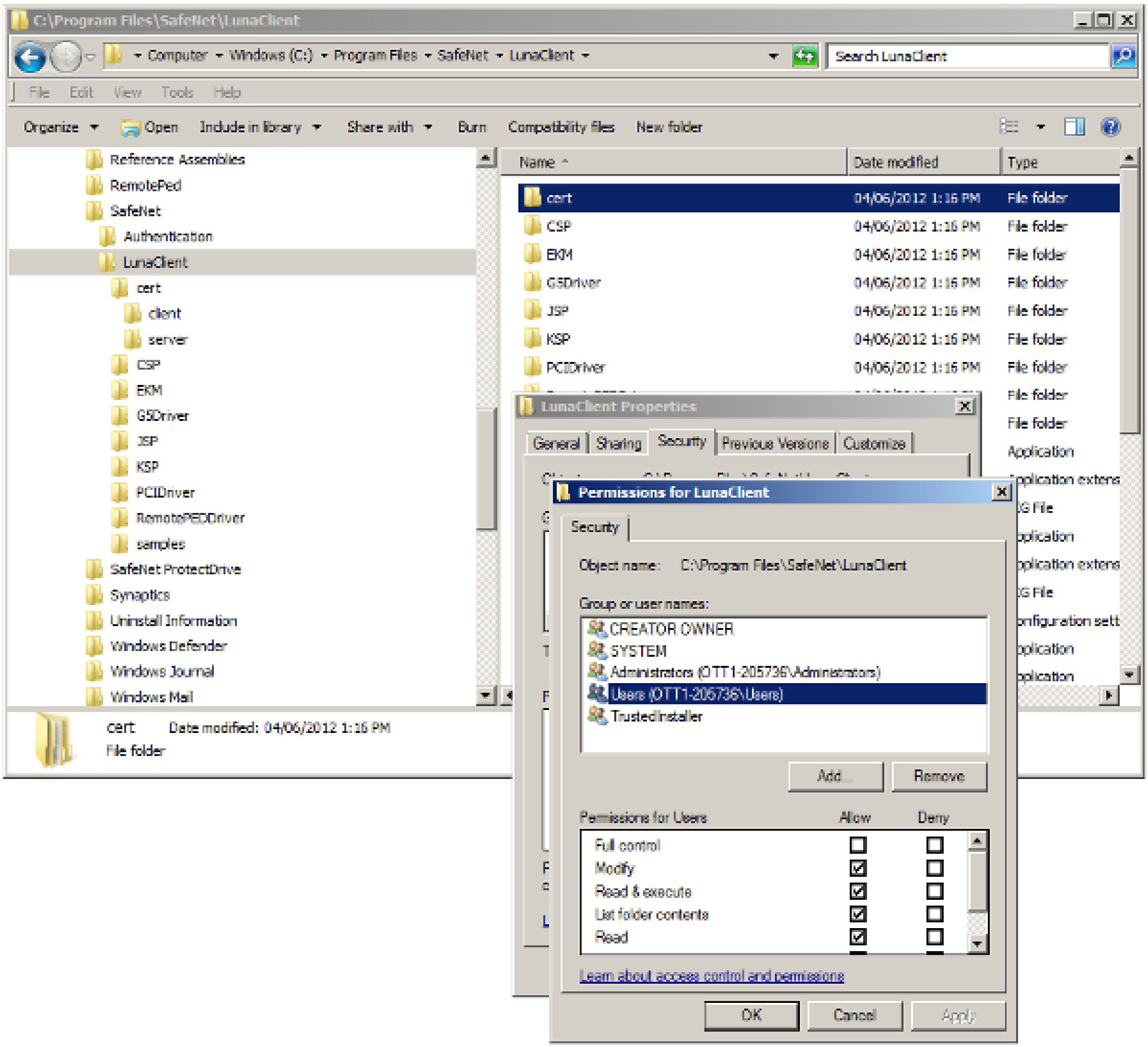
After the createCert command, vtl gives the full pathname to the key and cert files that were generated.

Note: "-n" (name) is the only mandatory item, and must be the client hostname. Additional optional parameters can be added. Refer to the Reference section of this Help for full command syntax and description.

You might need to surround the entire filespec (path and filename) within quotation marks if Windows stumbles at the space between Program and Files.

If the operations fail - and you have verified that the commands are typed correctly - then you might lack file permissions in the affected directories. If you lack administrator privileges on your computer, contact your IT department. If you do have the required privileges, then you might need to adjust the permissions for the affected directories (which by default are installed in the protected Windows directory "Program Files").

To adjust the permissions for the directory c:\Program Files\SafeNet\LunaClient\, right-click that directory. In the resulting context menu, select Properties, and in the ensuing dialog select the "Security" tab. Choose the appropriate user or group and adjust as needed. Then repeat the commands in the steps above, which should now work as expected.


C:\Program Files\SafeNet\LunaClient
Computer ▸ Windows (C:) ▸ Program Files ▸ SafeNet ▸ LunaClient ▸
Search LunaClient
File Edit View Tools Help
Organize ▾ Open Include in library ▾ Share with ▾ Burn Compatibility files New folder
Reference Assemblies
RemotePed
SafeNet
Authentication
LunaClient
cert
client
server
CSP
EKM
G5Driver
JSP
KSP
PCIDriver
RemotePEDDriver
samples
SafeNet ProtectDrive
Synaptics
Uninstall Information
Windows Defender
Windows Journal
Windows Mail
Name
Date modified
Type
cert 04/06/2012 1:16 PM File folder
CSP 04/06/2012 1:16 PM File folder
EKM 04/06/2012 1:16 PM File folder
G5Driver 04/06/2012 1:16 PM File folder
JSP 04/06/2012 1:16 PM File folder
KSP 04/06/2012 1:16 PM File folder
PCIDriver 04/06/2012 1:16 PM File folder
File folder
File folder
Application
Application extens
G File
plication
plication extens
G File
onfiguration sett
plication
plication
cert Date modified: 04/06/2012 1:16 PM
File folder
LunaClient Properties
General
Sharing
Security
Previous Versions
Customize
Permissions for LunaClient
Security
Add...
Remove
Learn about access control and permissions
OK
Cancel
Apply

Object name: C:\Program Files\SafeNet\LunaClient

Group or user names:

- CREATOR OWNER
- SYSTEM
- Administrators (OTT1-205736\Administrators)
- Users (OTT1-205736\Users)
- TrustedInstaller

Permissions for Users	Allow	Deny
Full control	☐	☐
Modify	☑	☐
Read & execute	☑	☐
List folder contents	☑	☐
Read	☑	☐

The appearance might vary slightly for different Windows versions. If the permissions change does not propagate to sub-directories, then you might need to repeat the process for the "cert" sub-directory and for the "client" and "server" sub-directories.

Note:
If you are working without DNS, then supply the client IP numerically, instead:

```
c:\Program Files\SafeNet\LunaClient\>vtl createCert  -n
<clientIPaddress>
```

In this case, the key and cert files are created with the filename being the IP address of the Client.

Note: In the `createCert` command, provide only the unqualified hostname, rather than the fully qualified hostname.

Next, see "Export a Client Cert to an HSM Appliance (Windows)" on page 99. That is the other half of the certificate exchange that creates the secure NTLS link.

Export a Client Cert to an HSM Appliance (Windows)

Send the client certificate (that you created on the previous page) to the HSM appliance, as follows.

The command is:

```
C:\Program Files\SafeNet\LunaClient\ > pscp cert\client\<clientCert>.pem admin@<serverhostname-or-IP>:
```

You are prompted for the HSM appliance admin password.

Example

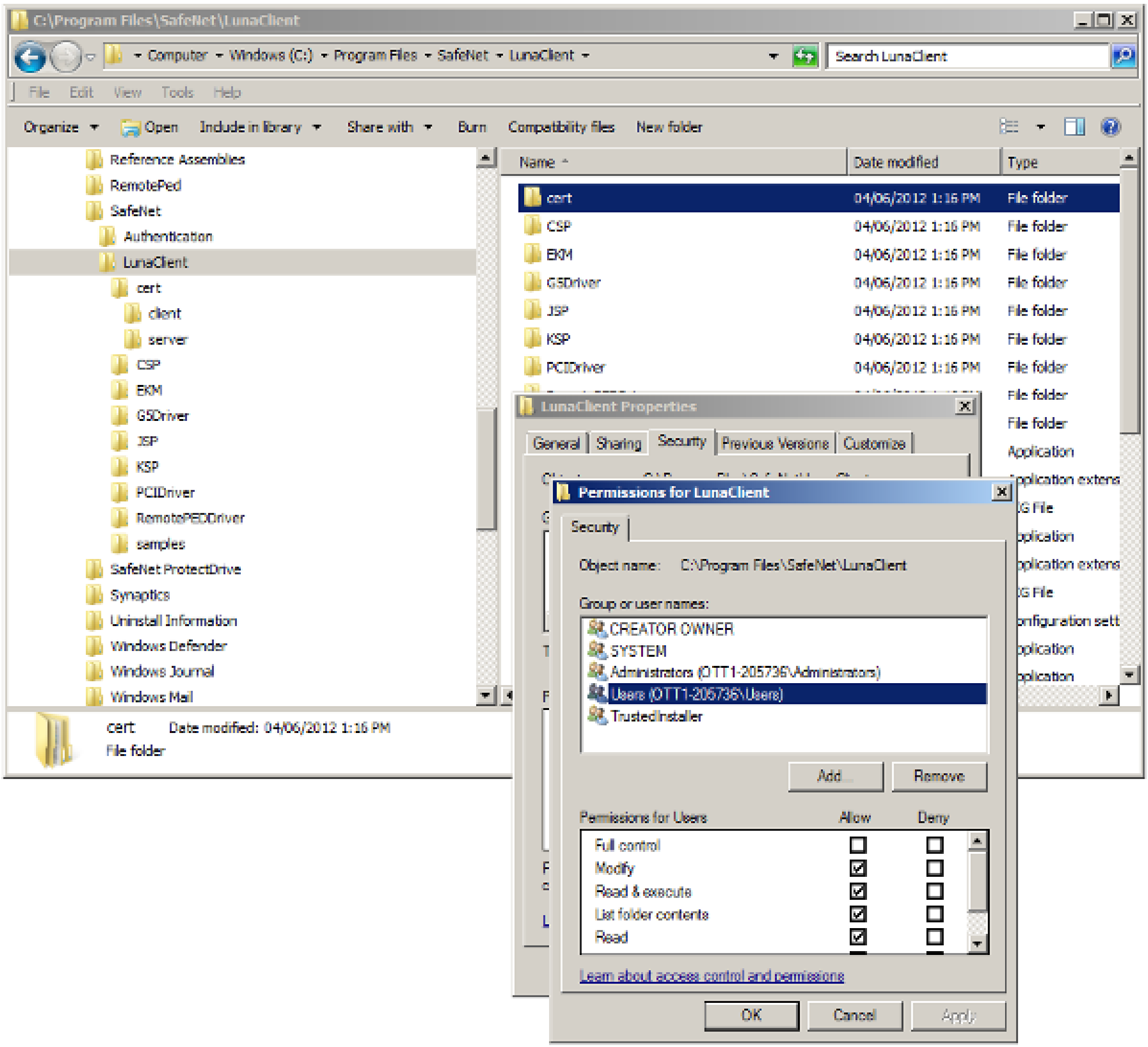
```
c:\> cd \Program Files\SafeNet\LunaClient\cert\client

c:\ Program Files\SafeNet\LunaClient\cert\client> dir

myClient1Key.pem  myClient1.pem

c:\ Program Files\SafeNet\LunaClient\> pscp “c:\Program Files\SafeNet\LunaClient\cert\client\myClient1.pem” admin@myLuna3:
```

You must scp to the admin account on the HSM appliance, or the client certificate will not register correctly.

You might need to surround the entire filespec (path and filename) within quotation marks if Windows stumbles at the space between Program and Files.

If the operations fail - and you have verified that the commands are typed correctly - then you might lack file permissions in the affected directories. If you lack administrator privileges on your computer, contact your IT department. If you do have the required privileges, then you might need to adjust the permissions for the affected directories (which by default are installed in the protected Windows directory "Program Files").

To adjust the permissions for the directory c:\Program Files\SafeNet\LunaClient\, right-click that directory. In the resulting context menu, select Properties, and in the ensuing dialog select the "Security" tab. Choose the appropriate user or group and adjust as needed. Then repeat the commands in the steps above, which should now work as expected.



C:\Program Files\SafeNet\LunaClient
Computer ▸ Windows (C:) ▸ Program Files ▸ SafeNet ▸ LunaClient ▸
Search LunaClient
File Edit View Tools Help
Organize ▾ Open Include in library ▾ Share with ▾ Burn Compatibility files New folder
Reference Assemblies
RemotePed
SafeNet
Authentication
LunaClient
cert
client
server
CSP
EKM
GSDriver
JSP
KSP
PCIDriver
RemotePEDDriver
samples
SafeNet ProtectDrive
Synaptics
Uninstall Information
Windows Defender
Windows Journal
Windows Mail
cert Date modified: 04/06/2012 1:16 PM
File folder
LunaClient Properties
General Sharing Security Previous Versions Customize
Permissions for LunaClient
Security
Add... Remove
Learn about access control and permissions
OK Cancel Apply

Name	Date modified	Type
cert	04/06/2012 1:16 PM	File folder
CSP	04/06/2012 1:16 PM	File folder
EKM	04/06/2012 1:16 PM	File folder
GSDriver	04/06/2012 1:16 PM	File folder
JSP	04/06/2012 1:16 PM	File folder
KSP	04/06/2012 1:16 PM	File folder
PCIDriver	04/06/2012 1:16 PM	File folder

Object name: C:\Program Files\SafeNet\LunaClient

Group or user names:

- CREATOR OWNER
- SYSTEM
- Administrators (OTT1-205736\Administrators)
- Users (OTT1-205736\Users)
- TrustedInstaller

Permissions for Users	Allow	Deny
Full control	☐	☐
Modify	☑	☐
Read & execute	☑	☐
List folder contents	☑	☐
Read	☑	☐

The appearance might vary slightly for different Windows versions. If the permissions change does not propagate to sub-directories, then you might need to repeat the process for the "cert" sub-directory and for the "client" and "server" sub-directories.

Note: For networks without DNS, use the HSM appliance's IP address, instead of the hostname.

Example

```
c:\> cd \Program Files\SafeNet\LunaClient\cert\client

c:\ Program Files\SafeNet\LunaClient\cert\client> dir

<client-ip-address>Key.pem  <client-ip-address>.pem
```

```
c:\ Program Files\SafeNet\LunaClient\> pscp “c:\Program Files\SafeNet\LunaClient\cert\client\<client-ip-address>.pem” admin@<appliance-ip-address>:
```

Note: The “:” after the destination is required. Without the colon, scp does not recognize the supplied destination as a remote server. The file arriving at the HSM is automatically placed in the appropriate directory. Do not specify a directory for destination.

Next, see "Register the Client Certificate to an HSM Server" on page 105, to continue the setup (configuration is nearly done at this point).

Prepare a Network Trust Link - UNIX/Linux

In this section, create and exchange certificates from Linux and UNIX systems, to configure a Network Trust Link with your Luna SA appliance.

Import HSM Appliance Server Certificate onto Client (UNIX)

1. Ensure that you are in the `/usr/lunaclient/bin` directory on the Client.
2. Securely transfer the `server.pem` file from the Luna SA, using the scp utility.

   ```
   bash-2.05# scp admin@myLuna3:server.pem .
   admin@myLuna3's password:
   server.pem           100%
   |*****************************************************| 928
   00:00
   ```

   Note the dot (.) at the end of the command, denoting “place the resulting file in the current directory”.
3. Verify that the Server Certificate has arrived on the Client:

   ```
   bash-2.05# ls
   multitoken2  openssl.cnf server.pem vtl
   ```

Example

Securely transfer the server.pem file from the Luna SA, using the scp utility.

```
bash-2.05# scp admin@192.168.0.123:server.pem .
admin@192.168.0.123's password:
server.pem           100%
|*****************************************************| 928
00:00
```

Any time the IP or hostname of the HSM appliance has changed (such as moving from a pre-production environment), the client(s) that have previously connected via SSH will detect a mismatch in the HSM appliance's server certification information and warn you of potential security breach. In this case you will need to remove that server's certificate information from the client’s known host file found in:

```
/<user home dir>/.ssh/known_hosts2
```

If this is happening in a production environment, this could potentially be a security breach needing investigation.

Similarly, when you first open a scp or ssh link, you must accept the certificate.
You can check the fingerprint of the certificate with:

```
lunash:> sysconf fingerprint -ssh
```

Next, see "Register the HSM Server Certificate with the Client (UNIX)" on page 102.

Register the HSM Server Certificate with the Client (UNIX)

Use vtl, the supplied client-side tool for managing HSM client/server setup. The vtl command is not interactive. It is called from the command line or a shell prompt, it completes its current task, and it exits back to the shell.

Invoke the `vtl addServer` command so that the client can create a secure connection with the HSM (the server).

The vtl executable is located at /usr/safenet/lunaclient/bin/ unless you changed the default.

Register

```
bash-2.05# ./vtl addServer -n <LunaSAhostname-or-IPaddress> -c server.pem
```

Example

```
bash-2.05# ./vtl addServer -n myLuna3 -c cert/server/server.pem
```

If you are working without DNS, then give the server IP number, rather than its name, as in:

```
bash-2.05# ./vtl addServer -n <sa-IP-address> -c <serverCert-file>
```

Next, see "Create a Client Certificate (UNIX)" on page 103.

Create a Client Certificate (UNIX)

Begin by creating a certificate and private key for the client, using the vtl command-line interface.

Note: Before you run the vtl createCert command, run hostname to view the hostname of your client computer. Then, when you run the vtl createCert -n <clientHostname> command (below), be sure to input the hostname exactly as reported (uppercase/lowercase). If you create a certificate using a hostname parameter that is not an exact case-match for the client's hostname, you might be unable to create an NTLS link.

```
bash-2.05# ./vtl createCert -n <clientHostname>
```

Example

```
bash-2.05# ./vtl createCert -n myClient1

bash-2.05# ls -lr
total 816
-rwxr-xr-x 1 root root 735720 Apr 19 14:08 vtl
-rw-r--r-- 1 root root 908 Apr 23 14:38 myClient1.pem
-rw-r--r-- 1 root root 887 Apr 23 14:38 myClient1Key.pem
-rwxr-xr-x 1 root root 7144 Apr 19 14:08 openssl.cnf
```

After the createCert command, vtl gives the full pathname to the key and cert files that were generated.

Note: "-n" (name) is the only mandatory item, and must be the client hostname. Additional optional parameters can be added.

Note: If you are working without DNS, then supply the client IP numerically, instead:

```
bash-2.05# ./vtl createCert -n <clientIPaddress>
```

The cert and key files are created with the Client computer's IP address as the filenames.

Note: In the `createCert` command, provide only the unqualified hostname, rather than the fully qualified hostname.

Next, see "Export a Client Cert to an HSM Appliance (UNIX)" on page 104. That is the other half of the certificate exchange that creates the secure NTLS link.

Export a Client Cert to an HSM Appliance (UNIX)

Send the client certificate (that you created on the previous page) to the HSM appliance, as follows.

The command is:

```
bash-2.05# scp /usr/safenet/lunaclient/cert/client/<clientCert>.pem
 admin@<serverhostname-or-IP>:
```

You are prompted for the HSM appliance admin password.

Example

```
bash-2.05# cd ../cert/client
bash-2.05# ls
myClient1Key.pem  myClient1.pem
bash-2.05# scp myClient1.pem admin@myLuna3:
```

You must scp to the admin account on the HSM appliance, or the client certificate will not register correctly.

Note: For networks without DNS, use the HSM appliance's IP address, instead of the hostname.

Example

```
bash-2.05# cd ../cert/client
bash-2.05# ls
<client-ip-address>Key.pem  <client-ip-address>.pem
bash-2.05# scp <client-ip-address>.pem admin@<appliance-ip-address>:
```

Note: The “:” after the destination is required. Without the colon, scp does not recognize the supplied destination as a remote server. The file arriving at the HSM is automatically placed in the appropriate directory. Do not specify a directory for destination.

Next, see "Register the Client Certificate to an HSM Server" on page 105, to continue the setup (configuration is nearly done at this point).

Register the Client Certificate to an HSM Server

The client certificate, which has been securely transferred (scp'd) from the client to the HSM Server, in previous sections, must be registered by the HSM Server.

You must be connected to the HSM Server and logged in as “admin”.

The basic command is:

```
lunash:> client register -client <client’s-name>
 -hostname <client’s-hostname>
```

The <client’s-name>, above can be any string that allows you to easily identify this client - many people use the hostname, but the <client's-name> can be any string that you find convenient. This might sound a little redundant (naming the client twice in one command), but it becomes especially useful if you are not using DNS -in that case, a well-considered <client's-name> is likely going to be easier to remember or recognize (more meaningful) than would the client's ip-address.

The command is expecting to find (on the Luna SA appliance) a client certificate filename that matches the client’s hostname (or ip-address if you are not using DNS hostnames), as you provide it here. In other words, this is a check that you are registering the client whose .pem file you created in the previous steps and scp'd to the appliance. You can register several clients to the appliance.

Example – lunash client registerClient Command

```
lunash:> client register -client MyClient -hostname MyClient

Client registration successful.
lunash:> client list
registered client 1: MyClient
lunash:>
```

Note: If you are working without DNS, then register the client by its IP address, rather than its hostname.

lunash:> client register -client <client’s-name> -ip <clientIPaddress>

The foregoing is sufficient for "real" (non-VM) clients. See below if your client is a virtual-machine instance.

The Client is now registered with the Luna SA.

You can verify on the Luna SA, with the `client list` command.

Refer to the Reference section of this Help for command syntax and descriptions.

Note: De-Register (registration not complete)
If you have multiple HSM appliances connected and registered with a client and you de-register that client from one of the HSM appliances, then you must also de-register that HSM appliance on the client side.
Failure to do so will result in a “Broken pipe” error, which indicates an incomplete registration.

Note: Re-Register
If you wish to de-register a client and then re-register with a new certificate, on the same HSM appliance, then you must copy the certificate to the HSM appliance (HSM server) and stop and re-start the NTLS service. Before such a restart, any connection attempts fail, and “Error on SSL accept” is logged.

Note: Administration commands can take a few seconds to be noted by the NTLS. If you have added or deleted a client, we suggest that you wait a few seconds before connecting.

How Many Clients?

Most applications require only a few separate clients to be registered with the Luna SA, and then those clients act as application servers or web servers to the rest of the world. The rest of the world usually has no need to connect as clients directly to the Luna SA.

Regardless of who is connecting (your servers acting as clients to the Luna SA, or your own customers given client access to your Luna SA) note that any registered client might make dozens or hundreds of simultaneous connections while running multi-process applications against the Luna SA HSM server.

The Luna SA appliance is designed for such multi-connection operation. See "Connections to the Appliance - Limits " on page 1 for a discussion of how total connections are determined.

Register VM Clients

When the client is a virtual machine instance, the possibility exists that the VM could be cloned or moved. NTL is not aware of such an event. For optimum security, when registering VM clients with Luna SA partitions, you should invoke the additional layer "HTL".

The "client register" command includes the options "-requireHtl", which invokes the Host Trust Link, and "-ottExpiry" and "-generateOtt" to create and configure the One Time Token used by HTL in setting up its hardware-independent trust link.

HTL should be considered mandatory for virtual clients, and optional (but a good idea) for "real" clients.

What's the Next Step?

Proceed to the next section "Assign a Client to an HSM Partition" on page 107 , which is the last configuration step before you start using your application with the Luna SA HSM server.

Optionally (as mentioned above), for use with virtual/cloud environments, or to additionally secure non-virtual configurations, you can choose to establish a Host Trust Link "Configuring and Using HTL".

CHAPTER 8

Assign a Client to an HSM Partition

At this point, you should already have performed the following tasks to create a Network Trust Link (NTL) between Client and Luna SA.:

- initialized the HSM and created one-or-more HSM Partitions
- exchanged certificates between the Luna SA and the Client
- registered the certificates of Client and Luna SA with each other

The final Configuration step, before your Client can begin using the Luna SA, is to assign the Client to a specific Partition. You will perform the actions in this section whenever you have a new client that needs access to an HSM Partition.

> **Note:** You must be connected to the HSM Server and logged in as “admin”.

Assign a Client to a Partition

Assign the registered client to the HSM Partition.

The command is:

```
lunash:> client assignPartition -client <clientname> -partition <partition name>
```

Example – lunash client - assignPartition Command

```
lunash:> client assignPartition -client myClient1 -partition myPartition1
'client assignpartition ' successful.
```

> **Note:**
> The parameter <partition name> is the name of the HSM Partition that was created earlier, following configuration of the HSM.

To verify, look at the HSM Partition assigned to the client.

```
lunash:> client show -client <clientname>
```

Refer to the Reference section of this Help for command syntax and descriptions.

Verify Your Setup

Before beginning to use a Client application with your newly configured Luna SA system, you can verify that the foregoing setup has been properly performed.

1. On your Client computer, open a command-line console.

2. Go to the software directory (`c:\Program Files\SafeNet\LunaClient` for Windows, or `/usr/safenet/lunaclient` for Linux, Solaris or AIX, or `/opt/safenet/lunaclient` for HP-UX), and type `vtl verify`.
3. The response should be similar to:

```
Slot    Serial #     Label
====    ======== =====
1       2279315 Partition1
```

  If you get an error message, then some part of the configuration has not been properly completed. Retrace the procedure.

At this point, the client and HSM are configured and registered with each other. You can now begin to use the Luna SA with your application.

You can use the “`partition list`” command for a list of HSM Partitions on the HSM, and the “`client list`” command for a list of the clients assigned to an HSM Partition.

DONE!

Yes. That was the complete setup. We suggest that you browse the Administration & Maintenance manuals to develop a deeper understanding of the options and capabilities of your Luna SA appliance, and of the housekeeping tasks and utilities that you might need. The SDK section is provided for programmers/developers.

Client Connection Limits

See "Connections to the Appliance - Limits ", for a discussion of the limits for client connections to a Luna SA appliance and HSM.

Applications and Integrations

If you have any of dozens of third-party applications, we might already have performed system integration with it, and published an Integration Guide for the application or API that you wish to use. Contact SafeNet Customer Support for the latest list of current integrations, or to request that one be developed.

CHAPTER 9
Optional Configuration Tasks

After completing the base configuration, you can also perform any of the following optional configuration tasks:

Configure a host trust link (HTL)

Host trust links ensure that the HSM connects only to a trusted host that is in possession of a one-time-token. See "Host Trust Link Client Authentication" on page 1 in the *Administration Guide*.

Configure the Luna SA appliance to use a Network Time Protocol (NTP) server

You can synchronize a Luna SA 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. Luna SA also provides secure NTP. See "Timestamping – NTP and Time Drift" on page 1 in the *Luna SA 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) Mode " on page 1 in the *Administration Guide*.

Configure SNMP

You can use the Luna 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*.