SafeNet Luna Network HSM 7.0

Configuration Guide

gemalto

security to be free

Document Information

Product Version	7.0
Document Part Number	007-013576-002
Release Date	02 June 2017

Revision History

Revision	Date	Reason
Rev. A	02 June 2017	Initial release.

Trademarks, Copyrights, and Third-Party Software

Table 1: Third-party software used in this product

Software	License and copyright
editline	This product incorporates editline licensed under Apache v2.0 Open Software. Copyright 1992,1993 Simmule Turner and Rich Salz. All rights reserved. You can obtain the full text of the Apache v2.0 Open Software license at the following URL: https://www.apache.org/licenses/LICENSE-2.0
libFDT	Dual License Choice of BSD or GPL-2.0 Copyright (C) 2006 David Gibson, IBM Corporation.
libsodium	ISC License (ISCL) Copyright (C) 2013-2016
Linux Kernel	GPL-2.0
OpenSSH	This product uses a derived version of OpenSSH Copyright 1995 Tatu Ylonen , Espoo, Finland. All rights reserved . Copyright 1995, 1996 by David Mazieres . Copyright 1983, 1990, 1992, 1993, 1995 The Regents of the University of California. All rights reserved You can obtain the full text of the OpenSSH license at the following URL: https://www.openbsd.org/policy.html
OpenSSL	SSLeay License Copyright (C) 1995-1998 Eric Young (eay@cryptsoft.com) OpenSSL license

Software	License and copyright
	Copyright (C) 1998-2002 The OpenSSL Project
Software implementation of SHA2	Proprietary license Copyright (C) 2002, Dr Brian Gladman, Worcester, UK.
Software implementation of AES	Proprietary license Copyright (C) 2001, Dr Brian Gladman <brg@gladman.uk.net>, Worcester, UK.

Disclaimer

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

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

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

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

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

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

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

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

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

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

All intellectual property is protected by copyright. All trademarks and product names used or referred to are the copyright of their respective owners. No part of this document may be reproduced, stored in a retrieval system or transmitted in any form or by any means, electronic, mechanical, chemical, photocopy, recording or otherwise without the prior written permission of Gemalto.

Regulatory Compliance

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

USA, FCC

This equipment has been tested and found to comply with the limits for a "Class B" digital device, pursuant to part 15 of the FCC rules.

Canada

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

Europe

This product is in conformity with the protection requirements of EC Council Directive 2014/30/EU. This product satisfies the CLASS B limits of EN55032.

CONTENTS

PREFACE
About the Configuration Guide

This document provides step-by-step instructions for configuring your SafeNet 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 102.

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

1. "Planning Your Configuration" on page 12

2. "Configure the SafeNet Luna Network HSM for Your Network" on page 28

3. "HSM Initialization" on page 44

4. "Set the HSM Policies" on page 54

5. "Create Application Partitions" on page 60

6. "Create a Network Trust Link Between the Client and the Appliance" on page 67

7. "Enable the Client to Access a Partition" on page 73

8. "Configure Application Partitions" on page 88

9. "Set Partition Policies" on page 99

Also review "Optional Configuration Tasks" on page 102 for more configuration options.

This preface also includes the following information about this document:

• "Customer Release Notes" below

• "Audience" below

• "Document conventions" on the next page

• "Support Contacts" on page 10

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

Customer Release Notes

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

Audience

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

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

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

Document conventions

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

Notes

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

> **Note:** Take note. Contains important or helpful information.

Cautions

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

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

Warnings

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

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

Command syntax and typeface conventions

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

Format	Convention
	• User input (In the **Date** box, type **April 1**.)
italics	In type, the italic attribute is used for emphasis or to indicate a related document. (See the *Installation Guide* for more information.)
<variable>	In command descriptions, angle brackets represent variables. You must substitute a value for command line arguments that are enclosed in angle brackets.
[**optional**] [<optional>]	Represent optional **keywords** or <variables> in a command line description. Optionally enter the keyword or <variable> that is enclosed in square brackets, if it is necessary or desirable to complete the task.
{a|b|c} {<a>|<b>|<c>}	Represent required alternate **keywords** or <variables> in a command line description. You must choose one command line argument enclosed within the braces. Choices are separated by vertical (OR) bars.
[a|b|c] [<a>|<b>|<c>]	Represent optional alternate keywords or variables in a command line description. Choose one command line argument enclosed within the braces, if desired. Choices are separated by vertical (OR) bars.

Support Contacts

Contact method	Contact	
Phone (Subject to change. An up-to-date list is maintained on the Technical Support Customer Portal)	Global	+1 410-931-7520
	Australia	1800.020.183
	India	000.800.100.4290
	Netherlands	0800.022.2996
	New Zealand	0800.440.359
	Portugal	800.863.499
	Singapore	800.1302.029
	Spain	900.938.717
	Sweden	020.791.028
	Switzerland	0800.564.849
	United Kingdom	0800.056.3158
	United States	(800) 545-6608
Web	https://safenet.gemalto.com	
Technical Support Customer Portal	https://supportportal.gemalto.com	

Contact method	Contact
	Existing customers with a Technical Support Customer Portal account can log in to manage incidents, get the latest software upgrades, and access the Knowledge Base. To create a new account, click the **Register** link at the top of the page. You will need your Customer Identifier number.

Planning Your Configuration

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

- "Appliance Roles" below
- "HSM Roles and Secrets" on page 14
- "Domain Planning" on page 16
- "Password-authenticated HSM Planning" on page 18
- "PED-authenticated HSM Planning" on page 20
- "Recommended Network Characteristics" on page 24
- "IPv6 Support and Limitations" on page 25

Appliance Roles

For the SafeNet Luna Network HSM, roles fall under two main hierarchies:

- Roles to access the appliance that contains the HSM and that provides the network connectivity; these are accessed through SSH or local serial connection, via the LunaSH command line, and include:
  - The highest-level, full-access administrative role, called 'admin'
  - The medium-level operational administrative role, called 'operator'
  - The lowest-level observation-only administrative role, called 'monitor'
  - The role responsible for managing HSM audit logging, independent from other roles on the HSM, called 'audit'
- Roles that access the HSM, described in "HSM Roles and Secrets" on page 14

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

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 enabled by the 'admin' user, default password "PASSWORD"
- One 'monitor' user, with role 'monitor,' disabled until enabled by the 'admin' user, default password "PASSWORD"
- One 'audit' user, with role 'audit', disabled until enabled by the 'admin' user, default password "PASSWORD"

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

You can leave that arrangement as-is, or you can create additional users with names of your own choice, and assign them any of the roles (and the powers that go with those roles).

Thus, you could choose to have:

- Multiple admin-level users, each with a different name

- Multiple operator-level users (or none, if you prefer), each with a different name

- Multiple monitor-level users (or none, if you prefer), each with a different name

- Multiple audit-level users (or none, if you prefer), each with a different name

> **Note:** 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. No two users (regardless of role) can have the same name.

Abilities or Privileges of Created Users

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

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

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

User accounts granted the 'audit' role are restricted to commands governing HSM audit logging functions. See "Audit Logging " on page 1 in the *Administration Guide* for more information on this specialized role.

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

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

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

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

The commands available to the roles are listed in "User Accounts and Their Privileges" on page 1.

Rationale for Creating 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 command **syslog tail** would appear in the April 13 log as:

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

Command Result : 0 (Success)
```

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

Implications of Backup and Restore of User Profiles

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

⚠️   **CAUTION:** Restoring from backup restores the database of user profiles that existed before the backup was made. 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; disabled users might be enabled; and any user accounts removed since that backup will be restored.

Your records should indicate when user-profile changes were made, and what those changes were. Any time you restore a backup, 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.

Security of Shell User Accounts

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

HSM Roles and Secrets

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

Roles

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

Mandatory Roles
- **HSM Security Officer** (**SO**): responsible for initialization of the HSM, setting and changing of HSM Policies (based on the HSM's Capabilities), creation and deletion of application partitions
- **Partition Security Officer** (**PO**): responsible for initializing the Crypto Officer role on the partition, resetting passwords, setting and changing partition-level Policies (based on the HSM's and the partition's Capabilities)
- **Crypto Officer** (**CO**): responsible for initializing the Crypto User role, and for creating and modifying cryptographic objects in the HSM partition (see "HSM Roles and Secrets" above)

Optional Roles
- **Auditor** (**Au**): responsible for managing HSM audit logging, independent from other roles on the HSM
- **Crypto User** (**CU**): responsible for using cryptographic objects (encrypt/decrypt, sign/verify…) in the HSM partition (see "HSM Roles and Secrets" above)

Secrets

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

- Cloning domain: determines whether the "cloning" (secure copy of cryptographic objects) operation is possible between two HSMs (which must share identical domain secrets) - applies to password-authenticated HSMs and to PED-authenticated HSMs; cloning is used in some forms of backup, as well as in HA

- Remote PED vector (PED-authenticated HSMs only): permits establishing a secure path for the HSM to access remotely-located Luna PED and PED keys

Enhanced Cryptoki Model

The separation of roles on the SafeNet Luna Network HSM follows an enhanced Cryptoki model:

Appliance Admin

This is the basic administrative access to a SafeNet Luna HSM appliance. When you connect via SSH (putty.exe or other SSH utility), the SafeNet 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 additional authentication. Therefore, by controlling access to passwords (for a SafeNet Luna HSM with Password Authentication) or to PED keys (for a SafeNet Luna HSM with Trusted Path Authentication), you can compartmentalize the various administrative and security roles.

HSM Security Officer (SO)

The HSM SO has control of the HSM within the SafeNet Luna Network HSM appliance. To access HSM SO 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 SO credential can:

- Create and delete partitions

- Backup and restore the HSM

- Change HSM Policies

Partition Security Officer (PO)

The Partition Security Officer has control of one or more partitions (virtual HSMs) within the SafeNet Luna Network HSM. To access Partition SO functions, you must log in using LunaCM on a registered Client computer.

The Partition SO, when logged in to the partition, can:

- Modify partition policies

- Backup and restore partition contents

- Initialize the Crypto Officer role

Crypto Officer (CO)

The Crypto Officer has full Read-Write access to the partition through the LunaCM utility on a registered Client computer. The Crypto Officer partition credential allows a Client application to perform any cryptographic operation, including:

- key generation/deletion

- wrap/unwrap

- encrypt/decrypt

- sign/verify

The Crypto Officer can also initialize the optional Crypto User role.

Crypto User (CU)

The Crypto User is a restricted Read-only Client user. Once initialized, the authenticated Crypto User can access cryptographic materials already existing on the partition (for signing, verifying, encrypting, decrypting), but cannot manipulate those objects (no generating, deleting, or wrapping/unwrapping).

The Crypto User role is optional. If you have no security requirement for this role, it can remain uninitialized and all Client applications can access the partition using the Crypto Officer credential.

Comparing Password and PED Authentication

SafeNet Luna Network HSM with PED Authentication splits the partition access into two layers, a primary and optional secondary credential. The primary credential is the secret contained on the CO or CU's PED key (and the optional PED PIN). The secondary credential is a password string, set by the CO or CU. The Partition SO can Activate a partition to allow the primary credential to be cached. Thereafter, the CO or CU (and their Client applications) can login to the partition using the secondary credential.

For SafeNet Luna Network HSM with Password Authentication, the partition password is the only layer of authentication to a partition. Therefore, any registered Client with that password has access to the partition.

Bad Login Attempts

By default, both the Crypto Officer and the Crypto User can each make 10 consecutive failed login attempts before invoking consequences.

Submissions of incorrect passwords are not counted as incorrect black PED key attempts.

> 📝 **Note:** The 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, it is not logged as a failed attempt. When you successfully login, the bad-attempt counter is reset to zero.

Domain Planning

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

- Cloning in backup and restore operations, and

- Synchronization in HA groups.

There is no provision to clone between an application partition and an HSM administrative partition, but you can apply the same domain secret for ease of administration. Password authenticated application partitions can clone partition contents one to the other, and PED authenticated application partitions can clone partition contents one to the other, but

password authenticated HSMs (and their partitions) cannot perform cloning with PED-authenticated HSMs (and their partitions).

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

Characteristics of Cloning Domains

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

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

have cloning domains in the form of encrypted secrets on red PED keys, for the HSM SO space and for any partitions that are created on the HSM.

The following characteristics are common to domains on all SafeNet Luna HSMs.

- The unique HSM SO-space domain can be created at the HSM at initialization time, or it can be imported, meaning that it is shared with one-or-more other HSMs.

- The application partition domain can be created by the current HSM when the partition is initialized, or it can be imported, meaning that it is shared with one-or-more other HSM partitions.

- The application partition domain is distinct from the HSM domain, as they are controlled by different people.

- The application partition domain can be the same as the domain of another partition on the same HSM (for HSMs that support multiple partitions).

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

In scenarios where multiple HSM partitions are in use, it can be useful to segregate those partitions according to department or business unit, or according to function groups within your organization. This ensures that personnel in a given group are able to clone or backup/restore only the contents of partitions sharing the domain for which they are responsible. The segregation is maintained by physical and procedural control of the relevant PED keys that each group is allowed to handle.

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.

Have your naming conventions and allotments planned out ahead of HSM initialization and partition creation, including a well-thought-out map of who should control cloning domain access for HSM SO spaces and for application partitions. These decisions must be made before you create the partitions.

Password-authenticated HSM Planning

Planning for configuration of a password-authenticated SafeNet Luna Network HSM is straightforward. You must determine:

- Whether the HSM authentication secrets should fall under your organization's rules for password change cycles.

- HSM and partition labels, in keeping with your organization's requirements.

- Passwords for each role:

  - HSM Security Officer (SO)

  - Partition Security Officer (PO) for each application partition

  - Crypto Officer (CO) for each application partition

  - Crypto User (CU) for each application partition (optional)

  - Auditor (Au, optional)

- Cloning domain for each partition.

HSM Initialization

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

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

The Partition SO is a completely separate role from the HSM SO. As long as they do not use the same secret, the HSM SO is completely excluded from the application partition.

HSM Cloning Domain

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

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

Crypto Officer/Crypto User

SafeNet Luna Network HSM application partitions can divide administrative and cryptographic access to the partition into an unrestricted Crypto Officer and restricted Crypto User role.

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

Application Partition Cloning Domain

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

See "Domain Planning" on page 16.

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.

PED-authenticated HSM Planning

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

- Whether the HSM authentication secrets should fall under your organization's rules for password change cycles. For example, it could be a major undertaking to change passwords for all PED keys and their backup copies every couple of months.

- Your backup policy for PED keys:

    - How many copies of each PED key should exist

    - How they should be stored (on-site and off-site)

    - Who has control of the backup copies of your HSM authentication

- HSM and partition text labels, in keeping with your organization's requirements.

- Whether it is necessary or desirable to have split-secret, multi-person access control (MofN) for any or all of the roles and secrets of the HSM.

- Whether it is necessary or desirable to invoke "something you know" secrets (PED PINs) in addition to the "something you have" PED key for any or all of the roles and secrets of the HSM.

- If PED PINs are used, how your organization's security policy deals with the departure or replacement of personnel who know the PED PINs.

- Which person or role within your organization will hold the PED key(s) and passwords for each role:

    - SO of the HSM

    - SO of each application partition

    - Crypto Officer and Crypto User

    - Auditor (optional)

    - Cloning Domain(s),

    - RPK (for optional Remote PED operation)

- How PED keys should be physically identified (which one is which copy), especially if you have invoked MofN.

PED Key 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.

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 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.

PED Prompts

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

Reuse

- **No**: You wish to have the current HSM generate a new secret and imprint it on the PED key

- **Yes**: You wish to accept an old secret from the currently inserted PED key, and imprint that secret onto the HSM

If you want this HSM to be accessed by the same secret that accesses this function/role on one or more other HSMs, reuse the PED key secret. 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. For example, you cannot tell a partition to accept a secret from a black (Crypto User) PED key if you are setting up domain.

MofN

- M=1, N=1: refuse MofN

- N > M > 1: invoke MofN

Invoking MofN splits the current secret over quantity N same-color PED keys, such that quantity M of them will always be needed to assemble the full secret and authenticate that role. You invoke MofN by providing the M value and the N value using the PED keypad, when prompted. MofN is the more secure choice, when you require multiple persons to be present (with their splits of the role secret) in order to access that role and perform its functions.

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.

- **No**: Do not overwrite what was found. Remove the key and go back to the PED prompt.

- **Yes**: Overwrite the secret on the inserted PED key.

If you say **Yes**, the PED gives you one more chance to reconsider with the prompt, "WARNING*** Are you sure...". The PED is very thorough about making sure that you do not accidentally overwrite a useful authentication secret.

PED PIN

- No: Press **Enter** on the PED keypad without entering any digits.

- Yes: Type a minimum of four digits on the PED keypad and press **Enter**.

If you type any 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).

Duplicate

- **Yes**: Duplicate the secret imprinted on the current PED key onto another PED key.

- **No**: Do not duplicate the secret.

You should always have duplicate keys for each role (or duplicate MofN sets, per role, if you chose to invoke the MofN split), so that you can have at least one off-site backup, and an on-site standby or backup set as well. Your security and operational policies will dictate how many sets you need.

HSM Initialization and the Blue SO PED Key

The first action that invokes Luna PED 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 policies 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 is rarely 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.

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

Furthermore, when you initialize an HSM with a new secret, you have the opportunity to split that secret using the MofN feature. Consider how complicated your administration and key-handling/key-update procedures should be.

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 "HSM Cloning Domain and the Red Domain PED Key" 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.

1. You must apply the same 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.

2. There is no provision to reset or change a cloning domain. An HSM domain is part of an HSM until it is reinitialized. 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 initialization process, have your red PED keys ready, either with an existing cloning domain secret to reuse, or blank (or outdated secret) to be overwritten by a unique cloning domain secret generated by the HSM. See "Domain Planning" on page 16.

Partition Security Officer Blue PED Key

The Partition SO also has a blue PED key. Once the partition is initialized, the Partition SO administers all partition policies, and initializes the Crypto Officer role. The blue PED key for a partition (or group of partitions):

• Allows the holder to log in as the Partition SO to perform administrative tasks on the partition

• Allows the holder to Activate the partition - applications can then present the partition challenge secret and make use of the partition.

When a partition is initialized and a blue PED key 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.

• 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.

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 a High Availability group. All members of an HA group must share a common cloning domain.

Before you begin the partition initialization process, have your blue PED keys ready, either with an existing Partition SO secret to reuse, or blank (or outdated secret) to be overwritten by a new Partition 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 partition is part of the partition creation process. See "HSM Cloning Domain and the Red Domain PED Key" on the previous page.

Crypto Officer Black PED Key

The Crypto Officer secret on the black PED key allows Read-Write access to the contents of the partition, for performing cryptographic operations. If the partition is Activated, the black PED key secret is cached, and applications can access the partition by providing a partition challenge secret set by the Partition SO (and subsequently changed by the CO).

Crypto User Gray PED Key

The Crypto User secret on the gray PED key allows Read-Only access to the contents of the partition, for performing cryptographic operations. If the partition is Activated, the gray PED key secret is cached, and applications can access the partition by providing a partition challenge secret set by the Crypto Officer (and subsequently changed by the CU).

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 SafeNet PED, and want to use it for remote authentication, 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 init** to create a Remote PED Vector, the PED prompt sequence is similar to the sequence for the blue or black PED keys, with the same questions about reuse, MofN, 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 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 SafeNet PED attached. See "About Remote PED" on page 1 in the *HSM Administration Guide* for directions.

Auditor White PED Key

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 initialized 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, black, or gray PED keys, with the same questions about reuse, MofN, 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.

Recommended Network Characteristics

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

Bandwidth and Latency Recommendation

Bandwidth

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

> **Note:** Ensure that your network switch is set to AUTO negotiation, as the SafeNet appliance negotiates at AUTO. If it is not, there is a risk that the switch and the SafeNet appliance will settle on a much slower speed than is actually possible in your network conditions.

Network Latency

- Maximum supported: 500ms
- Recommended: 0.5ms

Latency and Testing Troubleshooting

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

When you disconnect the network cable between any SafeNet appliance and a switch, and then reconnect, traffic should resume immediately, but with certain network switch configurations it might take 30 seconds for traffic to resume. The problem here is at the switch (not the SafeNet appliance).

If the switch is configured to run the Spanning Tree Protocol on the port, 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.

IPv6 Support and Limitations

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

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

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

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

• 128-bit IP address

• Fixed length, 40-byte header with support for new, optional Extension Headers

• Native security

• Auto-configuration

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

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

Global Unicast Address format

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

IPv6 in the Context of the SafeNet Luna Network HSM

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

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

IPv6 Address Configuration Options

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

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

IPv6 Network Gateway

IPv6 devices must use an IPv6 gateway.

IPv6 Subnet Mask (Network Mask)

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

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

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

Limitations When Using IPv6 on the SafeNet Luna Network HSM

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

Client and SafeNet Luna Network HSM must use the same IP version

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

Secure Trusted Channel (STC) links not available via IPv6

STC links are not supported over an IPv6 network. You must use NTLS to make partition-client connections via IPv6.

Single global IPv6 address per network interface

You must use a single global IPv6 address for each active network interface: eth0, eth1, eth2, and/or eth3. You must use a single global IPv6 address for each active Luna Client.

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

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

Notes:

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

2. The above table assumes that a functioning DHCPv6 server is on the network.

3. Scheme #3 ("Stateless" DHCPv6) is configured on SafeNet Luna Network HSM 7.x using SLAAC for address assignment, but DHCPv6 is still used to configure network services like DNS.

Example:

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

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

Configure the IP Address and Network Parameters

To proceed with configuring the IP address and other network parameters for the SafeNet Luna Network HSM, go to

2
Configure the SafeNet Luna Network HSM for Your Network

This chapter describes how to configure your SafeNet Luna Network HSM appliance so that you can access it over the network. This involves performing the following tasks, in the order specified:

1. "Power-up the Appliance" below
2. "Open a Connection" on the next page
3. "Logging In to the Appliance" on page 31
4. "Network Configuration" on page 32
5. "Make Your Network Connection" on page 36
6. "Set the System Date and Time" on page 37
7. "Generating the HSM Server Certificate" on page 40
8. "Binding Your NTLS or SSH Traffic to a Device" on page 41

Power-up the Appliance

Instructions on this page assume that the SafeNet Luna Network HSMappliance has been installed, including the following:

- 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.

- A connection between the HSM appliance's serial terminal port and your administration computer or a terminal. This is a recommended option, 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. See "Make Your Network Connection" on page 36.

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

Power On Instructions for the SafeNet 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 ⏻ on the front panel.
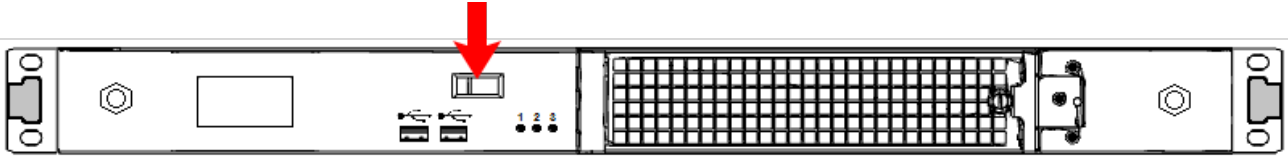
The HSM appliance begins to power up.

If power was removed while the system was on (either a power failure, or the power cable was disconnected), then the system should restart without a button press. This behavior allows unattended resumption of activity after power interruption.

The front-panel LCD begins showing activity, then settles into the ongoing system status display once the appliance has completed its boot-up and self-test activity. See "Front-panel LCD Display" on page 1 in the *Appliance Administration Guide*.

Power Off

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

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

To switch off the HSM appliance from the LunaSH command line, use the command **sysconf appliance poweroff**.

Next, see "Open a Connection" below.

Open a Connection

It is best to perform your initial configuration via direct serial connection to the SafeNet Luna Network HSM appliance. Once network parameters are established, you can switch to an SSH session over your network. However, if you are setting up your appliance on a network using DHCP, you can connect via SSH using the IP automatically assigned to the appliance's network interface.

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

• When configuring network settings via SSH, in addition to requiring the original IP address, you may lose the connection when a new IP is set.

• A direct serial connection is the only route to log into the "Recover" account, in case you ever lose the appliance's admin password and need to reset. Therefore, you should verify that the connection works before you need it - performing the appliance's network configuration is an ideal test.

• If you ever need to issue the **hsm factoryreset** command, you must be connected through a local serial console for that command to be accepted.

To open a serial connection:

1. Connect the serial port on the HSM appliance's rear panel to a terminal server, dumb terminal, PC, or laptop, using

the supplied Prolific Technology Inc. USB to RJ45 (with 8P8C connector) adapter.
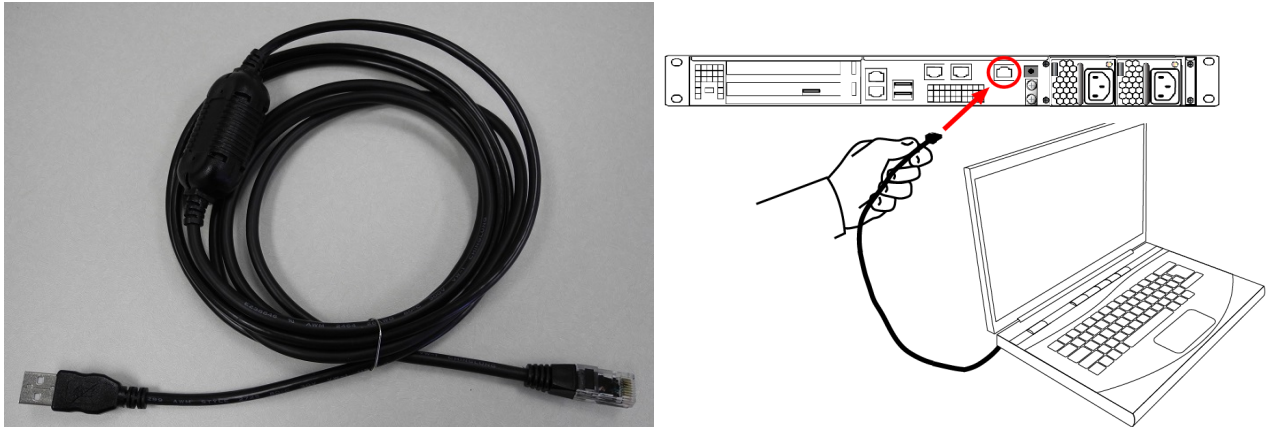
> ✍ **Note:** Do not connect the serial cable to one of the Ethernet ports.

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

3. Open **Device Manager** (**Control Panel** > **Hardware** > **Device Manager**) and expand the **Ports (COM and LPT)** folder. If the driver installed successfully, an entry is displayed for the **Prolific USB-to-Serial Comm Port**, followed by the port associated with the adapter. For example:

```
Prolific USB-to-Serial Comm Port (COM4)
```

Record the COM port (COM4 in this example) associated with the adapter. You will need this port number when you open a serial connection.

4. Use a terminal emulation package, such as PuTTY, to open a serial connection to the COM port associated with your Prolific USB-to-Serial adapter. Set the serial connection parameters as follows:

Baud rate	115200
Data bits	8
Parity	None
Stop bits	1

5. When the connection is made, the HSM appliance login prompt appears: **[local_host] login:**, where [local_host] is the currently configured host name. The displayed host name is updated when you assign a new host name to your HSM appliance and open a new session.

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

To open an SSH connection:

1. Connect one or more network devices in the rear panel of the appliance to a network with a running DHCP server.
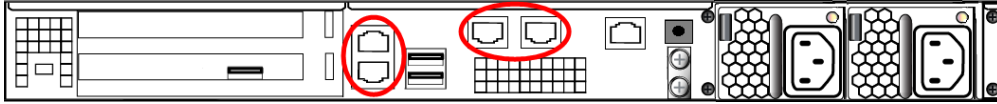
2.   Wait for the appliance to acquire a new IP address from the DHCP server. The new IP will be displayed on the front-panel LCD screen.

3.   Use SSH, or an SSH application such as PuTTY, to connect to the appliance using the displayed IP address.

Next, see "Logging In to the Appliance" below.

Logging In to the Appliance

When you open a connection to the appliance (serial or SSH) you are presented with the **login as:** prompt. By default, only the "admin" user is enabled; the other roles must be enabled by an admin user before they can login. After entering the user name and password, you are presented with the **lunash:>** prompt. The commands you are able to execute depends on the user account you logged in as, as detailed in "LunaSH Command Summary" on page 1 in the *LunaSH Command Reference Guide*.

If you are logging in to the account for the first time, use the default password, as specified below. You are immediately prompted to change it.

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)
Audit (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 **login as:** prompt, enter the name of the account you want to use. You are prompted for the password. The initial password is "PASSWORD".

> 📝   **Note:** You must login within two minutes of opening an administration session, or the connection will time out. The username and passwords are case-sensitive.

2.   For security, you are immediately prompted to change the factory-default password. 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:** If you forget your password, you can use a local serial connection to login to the Recover account. See "Forgotten Passwords/Lost Authentication" on page 1.

After successful login, the HSM appliance presents a **lunash:>** prompt. 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.

Network Configuration

The SafeNet Luna Network HSM is a network device that is intended to be installed in a data center and accessed remotely over a network. Network access to the SafeNet Luna Network HSM is provided by four 1 Gb/s Ethernet LAN ports. The SafeNet Luna Network HSM is also equipped with an RJ-45 serial port, used to provide serial access to the appliance for initial network configuration.

The network device interfaces (eth0, eth1, eth2, and eth3) and serial port are located on the rear of the appliance, as illustrated below:
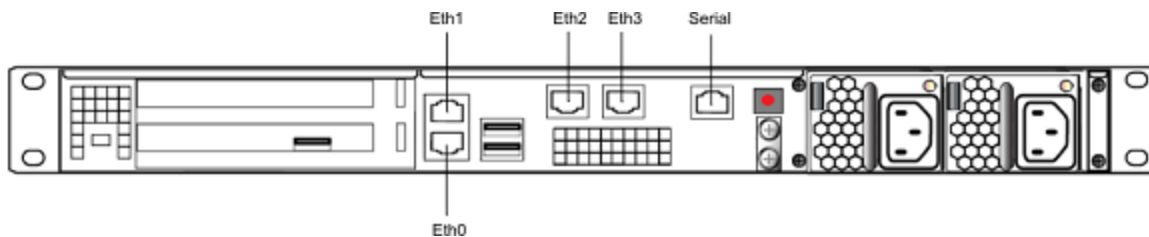
Serial port

Use the serial port to connect a serial device to the SafeNet Luna Network HSM for access to LunaSH to perform initial network configuration. You will need to use the serial port to configure at least one of the network interfaces. Once you have configured an interface, you can connect the appliance to the network and access LunaSH to complete the network configuration.

Appliance network configuration

The following network parameters are configured at the appliance level:

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

Ethernet LAN device configuration

The SafeNet Luna Network HSM is equipped with four individually-configurable 1 GB/s auto-sensing Ethernet LAN network devices. You can configure the following network settings for each device:

- IPv4 or IPv6 address. You can configure the addresses using static or DHCP addressing. If you are using IPv6 addressing, you can also use Stateless Autoconfiguration (SLAAC) to have a SLAAC-enabled router in your network automatically configure an IPv6 address on a device.

- Network gateway. IPv4 devices must use an IPv4 gateway. IPv6 devices must use an IPv6 gateway.

- Network mask. IPv4 devices must use IP address format (for example, 255.255.255.0). IPv6 devices can use full or shorthand syntax.

- Static network route.

- DNS configuration. Although you configure DNS at the device level, the settings you configure for a device are available to all devices on the appliance if the configured device is connected to the network. To ensure DNS

access, it is recommended that you configure each device. You can configure the following settings:

  – DNS nameservers. You can add up to three DNS nameservers.

  – DNS search domains.

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

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

The SafeNet Luna Network HSM supports port bonding. Port bonding allows you to create a bond between two interfaces (eth0 and eth1, or eth2 and eth3) into a single bonded interface (bond0 or bond1). In a bonded interface, both ports are bound to a virtual interface with a single IP address, with one port active and one port standby. See "SafeNet Luna Network HSM Appliance Port Bonding" on page 1 for more information.

NTLS binding: Bind NTLS traffic to a specific device

You can bind the NTLS traffic (used to securely transport cryptographic messages exchanged between a client and the HSM across the network) to a specific Ethernet device (eth0, eth1, eth2, eth3, bond0, bond1, all) on the appliance. This allows you to divide the traffic going to the appliance into cryptographic (destined for the HSM) and administrative (LunaSH) streams, for enhanced security and performance. See "Binding Your NTLS or SSH Traffic to a Device" on page 41 for more information.

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

You can optionally bind/restrict the SSH traffic (used to securely transport administrative messages across the network) to a specific Ethernet device (eth0, eth1, eth2, eth3, bond0, bond1, all) on the appliance, to the appliance hostname, or to a specific IP address. This allows you to divide the traffic going to the appliance into cryptographic (destined for the HSM) and administrative (LunaSH) streams, for enhanced security and performance. By default, SSH traffic is unrestricted. See "Binding Your NTLS or SSH Traffic to a Device" on page 41 for more information.

Gathering Appliance Network Information

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

HSM Appliance Network Parameters

• IP address and subnet mask for each LAN port you want to use (if you are using static IP addressing)

• Hostname for the HSM appliance (registered with network DNS)

• Domain name (per port)

• Default gateway IP address (per port)

• DNS Name Server IP address(es) (per port)

• Search Domain name(s) (per port)

• Device subnet mask (per port)

DNS Entries

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

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

Other Considerations

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

Configuring the Network Parameters

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

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

To configure the appliance and port network parameters:

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

Once configured, you can find the interface IP addresses on the appliance's front-panel LCD screen. If there is no IP address shown on the LCD, you must use a serial port connection to connect to the appliance.

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

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

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

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

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

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

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

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

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

2. Optional: If you wish to use the Port Bonding feature described above to configure bond0 and/or bond1 interface, use the **network interface bonding config** and **network interface bonding enable** commands. See "SafeNet Luna Network HSM Appliance Port Bonding" on page 1 for more information.

3. Optional: If desired, set the appliance hostname and domain name using the **network hostname** command. You can specify a simple hostname or a Fully Qualified Domain Name (FQDN) using the format <hostname.domainname>. If you supply a hostname that includes a space, all text after the space is ignored. For example, if you typed **network hostname my hsm** the system would assign a hostname of "my". Therefore, if you want "my hsm", use "my_hsm", "my-hsm", or similar.

   lunash:> **network hostname** <hostname>

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

4. Optional: If you wish to use the NTLS or SSH binding features described above to restrict NTLS or SSH messages to an interface (eth0, eth1, eth2, eth3, bond0, bond1, all),use the **ntls bind** or **sysconf ssh** commands. See "Binding Your NTLS or SSH Traffic to a Device" on page 41 for more information.

5. Optional: If desired, add a domain name server to the network configuration for the appliance using the **network dns add nameserver** command. The name server is added to the appliance DNS table. You can add up to three different DNS name servers to the appliance DNS table. There is one DNS table that applies to all network devices (ports) on the appliance.

> 🗎 **Note:** The domain name settings apply to static network configurations only. If you are using DHCP, the DNS name servers configured on the DHCP server are used.

When you add a DNS server, you add it to a specific network device on the appliance (eth0, eth1, eth2, eth3, bond0, bond1). When you add a DNS server to a device, it is added to the DNS table for the appliance and becomes available to all devices on the appliance, provided the device you added it to is connected to the network. For example, if you add a DNS server to eth0, all devices will be able to access the DNS server if eth0 is connected to the network. If eth0 is disconnected from the network, access to the DNS server is lost for any devices to which you did not add the DNS server. To ensure that any DNS server you add is available in the event of a network or port failure, it is recommended that you add it to all devices you will use to connect the appliance to the network.

   lunash:> **network dns add nameserver** <ip_address> **-device** <net_device>

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

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

> **Note:** The search domain settings apply to static network configurations only. If you are using DHCP, the DNS search domains configured on the DHCP server are used.

When you add a DNS search domain, you add it to a specific network device on the appliance (eth0, eth1, eth2, eth3, bond0, bond1). When you add a search domain to a device, it is added to the DNS table for the appliance and becomes available to all devices on the appliance, provided the device you added it to is connected to the network. For example, if you add a search domain to eth0, all devices will use the search domain if eth0 is connected to the network. If eth0 is disconnected from the network, the search domain is not used by any devices to which you did not add the search domain. To ensure that any search domain you add is available in the event of a network or port failure, it is recommended that you add it to all devices you will use to connect the appliance to the network.

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

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

7. View the new network settings with **network show**.

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

Make Your Network Connection

After you have configured at least one of the Ethernet LAN ports on the appliance using a serial terminal connection, you can connect the configured ports to your network and begin connecting to the appliance over the network.

To make a network connection to the appliance:

1. Connect an Ethernet cable to each Ethernet port you configured on the appliance.

2. Use SSH, or an SSH application such a s PuTTY, to connect to the appliance via one of the configured ports. For example, if you set the IP address on eth0 to 123.45.67.89, you could connect from a Linux computer using the following command:

    ```
    ssh admin@123.45.67.89
    ```

3. You will be alerted that the server's host key is not cached in the registry. Examine the fingerprint and add the key to your SSH cache to allow the connection to proceed.

4. Login as admin, using the password you configured in "Logging In to the Appliance" on page 31.

5. Verify correctness of your network setup by pinging another server (with the LunaSH **network ping** <server_name> command) and having the other server ping this HSM appliance. Try pinging by IP address, if pinging by host name is not successful. If you are using DNS name servers, but you are unable to ping by host name, use the **network show** command to verify the DNS name server configuration.

> **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.

6. Verify your client's network configuration by attempting to ping the HSM appliance by host name and by IP address, from the client. Repeat for each client where the client software was installed.

Network LEDs

The network LEDs glow or blink to indicate the exchange of traffic, as follows.

State Indicated	Indication
Activity status	**Green** (Blinking): Activity detected
	Off: Not active, or LAN cable has no connection
Speed range	**Orange**: 1G
	Green: 100M
	Off: 10M/No connection

When your connection is working, go to "Set the System Date and Time" below.

Set the System Date and Time

You can set the date and time manually using the appliance's internal clock, or by synchronizing the appliance with a network time protocol (NTP) server. NTP provides a reliable, consistent, and accurate timing mechanism using Coordinated Universal Time (UTC), and is the recommended option for providing an accurate date and time. Accurate time is important for security auditing and troubleshooting using the logs.

New HSM

When setting up a new HSM, ensure that you set the HSM server's system date, time and timezone as appropriate for your network before generating the 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.

Setting the Timezone

You must set the timezone before setting the date and time, regardless of whether you are manually configuring the date and time, or using NTP.

To set the timezone:

Use the following command:

sysconf timezone set <timezone_code>

Timezone codes

You can view a list of all available timezone codes using the **sysconf timezone list** command. See "Setting the Time Zone" on page 1 in the *Appliance Administration Guide*.

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

The code that you enter may not look exactly like the code displayed by **status date** or **status zone** commands. 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.

SO login may be required

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. This way, you can perform your intended initialization out of order, and set the appliance time and zone later. 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. However, it is important to have the time set before you create certificates later on.

Manually Configuring the Appliance Date and Time

If the SafeNet Luna Network HSM has been used before, then it might have been initialized with the option **-authtimeconfig**, which requires that the SO/HSM Admin be logged in before you are allowed to set time/timezone. If that is the case, then you will need to log in with the old SO credentials, or initialize the HSM first, before you can set time and timezone.

> 📝 **Note:** Manual adjustment of the time may cause events to appear out of order. It is highly recommended that you use NTP to synchronize the appliance time.

To set the date and time:

1. Verify the currently configured date, time, and timezone on the appliance, using the status date command. The command returns the current settings for date, time, and timezone. If desired, you can also use **status time** and **status zone**.

   lunash:> **status date**

   lunash:> **status time**

   lunash:> **status timezone**

   At the LunaSH prompt, type the command **status date**.

2. If the date, time, or timezone are incorrect for your location, change them using the following command:

   lunash:> **sysconf timezone set** <timezone>

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

   lunash:> **sysconf time** <time> [<date>]

   ```
   lunash:>sysconf time 15:54 20170427
   Thu Apr 27 15:54:00 EDT 2017
   ```

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

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, use the system's clock-drift correction protocol. See "Correcting Time Drift" on page 1 in the *Appliance Administration Guide*.

Synchronizing the Appliance With a Network Time Protocol (NTP) Server

You can optionally configure the appliance to synchronize its date and time 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. The appliance automatically selects the highest stratum NTP server with which it can reliably communicate. If the appliance loses communications with an NTP server, it automatically selects the next best available server.

> **Note:** If you wish to use Network Time Protocol (NTP), you must set the system time to within 15 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 15 minutes, the NTP daemon ignores the servers and quits. To ensure that you are within the 15-minute window, we recommend setting the date and time by fetching it from an NTP server, using the **sysconf ntp ntpdate** command.

To configure the appliance to use NTP

To use NTP, you must add one or more NTP servers to the appliance's NTP server list, and then enable the appliance to synchronize its time to the servers.

1. If you have not already done so, configure the appliance's DNS server settings. See "Network Configuration" on page 32.

2. Ensure that the correct timezone is set on the appliance:

    sysconf timezone show

    If the appliance does not have the correct timezone configured, set it before continuing. See "Setting the Timezone" on page 37.

3. You must now set the correct date and time. You can do this:

    –   manually; see "Manually Configuring the Appliance Date and Time" on the previous page

    –   by fetching it from an NTP server, using the command:

        sysconf ntp ntpdate <NTP_server_IP_or_hostname>

4. Add one or more NTP servers to the appliance's NTP server list, using the command:

    sysconf ntp addserver <NTP_server_IP_or_hostname>

    This command automatically starts the NTP service and enables time synchronization with the NTP server.

5. Verify the NTP status, using the command:

    sysconf ntp status

```
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. If the initial time-gap between your appliance and the server is greater than 15 minutes, the appliance gives up and never synchronizes with that server. If the initial time-gap is less than 15 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.

Generating the HSM Server Certificate

You must generate a new HSM server certificate before placing the HSM in service. Do not use the default certificate generated at the factory.

You can also regenerate the server certificate anytime, once the HSM is in service. If you generate a new certificate, you must update your client NTLS links to use the new certificate.

To generate a new server certificate for the SafeNet Luna Network HSM:

Use the following command in LunaSH.

sysconf regencert [**-startdate** <YYYYMMDD>] [**-days** <number_of_days>]

If your security policy requires you to change your HSM server certificates periodically, include the **-days** option to place a time limit on the certificate's validity. By default, SafeNet Luna Network HSM server certificates are valid for 3653 days (10 years).

If you want the certificate to become valid on a specific date, include the **-startdate** option. By default, the date is set to 24 hours earlier, to ensure the certificate is valid in every timezone at the time of creation.

See "sysconf regencert" on page 1 in the *LunaSH Command Reference Guide* for complete command syntax.

For example:

```
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 and STC must be (re)started before clients can connect.

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

Command Result : 0 (Success)
```

> ☑ **Note:** If your Remote PED connections are server-initiated (peer-to-peer), you must restart the Call-Back Service (CBS) anytime you regenerate the SafeNet Luna Network HSM server certificate, or new peer-to-peer PedServer connections to the appliance will fail. In LunaSH, use the command **service restart cbs**.

Binding Your NTLS or SSH Traffic to a Device

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

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

Binding Your NTLS Traffic

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

- A specific device (eth0, eth1, eth2 or eth3)
- All devices (eth0, eth1, eth2 and eth3)

- A bonded device (bond0 or bond1). See "SafeNet Luna Network HSM Appliance Port Bonding" on page 1 in the *Appliance Administration Guide* for more information.

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

- it has been configured with a valid IP address

- it is active on the network

- the NTLS service is restarted

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

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

To bind your NTLS traffic to a device

Use the **ntls bind** command: to bind the NTLS traffic to a network device (eth0, eth1, eth2, eth3, bond0, bond1, all). You can use the **ntls show** command to see the current binding.

Example

```
lunash:>ntls bind eth0

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


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

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

Starting ntls:                                          [  OK  ]

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.

```
lunash:>ntls show

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

Command Result : 0 (Success)

lunash:>ntls bind eth1

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

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

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

Starting ntls:                                              [  OK  ]

Command Result : 0 (Success)

lunash:>ntls show

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

Command Result : 0 (Success)
```

Binding Your SSH Traffic

You can optionally bind your SSH traffic a specific device (eth0, eth1, eth2, eth3, all) on the appliance or to a specific IP address. By default, SSH traffic is unrestricted.

To bind your SSH traffic to a device or IP address

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

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

```
lunash:>sysconf ssh device eth1

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

[myluna] lunash:>sysconf ssh show

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

Command Result : 0 (Success)
```

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

```
lunash:>sysconf ssh ip 192.20.10.200

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

Command Result : 0 (Success)
```

HSM Initialization

Initialization prepares a new HSM for use, or an existing HSM for reuse, as follows. You must initialize the HSM before you can generate or store objects, allow clients to connect, or perform cryptographic operations:

- On a new HSM or factory-reset HSM, initialization sets the HSM SO credentials, the HSM label, and the cloning domain of the HSM Admin partition. This is often referred to as a 'hard' initialization. See "Initializing a New or Factory-reset HSM" on the next page.

- On an existing, non-factory-reset HSM, reinitialization destroys all existing partitions and objects, but retains the SO credentials and cloning domain. You have the option to change or retain the existing label. This is often referred to as a 'soft' initialization. See "Re-initializing an Existing, Non-factory-reset HSM" on page 47.

> 📝 **Note:** To ensure accurate auditing, perform initialization only after you have set the system time parameters (time, date, timezone, use of NTP (Network Time Protocol). You can use the **-authtimeconfig** option when initializing the HSM to require HSM SO authorization of any time-related changes once the HSM is initialized.

Hard versus soft initialization

The following table summarizes the differences between a hard and soft initialization.

Condition/Effect	Soft init	Hard init
HSM SO authentication required	Yes	No
Can set new HSM label	Yes	Yes
Creates new HSM SO identity	No	Yes
Creates new Domain	No	Yes
Destroys partitions	Yes	No (none exist to destroy, since the HSM is new or an **hsm factoryreset** was performed)
Destroys objects	Yes	No (none exist to destroy, since the HSM is new or an **hsm factoryreset** was performed)

Initializing a New or Factory-reset HSM

📝 **Note:** New HSMs are shipped in Secure Transport Mode (STM). You must recover the HSM from STM before you can initialize the HSM. See "To initialize a new or factory-reset HSM (hard init)" on the next page for details.

On a new, or factory reset HSM (using **hsm factoryreset**), you perform a 'hard init' to set the following:

HSM 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. Labels cannot contain a leading space.
HSM SO credentials	For PED-authicated HSMs, you create a new HSM SO (blue) PED key(set) or re-use an existing key(set) from an HSM you want to share credentials with. If you are using PED authentication, ensure that you have a PED key strategy before beginning. See "PED Authentication" on page 1. For password-authicated HSMs, you specify the HSM SO password. For proper security, it should be different from the appliance admin password, and employ standard password-security characteristics. Password can be between 7 and 256 characters in length: • Valid characters are !#$%'*+,-./0123456789:=?@ABCDEFGHIJKLMNOPQRSTUVWXYZ[]^_abcdefghijklmnopqrstuvwxyz{}~ (the first character in that list is the space character) • Invalid characters are "&';<>\`|()
Cloning domain for the HSM Admin partition	The cloning domain is a shared identifier that makes cloning possible among a group of HSM partitions. It specifies the security domain (group of HSM partitions) within which the HSM Admin partition can share cryptographic objects though cloning, backup/restore, or in high availability configurations. Note that the HSM Admin partition cloning domain is independent of the cloning domain specified when creating application partitions on the HSM. For PED-authenticated HSMs, you create a new Domain (red) PED key(set) or re-use an existing key(set) from an HSM you want to be able to clone with. For password-authenticated HSMs, you create a new domain password or re-use an existing password from an HSM you want to be able to clone with. Cloning domain strings can be between 1 and 128 characters in length: • Valid characters are !#$%'*+,-./0123456789:=?@ABCDEFGHIJKLMNOPQRSTUVWXYZ[]^_abcdefghijklmnopqrstuvwxyz{}~ (the first character in that list is the space character) • Invalid characters are "&';<>\`|() 📝 **Note:** Always specify a cloning domain when you initialize a Password-authenticated SafeNet Luna HSM in a production environment. The HSM allows you to specify "defaultdomain" at initialization, the factory-default domain. This is deprecated, as it is insecure. Anyone could clone objects to or from such an HSM. The default domain is provided for benefit of customers who have previously used the default domain, and for migration purposes. When you prepare a SafeNet Luna HSM to go into service in a real production environment, always specify a proper, secure domain string when you initialize the HSM.

To initialize a new or factory-reset HSM (hard init)

> ⚠️ **CAUTION:** Ensure that you are prepared. Once initialized, re-initializing the HSM forces the deletion of all partitions and objects on the HSM.

1. If Secure Transport Mode is set, you must unlock the HSM before proceeding. New SafeNet Luna HSMs are shipped from the factory in Secure Transport Mode (STM). STM allows you to verify whether or not an HSM has been tampered while it is not in your possession, such as when it is shipped to another location, or placed into storage. See "Secure Transport Mode " on page 1 in the *Administration Guide* for more information.

   To recover your HSM from Secure Transport Mode, proceed as follows:

   a. As part of the delivery process for your new HSM, you should have received an email from Gemalto Client Services, containing two 16-digit strings, as follows. You will need both of these strings to recover the HSM from STM:

      Random User String: XXXX-XXXX-XXXX-XXXX

      Verification String: XXXX-XXXX-XXXX-XXXX

   b. Ensure that you have the Random User String and Verification String that were emailed to you for your new HSM.

   c. Enter the following command to recover from STM, specifying the Random User String that was emailed to you for your new HSM:

      lunash:> **hsm stm recover -randomuserstring** <XXXX-XXXX-XXXX-XXXX>

   d. You are presented with a verification string. If the verification string matches the original verification string emailed to you for your new HSM, the HSM has not been tampered, and can be safely deployed. If the verification string does not match the original verification string emailed to you for your new HSM, the HSM has been tampered while in STM. If the verification strings do not match, contact Gemalto Technical Support immediately.

   e. Enter **proceed** to recover from STM (regardless of whether the strings match or not), or enter **quit** to remain in STM.

2. If you are initializing a PED-authenticated HSM, have the Luna PED connected and ready (via USB, in Local PED-USB mode). If your PED is not in USB mode, see "Changing Menus" on page 1 in the *HSM Administration Guide*.

3. Log into LunaSH as the appliance administrator 'admin'. You can use a serial terminal window or SSH connection.

4. Run the **hsm init** command, specifying a label for your SafeNet Luna Network HSM:

   lunash:> **hsm init** <label>

5. Respond to the prompts to complete the initialization process:

   – on a password-authenticated HSM, you are prompted for the HSM password and for the HSM Admin partition cloning domain string (cloning domains for application partitions are set when the application partitions are initialized).

   – on a PED-authenticated HSM, you are prompted to attend to the PED to create a new HSM SO (blue) PED key for this HSM, re-use an HSM SO PED key from an existing HSM so that you can also use it to log in to this HSM, or overwrite an existing key with a new PED secret for use with this HSM. You are also prompted to create, re-use, or overwrite the Domain (red) PED key. You can create MofN keysets and duplicate keys as required. See "PED Authentication" on page 1 for more information.

The prompts are self explanatory. New users (especially those initializing a PED-authenticated HSM) may want to refer to the following examples for more information:

- " PED-authenticated HSM Initialization Example" below

- "Password-authenticated HSM Initialization Example" on page 52 for more information.

Re-initializing an Existing, Non-factory-reset HSM

On an existing, non-factory-reset HSM, re-initialization clears all existing partitions and objects, but retains the SO credentials and cloning domain. You have the option to change or retain the existing label. Re-initialization is also referred to as a soft init. If you do not want to do a soft init, and also change the SO credentials and cloning domain, you need to use the **hsm factoryreset** command to factory reset the HSM, and then perform the procedure described in "Initializing a New or Factory-reset HSM" on page 45.

> ⚠ **CAUTION:** Ensure you have backups for any partitions and objects you want to keep, before reinitializing the HSM.

To re-initialize an existing, non-factory-reset HSM (soft init)

1. Log in as the HSM SO.

2. If Secure Transport Mode is set, you must unlock the HSM before proceeding. See "Secure Transport Mode " on page 1 in the *Administration Guide.*

3. If you are initializing a PED-authenticated HSM, have the Luna PED connected and ready (via USB, in Local PED-USB mode). If your PED is not in USB mode, see "Changing Menus" on page 1 in the *HSM Administration Guide.*

4. Log into LunaSH as the appliance administrator 'admin'. You can use a serial terminal window or SSH connection.

5. Run the **hsm init** command, specifying a label for your SafeNet Luna Network HSM:

   lunash:> **hsm init** <label>

PED-authenticated HSM Initialization Example

This section provides detailed examples that illustrate your options when initializing a PED-authenticated HSM. It provides the following information:

- "Detailed procedure" below

- "Imprinting the Blue HSM SO PED Key" on page 49

- "Imprinting the Red Cloning Domain PED Key" on page 51

- "New, reuse, and overwrite options" on page 51

> 🗏 **Note:** Respond promptly to avoid PED timeout Error. 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 a LunaSH command that invokes the PED.

Detailed procedure

1. Your Luna PED must be connected to the HSM, either locally/directly in USB mode (see "Changing Modes" on page 1), or remotely via Remote PED connection (see "About Remote PED" on page 1).

Note: To operate in Local PED-USB mode, the PED must be connected directly to the HSM card's USB port, and not one of the other USB connection ports on the appliance.

2. When you issue the **hsm init** command, the HSM passes control to the Luna PED, and the command line (lunash:>) directs you to attend to the PED prompts.

3. A "default" login is performed, just to get started (you don't need to supply any authentication for this step).

4. Luna PED asks: "Do you wish to reuse an existing keyset?". If the answer is **No**, the HSM creates a new secret which will reside on both the HSM and the key (or keys) that is (or are) about to be imprinted. If the answer is **Yes**, then the HSM does not create a new secret and instead waits for one to be presented via the PED.

5. Luna PED requests a blue PED key. It could be blank to begin with, or it could have a valid secret from another HSM (a secret that you wish to preserve), or it could have a secret that is no longer useful.

6. Luna PED checks the key you provide. If the PED key is not blank, and your answer to "...reuse an existing keyset" was **Yes**, then Luna PED proceeds to copy the secret from the PED key to the HSM.

7. If the key is not blank, and your answer to "...reuse an existing keyset" was **No**, then the PED inquires if you wish to overwrite its contents with a new HSM secret. If the current content of the key is of no value, you say **Yes**. If the current content of the key is a valid secret from another HSM (or if you did not expect the key to hold any data) you can remove it from the PED and replace it with a blank key or a key containing non-useful data, before you answer **Yes** to the 'overwrite' question.

8. Assuming that you are using a new secret, and not reusing an existing one, Luna PED asks if you wish to split the new HSM secret. It does this by asking for values of "M" and "N". You set those values to "1" and "1" respectively, unless you require MofN split-secret, multi-person access control for your HSM (See "MofN Split Secret Keys" on page 1 for details).

9. Luna PED asks if you wish to use a PED PIN (an additional secret; see "Using the PED" on page 1 for more info).

10. If you just press **Enter** (effectively saying 'no' to the PED PIN option), then the secret generated by the HSM is imprinted on the PED key, that same secret is retained as-is on the HSM, and the same secret becomes the piece needed to unlock the Security Officer/HSM Admin account on the HSM.

11. If you press some digits on the PED keypad (saying 'yes' to the PED PIN option), then the PED combines the HSM-generated secret with your PED PIN and feeds the combined data blob to the HSM. The HSM throws away the original secret and takes on the new, combined secret as its SO/HSM Admin secret.

12. The PED key contains the original HSM-generated secret, but also contains the flag that tells the PED whether to demand a PED PIN (which is either no digits, or a set of digits that you supplied, and must supply at all future uses of that PED key).

13. Luna PED gives you the option to create some duplicates of this imprinted key. You should make at least one duplicate for backup purposes. Make additional duplicates if your security policy permits, and your procedures require them.

14. Next, Luna PED requests a red Domain PED key. The HSM provides a cloning Domain secret and the PED gives you the option to imprint the secret from the HSM, or to use a domain that might already be on the key. You choose appropriately. If you are imprinting a new Domain secret, you have the same opportunities to split the secret, and to apply a PED PIN "modifier" to the secret. Again, you are given the option to create duplicates of the key.

15. At this point, the HSM is initialized and Luna PED passes control back to LunaSH.

Further actions are needed to prepare for use by your Clients, but you can now log in as SO/HSM Admin and perform HSM administrative actions.

Imprinting the Blue HSM SO PED Key

1.   Decide if you want to reuse a keyset.

```
SLOT 01
SETTING SO PIN...
Would you like to
reuse an existing
keyset? (Y/N)
```
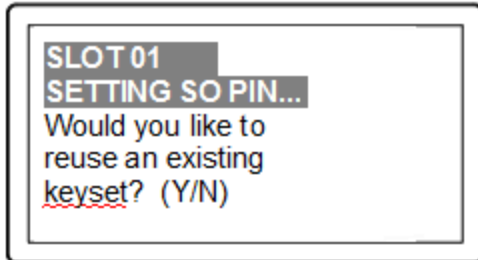
–   If you say **No** (on the PED keypad), then you are indicating there is nothing of value on your PED keys to preserve, or you are using blank keys.

–   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.

2.   Set MofN.

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

>00                        >00
```
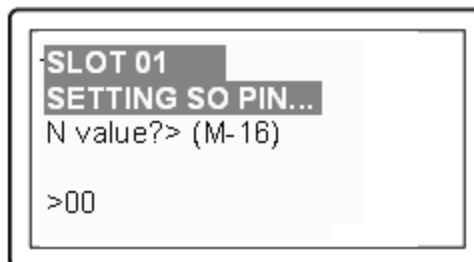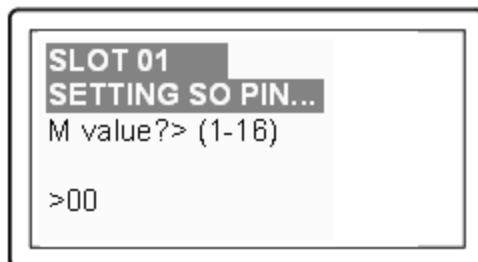
–   Setting M and N to **1** means that the authentication is not to be split, and only a single PED key will be necessary when the authentication is called for in future. Input **1** for each prompt if you do not want to use MofN.

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

3.   Insert your blank key or the key you wish to overwrite.

```
SLOT 01
SETTING SO PIN...
Insert another SO /
HSM Admin
PED Key (BLUE).
Press ENTER.
```
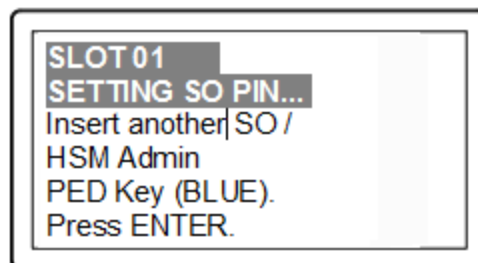
Insert a blue HSM Admin/SO PED key and press **Enter**.

```
SLOT 01
SETTING SO PIN...
****WARNING****
This PED Key is
blank.
Overwrite?  YES/NO
```
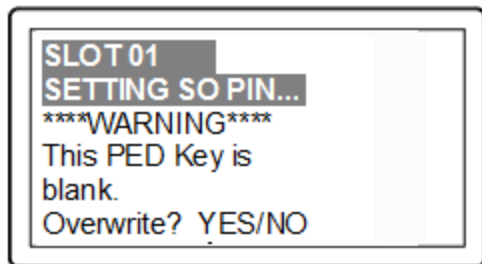
- **Yes**: If the PED should overwrite the PED key with a new SO authentication.
  If you overwrite a PED key that contains authentication secret for another HSM, then this PED key will no longer be able to access the other HSM, only the new HSM that you are currently initializing with a new, unique authentication secret .

- **No**: If you have changed your mind or inserted the wrong PED key.

4. 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:
```
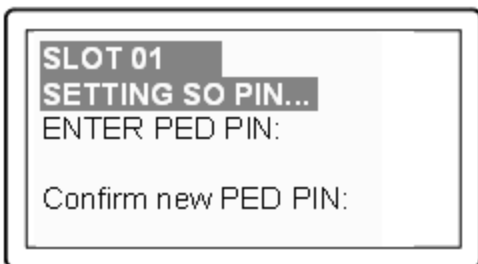
Type a numeric password on the PED keypad, if you wish. Otherwise, just press **Enter** twice to indicate that no PED PIN is desired.

5. Decide if you want to duplicate your keyset.

```
SLOT 01
SETTING SO PIN...

Are you duplicating
this keyset? (Y/N)
```
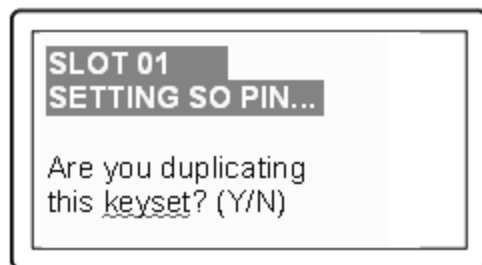
- **Yes**: Present one or more blank keys, all of which will be imprinted with exact copies of the current PED key's authentication.

- **No**: Do not make any copies.

> **Note:** You should always have backups of your imprinted PED keys, to guard against loss or damage.

Imprinting the Red Cloning Domain PED Key

To begin imprinting a Cloning Domain (red PED key), you must first log into the HSM. Insert your blue SO PED key.

1.   Decide if you want to reuse a keyset.
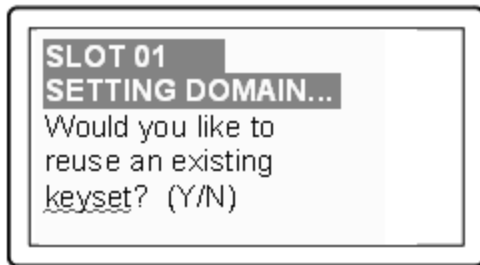
- **No**: If this is your first SafeNet Luna HSM, or if this HSM will not be cloning objects with other HSMs that are already initialized
- **Yes**: If you have another HSM and wish that HSM and the current HSM to share their cloning Domain.

2.   Set MofN.

3.   Insert your blank key or the key you wish to overwrite.

4.   Optionally set a PED PIN.

5.   Decide if you want to duplicate your keyset.

Once you stop duplicating the Domain key, or you indicate that you do not wish to make any duplicates, Luna PED goes back to "Awaiting command...". LunaSH says:

```
Command Result : No Error
```

New, reuse, and overwrite options

The table below summarizes the steps involving Luna PED immediately after you invoke the command **hsm init**. The steps in the table are in the order in which they appear as PED prompts, descending down the column.

The first column is the simplest, and most like what you would encounter the very first time you initialize, using "fresh from the carton" 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 "About the Luna PED" on page 1) or, to overwrite what is found and generate a new secret to be imprinted on both the PED key and the HSM.

New PED Keys	Existing PED Keys (Reuse)	Existing PED Keys (Overwrite)
SLOT 01 SETTING SO PIN… Would you like to reuse an existing keyset? (Y/N) **No**	SLOT 01 SETTING SO PIN… Would you like to reuse an existing keyset? (Y/N) **Yes**	SLOT 01 SETTING SO PIN… Would you like to reuse an existing keyset? (Y/N) **No**
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.

New PED Keys	Existing PED Keys (Reuse)	Existing PED Keys (Overwrite)
This PED Key is blank. Overwrite? (YES/NO) **Yes**	****Warning!**** This PED Key is for SO / HSM Admin Overwrite? (YES/NO) **No**	****Warning!**** This PED Key is for SO / HSM Admin Overwrite? (YES/NO) **Yes**
Enter a new PED PIN Confirm new PED PIN • Press **Enter** for no PED PIN • Input 4-16 digits on the PED keypad	Enter a new PED PIN Confirm new PED PIN • Press **Enter** for no PED PIN • Input 4-16 digits on the PED keypad	Enter a new PED PIN Confirm new PED PIN • Press **Enter** for no PED PIN • Input 4-16 digits on the PED keypad
Are you duplicating this keyset? YES/NO • **Yes**: duplicate. This option can be looped for as many duplicates as you need • **No**: do not duplicate	Are you duplicating this keyset? YES/NO • **Yes**: duplicate. This option can be looped for as many duplicates as you need • **No**: do not duplicate	Are you duplicating this keyset? YES/NO • **Yes**: duplicate. This option can be looped for as many duplicates as you need • **No**: do not duplicate
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
SETTING DOMAIN... Would you like to reuse an existing keyset? (Y/N) • **Yes** (unless you have good reason to create a new domain)	SETTING DOMAIN... Would you like to reuse an existing keyset? (Y/N) • **Yes**: make this HSM part of an existing domain • **No**: create a new domain for this HSM	SETTING DOMAIN... Would you like to reuse an existing keyset? (Y/N) • **Yes**: make this HSM part of an existing domain • **No**: create a new domain for this HSM

Password-authenticated HSM Initialization Example

```
lunash:>hsm init -label myLunaHSM

  Please enter a password for the HSM Administrator:
  > ********

  Please re-enter password to confirm:
  > ********

  Please enter a cloning domain to use for initializing this HSM:
  > *********

  Please re-enter cloning domain to confirm:
  > *********

CAUTION:  Are you sure you wish to initialize this HSM?

          Type 'proceed' to initialize the HSM, or 'quit'
```

```
        to quit now.
        > proceed

'hsm init' successful.

Command Result : 0 (Success)
```

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

Set the HSM 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 in LunaSH with the **hsm changepolicy** command.

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

Set HSM Policies (Password Authentication)

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

> ✎ **Note:** 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:    myLunaHSM
    Serial #:     66331
    Firmware:     7.0.1

    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                           Disallowed
    Enable cloning                           Allowed
    Enable full (non-backup) functionality   Allowed
```

```
Enable non-FIPS algorithms             Allowed
Enable SO reset of partition PIN       Allowed
Enable network replication             Allowed
Enable Korean Algorithms               Disallowed
FIPS evaluated                         Disallowed
Manufacturing Token                    Disallowed
Enable forcing user PIN change         Allowed
Enable portable masking key            Allowed
Enable partition groups                Disallowed
Enable remote PED usage                Disallowed
HSM non-volatile storage space         33554432
Enable unmasking                       Allowed
Maximum number of partitions           100
Enable Single Domain                   Disallowed
Enable Unified PED Key                 Disallowed
Enable MofN                            Disallowed
Enable small form factor backup/restore  Disallowed
Enable Secure Trusted Channel          Allowed
Enable decommission on tamper          Allowed
Enable partition re-initialize         Disallowed
Enable low level math acceleration     Allowed
Enable Fast-Path                       Disallowed
Allow Disabling Decommission           Allowed
Enable Tunnel Slot                     Disallowed
Enable Controlled Tamper Recovery      Allowed


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

Description                       Value
===========                       =====
PIN-based authentication          True


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

Changing policies marked "destructive" will erase all HSM partitions
on the HSM.

IMPORTANT NOTE: Changing policy 46 (Disable Decommission) will erase
all partitions AND zeroize your HSM.

Description                            Value     Code      Destructive
===========                            =====     ====      ===========
Allow cloning                          On        7         Yes
Allow non-FIPS algorithms              On        12        Yes
SO can reset partition PIN             Off       15        Yes
Allow network replication              On        16        No
Force user PIN change after set/reset  On        21        No
Allow offboard storage                 On        22        Yes
Allow unmasking                        On        30        No
Current maximum number of partitions   100       33        No
Allow Secure Trusted Channel           Off       39        No
Decommission on tamper                 Off       40        Yes
Allow low level math acceleration      On        43        No
Disable Decommission                   Off       46        Yes
Do Controlled Tamper Recovery          On        48        No


Command Result : 0 (Success)
```

According to the above example, the fixed capabilities require that this HSM be protected with HSM Password Authentication. This means 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 Luna HSM is designed to the standard, but can permit activation of additional non-FIPS-validated algorithms if your application requires them. An auditor would not validate your configuration unless the set of available algorithms is restricted to the approved subset.

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

```
lunash:>hsm login

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

'hsm login' successful.

Command Result : 0 (Success)
```

3. To modify a policy setting, type the **hsm changepolicy** command:

> **WARNING! This example is a change to a destructive policy, meaning that if you apply this policy, the HSM is zeroized and all contents are lost. This is not an issue when you have just initialized an HSM.**

```
lunash:>hsm changepolicy -policy 12 -value 0

        Changing this policy will result in erasing all partitions
        on the HSM.

        Type 'proceed' to erase all partitions or 'quit' to quit now.
        >proceed
'hsm changePolicy' successful.

Policy Allow non-FIPS algorithms is now set to value: 0

Command Result : 0 (Success)
```

Destructive Change of HSM Policy

The above example is a change to a destructive policy. This means 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 SafeNet Luna HSM has been in a "live" or "production" environment and contains useful or important data, keys, certificates.

Backup any important HSM or partition contents before making any destructive policy change, and then restore from backup after the HSM is re-initialized and the partition re-created.

Refer to "Capabilities and Policies" on page 1 in the *HSM Administration Guide* for a description of all policies and their meanings.

Set HSM Policies - PED Authentication

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

> 📝 **Note:** 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:    myLunaHSM
    Serial #:     532018
    Firmware:     7.0.1

    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                      Disallowed
    Enable cloning                      Allowed
    Enable full (non-backup) functionality    Allowed
    Enable non-FIPS algorithms          Allowed
    Enable SO reset of partition PIN    Allowed
    Enable network replication          Allowed
    Enable Korean Algorithms            Disallowed
    FIPS evaluated                      Disallowed
    Manufacturing Token                 Disallowed
    Enable forcing user PIN change      Allowed
    Enable portable masking key         Allowed
    Enable partition groups             Disallowed
    Enable remote PED usage             Allowed
    HSM non-volatile storage space      33554432
    Enable unmasking                    Allowed
    Maximum number of partitions        100
    Enable Single Domain                Disallowed
    Enable Unified PED Key              Disallowed
    Enable MofN                         Allowed
    Enable small form factor backup/restore   Disallowed
    Enable Secure Trusted Channel       Allowed
    Enable decommission on tamper       Allowed
    Enable partition re-initialize      Disallowed
    Enable low level math acceleration  Allowed
    Enable Fast-Path                    Disallowed
    Allow Disabling Decommission        Allowed
    Enable Tunnel Slot                  Disallowed
    Enable Controlled Tamper Recovery   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


    The following policies describe the current configuration of
    this HSM and may be changed by the HSM Administrator.
    Changing policies marked "destructive" will erase all HSM partitions
    on the HSM.

    IMPORTANT NOTE: Changing policy 46 (Disable Decommission) will erase
    all partitions AND zeroize your HSM.

    Description                            Value      Code      Destructive
    ===========                            =====      ====      ===========
    Allow cloning                          On         7         Yes
    Allow non-FIPS algorithms              On         12        Yes
    SO can reset partition PIN             Off        15        Yes
    Allow network replication              On         16        No
    Force user PIN change after set/reset  On         21        No
    Allow offboard storage                 On         22        Yes
    Allow remote PED usage                 On         25        No
    Allow unmasking                        On         30        No
    Current maximum number of partitions   100        33        No
    Allow MofN                             On         37        No
    Allow Secure Trusted Channel           Off        39        No
    Decommission on tamper                 Off        40        Yes
    Allow low level math acceleration      On         43        No
    Disable Decommission                   Off        46        Yes
    Do Controlled Tamper Recovery          On         48        No

Command Result : 0 (Success)
```

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

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

> **Note:** The FIPS 140-2 standard mandates a set of security factors that specify a restricted suite of cryptographic algorithms. The HSM is designed to the standard, but can permit activation of additional non-FIPS-validated algorithms if your application requires them. An auditor would not validate your configuration unless the set of available algorithms is restricted to the approved subset.

2. To change HSM policies, the HSM SO must first login with **hsm login**.

    Control is passed to the PED, which prompts you for the blue PED key. Input the appropriate PED key for this HSM, and press **Enter** on the PED keypad.

3. To modify a policy setting, type the **hsm changepolicy** command:

> ⚠ **WARNING! This example is a change to a destructive policy, meaning that if you apply this policy, the HSM is zeroized and all contents are lost. This is not an issue when you have just initialized an HSM.**

```
lunash:>hsm changepolicy -policy 12 -value 0

        Changing this policy will result in erasing all partitions
        on the HSM.

        Type 'proceed' to erase all partitions or 'quit' to quit now.
        >proceed
'hsm changePolicy' successful.

Policy Allow non-FIPS algorithms is now set to value: 0

Command Result : 0 (Success)
```

Destructive Change of HSM Policy

The above example is a change to a destructive policy. This means 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 SafeNet Luna HSM has been in a "live" or "production" environment and contains useful or important data, keys, certificates.

Backup any important HSM or partition contents before making any destructive policy change, and then restore from backup after the HSM is re-initialized and the partition re-created.

Refer to "Capabilities and Policies" on page 1 in the *HSM Administration Guide* for a description of all policies and their meanings.

Create Application Partitions

When you have initialized and configured the HSM, you are ready to create and configure application partitions, as described in this chapter.

SafeNet Luna Network HSMs have two types of partition spaces:

• HSM administrative partition - where HSM-wide policies are set and changed, application partitions are created/destroyed, HSM firmware and capabilities are updated, etc.

• Application partition - where cryptographic operations are performed by your applications

The high-level steps are summarized below, to go from a new or factory-reset HSM to having a configured application partition, ready for keys and objects and cryptographic operations. Normally, each set of actions is performed by a different person with different responsibilities.

HSM Security Officer (SO)

1. Initialize the HSM; this initializes the HSM SO role and the cloning domain for the HSM (see "HSM Initialization" on page 44).

2. Login as HSM SO.

3. Create the empty application partition.

4. Complete the certificate exchanges and registrations necessary to create the secure link between Client and application partitions on the appliance.

Partition Security Officer (PO)

1. Set the active slot to the newly created application partition.

2. Initialize the partition; this initializes the Partition SO role and the cloning domain for the partition.

3. Log into the application partition as Partition SO.

4. Initialize the Crypto Officer role.

5. Log out.

Partition Crypto Officer (CO)

1. Set the active slot to the initialized application partition.

2. Log into the application partition as Crypto Officer.

3. [Optional] Initialize the Crypto User role.

Next Steps

> **Note:** Before you begin configuring and initializing a PED-authenticated SafeNet Luna Network HSM, we recommend that you familiarize yourself with the PED by reviewing "PED Authentication" on page 1.

• For PED-authenticated SafeNet Luna Network HSM, the first step is to initialize the HSM; see "Creating a PED-Authenticated Partition" on page 63.

• For Password-authenticated SafeNet Luna Network HSM, the first step is to initialize the HSM; see "Creating a Password-Authenticated Partition" below.

Creating a Password-Authenticated Partition

An application owner/user has requested an application partition on the HSM, in which applications will run cryptographic operations. These instructions are the actions to be taken by the HSM Security Officer or SO. These instructions assume you are using a Password-authenticated SafeNet Luna Network HSM.

The SafeNet Luna Network HSMis initially accessed via SSH, and LunaSH is used to create the partition. After the partition is created, administrative access to that partition moves to a host computer where SafeNet Luna HSM Client software is installed, and where administrative actions are carried out through a Network Trust Link (NTL) or Secure Trusted Channel (STC) via the LunaCM tool.

Requirements

You will need:

• The appliance configured for network operation and server certificate created.

• SafeNet Luna Network HSM and your application host computer having exchanged certificates.

• The HSM in initialized state.

Create the Partition

1. Login to the SafeNet Luna Network HSM as HSM SO.

```
lunash:>hsm login

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

'hsm login' successful.

Command Result : 0 (Success)
```

2. Use the **partition create** command to create a new partition, specifying at least a partition name. Other command parameters are available. See "partition create" on page 1 in the *LunaSH Command Reference Guide* for details.

```
lunash:>partition create -partition LunaPar1

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

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

3. Verify that the partition has been created.

```
lunash:>hsm show

    Appliance Details:
    ==================
    Software Version:               7.0.0

    HSM Details:
    ============
    HSM Label:                      myLunaHSM
    Serial #:                       66331
    Firmware:                       7.0.1
    HSM Model:                      Luna K7
    HSM Part Number:                808-000048-002
    Authentication Method:          Password
    HSM Admin login status:         Logged In
    HSM Admin login attempts left:  3 before HSM zeroization!
    RPV Initialized:                No
    Audit Role Initialized:         No
    Remote Login Initialized:       No
    Manually Zeroized:              No
    Secure Transport Mode:          No
    HSM Tamper State:               No tamper(s)

    Partitions created on HSM:
    ==============================
    Partition:        154438865287, Name: LunaPar1
    Number of partitions allowed:   100
    Number of partitions created:   1

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

    HSM Storage Information:
    ========================
    Maximum HSM Storage Space (Bytes):  33554432
    Space In Use (Bytes):               335544
    Free Space Left (Bytes):            33218888

    Environmental Information on HSM:
    =================================
    Battery Voltage:                3.072 V
    Battery Warning Threshold Voltage:  2.750 V
    System Temp:                    36 deg. C
    System Temp Warning Threshold:  75 deg. C

Command Result : 0 (Success)
```

The partition now exists, and all future configuration and management of that partition will be handed over to the person who is to become the Partition SO. Once the partition is initialized, the HSM SO's administrative access is limited to the following actions:

• resizing the partition

• deleting the partition

• backing up the partition contents

- restoring the contents of the partition from backup

The Partition SO (and any additional roles that are created for the partition) performs all configuration and management actions on the partition, using LunaCM via a client connection.

The next step, depending on your configuration, is one of the following:

- "Create a Network Trust Link - Multi-step setup" on page 67
- "Create a Network Trust Link - One-Step Setup" on page 71

Creating a PED-Authenticated Partition

An application owner/user has requested an application partition on the HSM, in which applications will run cryptographic operations. These instructions are the actions to be taken by the HSM Security Officer or SO. These instructions assume you are using a PED-authenticated SafeNet Luna Network HSM.

The SafeNet Luna Network HSM is initially accessed via SSH, and LunaSH is used to create the partition. After the partition is created, administrative access to that partition moves to a host computer where SafeNet Luna HSM Client software is installed, and where administrative actions are carried out through a Network Trust Link (NTL) or Secure Trusted Channel (STC) via the LunaCM tool.

Requirements

You will need:

- The appliance configured for network operation and server certificate created.
- SafeNet Luna Network HSM and your application host computer having exchanged certificates.
- The HSM in initialized state.
- A Luna PED and PED keys with labels.
- Local physical access to your SafeNet Luna Network HSM appliance for local PED connection, an already-imprinted RPK (orange PED key) with your Luna PED remotely connected. See "Remote PED Setup and Configuration" on page 1 and "Using Remote PED" on page 1.

Preparation

If you are using a Luna PED connected locally to the SafeNet Luna Network HSM, skip to "Create the Partition" on the next page below.

1. If necessary, have a Luna PED connected to a host computer (can be the same computer that acts as your SafeNet Luna HSM Client, but can be another host if desired), with the PED set to "Remote PED mode," and an orange PED key ready containing the same RPV as your SafeNet Luna Network HSM.

2. On the host computer, launch **PedServer.exe**.

```
C:\Program Files\SafeNet\LunaClient>pedserver -mode start -ip 192.20.10.217 -port 1503
Ped Server Version 1.0.6 (10006)

Failed to load configuration file.  Using default settings.

Ped Server launched in startup mode.
Starting background process
Background process started
Ped Server Process created, exiting this process.
```

```
C:\Program Files\SafeNet\LunaClient>pedserver -mode show
Ped Server Version 1.0.6 (10006)

Failed to load configuration file.  Using default settings.

Ped Server launched in status mode.
failed to unlock: GetLastError(): 183 0xb7

    Server Information:
        Hostname:                    MyRPEDhost
        IP:                          192.20.10.217
        Firmware Version:            2.7.1-0
        PedII Protocol Version:      1.0.1-0
        Software Version:            1.0.6 (10006)

        Ped2 Connection Status:      Connected
        Ped2 RPK Count               0
        Ped2 RPK Serial Numbers      (none)

    Client Information:              Not Available

    Operating Information:
        Server Port:                 1503
        External Server Interface:   Yes
        Admin Port:                  1502
        External Admin Interface:    No

        Server Up Time:              52 (secs)
        Server Idle Time:            52 (secs) (100%)
        Idle Timeout Value:          1800 (secs)

        Current Connection Time:         0 (secs)
        Current Connection Idle Time:    0 (secs)
        Current Connection Total Idle Time: 0 (secs) (100%)
        Total Connection Time:           0 (secs)
        Total Connection Idle Time:      0 (secs) (100%)

    Show command passed.

C:\Program Files\SafeNet\LunaClient>
```

3. On the SafeNet Luna Network HSM, start the PED Client service, pointing to the PedServer that you just started.

```
[mynethsm] lunash:>hsm ped connect -ip 192.20.10.217 -port 1503

Luna PED operation required to connect to Remote PED - use orange PED key(s).

Command Result : 0 (Success)
```

Create the Partition

1. Login to the SafeNet Luna Network HSM as HSM SO.

```
lunash:>hsm login

Luna PED operation required to login as HSM Administrator - use Security Officer (blue) PED
key.
```

```
'hsm login' successful.

Command Result : 0 (Success)
```

2. Use the **partition create** command to create a new partition, specifying at least a partition name. Other command parameters are available. See "partition create" on page 1 in the *LunaSH Command Reference Guide* for details.

```
lunash:>partition create -partition LunaPar1

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

Command Result : 0 (Success)
```

3. Verify that the partition has been created.

```
lunash:>hsm show

    Appliance Details:
    ==================
    Software Version:               7.0.0

    HSM Details:
    ===========
    HSM Label:                      myLunaHSM
    Serial #:                       532018
    Firmware:                       7.0.1
    HSM Model:                      Luna K7
    HSM Part Number:                808-000048-002
    Authentication Method:          PED keys
    HSM Admin login status:         Logged In
    HSM Admin login attempts left:  3 before HSM zeroization!
    RPV Initialized:                No
    Audit Role Initialized:         No
    Remote Login Initialized:       No
    Manually Zeroized:              No
    Secure Transport Mode:          No
    HSM Tamper State:               No tamper(s)

    Partitions created on HSM:
    ==============================
    Partition:       154438865287, Name: LunaPar1

    Number of partitions allowed:   100
    Number of partitions created:   1

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

    HSM Storage Information:
    ========================
    Maximum HSM Storage Space (Bytes):  33554432
    Space In Use (Bytes):               335544
    Free Space Left (Bytes):            33218888

    Environmental Information on HSM:
    ================================
    Battery Voltage:                3.093 V
```

```
      Battery Warning Threshold Voltage:    2.750 V
      System Temp:                          40 deg. C
      System Temp Warning Threshold:        75 deg. C

Command Result : 0 (Success)
```

The partition now exists, and all future configuration and management of that partition will be handed over to the person who is to become the Partition SO. Once the partition is initialized, the HSM SO's administrative access is limited to the following actions:

- resizing the partition

- deleting the partition

- backing up the partition contents

- restoring the contents of the partition from backup

The Partition SO (and any additional roles that are created for the partition) performs all configuration and management actions on the partition, using LunaCM via a client connection.

The next step, depending on your configuration, is one of the following:

Create a Network Trust Link Between the Client and the Appliance

The first step in preparing your clients to use the cryptographic resources provided by the HSM appliance is to create a secure Network Trust Link (NTL) between the client and the appliance. After you create the NTL link between the client and the appliance, you can configure links to individual partitions on the appliance using NTL or Secure Trusted Channel (STC), as described in "Enable the Client to Access a Partition" on page 73.

About Network Trust Links

Network Trust Links (NTL) are secure, authenticated network connections between the SafeNet Luna Network HSM and Clients. NTLs use two-way digital certificate authentication and TLS data encryption (version 1.2 is supported in SafeNet Luna Network HSM 6.1) to protect sensitive data as it is transmitted between HSM Partitions on the SafeNet Luna Network HSM and Clients. NTLs consist of the following parts:

- Network Trust Link Service (NTLS): NTL server daemon runs on the SafeNet Luna Network HSM appliance and manages the NTL connections to the appliance. NTL uses port 1792 on the SafeNet Luna Network HSM appliance.

- Network Trust Link Agent (NTLA): NTL agent runs on a SafeNet Luna HSM client workstation and manages the NTL connections to the workstation. The NTL agent is included in the SafeNet Luna HSM client software.

- Network Trust Link itself: an encrypted, secure communications channel between the Client's NTLA and the HSM appliance's NTLS.

Network Trust Links use digital certificates to verify the identities of connecting clients. During the initial HSM appliance configuration (see "Generating the HSM Server Certificate" on page 40), the appliance administrator generated a unique certificate that identifies the HSM appliance. Similarly, each Client must generate its own certificate that identifies it uniquely. Both the Client and the HSM appliance use these certificates to verify the other's identity before an NTL is created between them.

In this chapter, we setup a network trust link between a Luna Client and an application partition on a SafeNet Luna Network HSM. You can use either of the following methods:

"Create a Network Trust Link - Multi-step setup" below

"Create a Network Trust Link - One-Step Setup" on page 71

Create a Network Trust Link - Multi-step setup

To create an Network Trust Link (NTL), the Client and HSM appliance must first exchange certificates. Once the certificates have been exchanged, the Client registers the SafeNet Luna Network HSM's certificate in a trust list, and the SafeNet Luna Network HSM appliance, in turn, registers the Client's certificate in its list of clients. When the certificates have been exchanged and registered at each end, the NTL is ready to use.

"Ready to use" means that an application at the client host (such as LunaCM or your crypto-using application) can see the registered SafeNet Luna Network HSM application partitions as slots in the client slot list, can select such

registered partitions by slot number, and can then perform cryptographic operations in those slots after providing appropriate partition authentication (Crypto Officer, Crypto User).

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

To create a network trust link:

You must have administrator access to perform this procedure. Read/write access to the SafeNet Luna HSM client installation directory is required for the certificate exchange.

1. Prepare the client workstation:

   a. Install the SafeNet Luna HSM client software. See "SafeNet Luna HSM Client Software Installation " on page 1 in the *Installation Guide* for details.

   b. Install an SSH client to provide secure shell access to the SafeNet appliance for certificate exchange and registration. The PuTTY SSH client (putty.exe) is included in the SafeNet Luna HSM client for Windows.

   c. Ensure that the client workstation has network access to the SafeNet Luna Network HSM appliance. The appliance auto-negotiates network bandwidth up to Gigabit Ethernet speeds. See "Recommended Network Characteristics" on page 24 for more information.

2. Open a SafeNet Luna HSM client session:

   a. Open a command prompt or terminal window.

   b. Go to the SafeNet Luna HSM client installation directory:

Windows	C:\Program Files\SafeNet\LunaClient
Linux/AIX	/usr/safenet/lunaclient/bin
Solaris/HP-UX	/opt/safenet/lunaclient/bin

3. Use **pscp** (Windows) or **scp** (Linux/UNIX) to import the HSM Appliance Server Certificate (**server.pem**) from the SafeNet Luna Network HSM appliance to the SafeNet Luna HSM client workstation. See "Using the scp and pscp Utilities" on page 1 for details. You require the SafeNet Luna Network HSM appliance admin password to complete this step.

If you are importing multiple SafeNet Luna Network HSM appliances' certificates to a client, we suggest that you import the certificates and process each one as it arrives. The **vtl addServer** command (just ahead) copies, moves and renames the current server.pem certificate to reflect the originating appliance's hostname or IP address, as appropriate, and you are always assured that the certificates that are registered in the .\cert\server folder are unique. In this method, each appliance server cert arrives in the SafeNet Luna HSM Client folder as (the default) "server.pem" and is safely registered uniquely (in the server cert folder) before the next server.pem arrives and overwrites any earlier version.

If you prefer to import server.pem certificates from multiple appliances, before registering them, then you must rename them as they arrive, to avoid overwriting and losing certificates that all arrive in the same folder with the same default filename.

Windows	**Syntax: pscp** [options] <user>@<host>:<source_filename> <target_filename>
	Example: To copy the server certificate from host myHSM to the current (.) directory, keeping the same name:
	`pscp admin@myHSM:server.pem .`

	```admin@myHSM's password:``` ```server.pem	1 kB	1.1 kB/s	ETA: 00:00:00	100%```

Linux/UNIX	**Syntax:scp** [options] <user>@<host>:<source_filename> <target_filename>
	
	Example: To copy the server certificate from host IP 192.168.0.123 to the current (.) directory, keeping the same name:
	
	```scp admin@192.168.0.123:server.pem .```
	```admin@192.168.0.123's password:```
	``server.pem
		1 kB	1.1 kB/s	ETA: 00:00:00	100%```

You must accept the SSH certificate the first time you open an scp or SSH link. You can use the LunaSH command **sysconf fingerprint ssh** to check the certificate fingerprint.

If the HSM appliance IP or hostname is changed, SSH will detect a mismatch in the HSM appliance's server certification information and warn you of a potential security breach. To resolve this issue, delete the server's certificate information from the client's known host file at: /<user home dir>**/.ssh/known_hosts2**, and re-import the server certificate.

> 📝 **Note:** On Windows, if the certificate fails to copy (but no error message appears), ensure the client machine is running with Administrator privileges. Alternatively, open the **cmd** prompt by right-clicking and selecting "Run as Administrator".

4. Register the HSM Server Certificate with the client, using the **vtl addserver** command. See "VTL" on page 1 in the *Utilities Reference Guide* for full command syntax. The **vtl** command is not interactive. It is called from the command line or a shell prompt, completes its current task, and exits back to the shell:

    vtl addServer -n <Network_HSM_hostname_or_IP> **-c** <server_certificate>

    If using a host name, ensure that the name you use is reachable over the network (**ping** <hostname>). To avoid network issues, it is recommended that you specify an IP address.

5. Create a certificate and private key for the client, using the **vtl createcert** command. See "VTL" on page 1 in the *Utilities Reference Guide* for full command syntax:

    vtl createcert -n <SafeNet_HSM_client_hostname_or_IP>

    > 📝 **Note:** The client hostname or IP address must be an exact match for the client hostname, as reported using the **hostname** command.

    The certificate and private key are saved to the <client_install_dir>**/cert/client** directory and are named <client_hostname_or_IP>**.pem** and <client_hostname_or_IP>**Key.pem**, respectively. The **vtl createcert** command displays the full path-name to the key and certificate files that were generated.

6. Export the client certificate to the HSM appliance, using **pscp** (Windows) or **scp** (Linux/UNIX). You require the SafeNet Luna Network HSM appliance admin password to complete this step. You must **scp** to the admin account on the HSM appliance, or the client certificate will not register correctly. The file arriving at the HSM is automatically placed in the appropriate directory. Do not specify a target directory.

Windows	**Syntax: pscp** [options] <source_filename> <user>@<host>**:**[<target_filename>] **Example:**To copy the client certificate (**myLunaClient.pem**) to the myLunaSA appliance, keeping the same name: ```pscp myLunaClient.pem admin@myLunaSA:```

<table>
<tr><td></td><td>

```
admin@myLunaSA's password: ********
myLunaClient.pem   | 1 kB |   1.1 kB/s | ETA: 00:00:00 | 100%
```

</td></tr>
<tr><td>**Linux/UNIX**</td><td>

Syntax:scp [options] <source_filename> <user>@<host>:[<target_filename>]

Example: To copy the client certificate (**myLunaClient.pem**) to the SafeNet Luna Network HSM appliance with IP 192.168.0.123, keeping the same name:

```
scp myLunaClient.pem admin@192.168.0.123:
admin@192.168.0.123's password: ********
myLunaClient.pem   | 1 kB |   1.1 kB/s | ETA: 00:00:00 | 100%
```

</td></tr>
</table>

7. Register the client certificate with the HSM appliance using the LunaSH **client register** command. You need an admin or operator-level account on the SafeNet Luna Network HSM appliance to complete this step.

   a. Use an SSH client to connect to the SafeNet Luna Network HSM appliance and login using an admin or operator-level account.

   b. Use the LunaSH **client register** command to register the client. See "client register" on page 1 in the *LunaSH Reference Guide* for details.

By hostname	**client register -client** <client_name> **-hostname** <client_hostname> Use this syntax if the client certificate was created using the client's hostname. You will then need to run **client hostip** command to map the hostname to an IP address. See "Creating a Network Trust Link Between a Client and a Partition" on page 73 step 4 under sub-section "Assigning a Client to a Partition".)
By IP address	**client register -client** <client_name> **-ip** <client_IP_address> Use this syntax if the client certificate was created using the client's IP address as the certificate name.

   The <client_name> can be any string that allows you to easily identify this client. Many people use the hostname, but the <client_name> can be any string that you find convenient. This becomes especially useful if you are not using DNS - in that case, a well-considered <client_name> is likely going to be easier to remember or recognize than the client's IP address.

8. Restart the Network Trust Link service. After registering a client, with a hostname certificate, or after registering a client with an IP certificate and then mapping the client hostname to its IP, stop and start the NTL service, to ensure that the new client is included.

   `lunash:>`**service restart ntls**

   You can use the LunaSH **client list** command to verify the client registration.

De-registering and Re-registering Clients

If you have multiple HSM appliances connected and registered with a client and you de-register that client from one of the HSM appliances, then you must also de-register that HSM appliance on the client side. Failure to do so will result in a "Broken pipe" error, which indicates an incomplete registration.

If you wish to de-register a client and then re-register with a new certificate, on the same HSM appliance, then you must copy the certificate to the HSM appliance (HSM server) and stop and re-start the service called NTLS (see "service list" on page 1 and "service restart" on page 1). Before such a restart, any connection attempts fail, and "Error on SSL accept" is logged.

Create a Network Trust Link - One-Step Setup

In this section, we setup a network trust link (NTL) between a Luna Client and an application partition on a SafeNet Luna Network HSM using the **clientconfig deploy** command. We then register each with the other, enabling applications on a client computer to access the partition.

This procedure is performed by the HSM SO on the client computer. If you do not have physical access to the client, you must use the multi-step procedure and exchange the appliance and client's certificates by other secure means. See "Create a Network Trust Link - Multi-step setup" on page 67.

When you run the **clientconfig deploy** command, it performs the following actions:

1. Check conditions prior to running the command

    – check if the SafeNet Luna Network HSM is already registered on the client station

    – check appliance and client connectivity

    – check if the client is already registered on the appliance

    – check that the target partition has been created

2. Retrieve the HSM appliance's certificate.

3. Register HSM appliance's certificate with the client.

4. Create client's certificate, if one does not already exist.

5. Export the client's **.pem** file to the SafeNet Luna Network HSM.

6. Connect to the appliance, register the client, and assign the partition.

7. Verify that the **clientconfig deploy** command has setup the NTLS connection successfully between the client and appliance.

During the process, if a failure is encountered, the command attempts to back out of the operation and clean-up, all the way back to the start of the operation.

Prerequisites

The following prerequisite conditions must be in place:

On the SafeNet Luna Network HSM side
• The SafeNet Luna Network HSM's server.pem file must be available on the appliance (**sysconf regencert** command in LunaSH).

• An application partition must exist on the HSM (use the **partition create** command in LunaSH - you did this in "Create Application Partitions" on page 60).

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

> ✎ **Note:** If you do not wish to install glibc.i686, you can use the multi-step NTL setup procedure in section "Create a Network Trust Link - Multi-step setup" on page 67.

Procedure

1. On the client computer, where LunaHSMClient is installed, launch LunaCM.

2. In LunaCM, run the **clientconfig deploy** command:

   clientconfig deploy -server <server_IP> **-client** <client_IP> **-partition** <partition_name> [**-password** <password>] [**-user** <username>]

Examples

On the SafeNet Luna Network HSM side

```
lunash:>partition list

                                                Storage (bytes)
                                           ---------------------------
 Partition           Name                  Objects  Total    Used    Free
 ========================================================================
 154438865287        LunaPar1                    0  325896       0  325896

Command Result : 0 (Success)
```

On the client side

```
lunacm:> clientconfig deploy -server 192.20.11.78 -client 10.124.0.31 -partition LunaPar1
Please wait...

The server's host key is not cached in the registry. You have no
guarantee that the server is the computer you think it is.
The server's rsa2 key fingerprint is:
ssh-rsa 2048 15:86:1d:82:d9:8f:e9:51:90:62:0d:f5:87:e5:89:a3
If you trust this host, enter "y" to add the key to
PuTTY's cache and carry on connecting.
If you want to carry on connecting just once, without
adding the key to the cache, enter "n".
If you do not trust this host, press Return to abandon the connection.
Store key in cache? (y/n) y

Using username "admin".
Please enter appliance admin role user's password:
Last login: Wed Mar 29 17:19:11 2017 from 10.124.0.31

Luna SA 7.0.0 Command Line Shell - Copyright (c) 2001-2017 SafeNet, Inc. All rights reserved.

New server 192.20.11.78 successfully added to server list.

The following Luna SA Slots/Partitions were found:

Slot    Serial #                Label
====    ================        =====
   0        154438865287

Command Result : No Error
```

Next

Go to .

Enable the Client to Access a Partition

After creating the network trust link between the client and the appliance, you need to enable the client to access a specific partition on the appliance. You can configure the client to access a partition using an NTLS or STC connection, as follows:

NTLS client-partiton links	Assign the partition to a specific client using the LunaSH **client assignpartition** command. This allows the client to create NTL connections to the partition to perform cryptographic operations. See "Creating a Network Trust Link Between a Client and a Partition" below.
STC client-partiton links	Enable Secure Trusted Channel (STC) on the client and partition. This disables the NTLS connection to the partition, and replaces it with an STC connection. See "Creating an STC Link Between a Client and a Partition" on page 75.

Creating a Network Trust Link Between a Client and a Partition

After you establish a network trust link between the client and the appliance, you can assign the client to a specific partition on the appliance to grant the client access to the partition. After you assign a client to a partition, the client can establish NTLS links to the partition, allowing you to:

• See the partition as a slot in LunaCM.

• Use the partition with your cryptographic applications.

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

Assigning a Client to a Partition

Use the LunaSH command **client assignpartition** to assign a registered client to a partition. You might need to use your client IP address as your client name, if you registered your client using an IP address.

This task is performed by the HSM SO, if you are not using STC. This is the final task you need to complete before handing off the partition to the partition owner.

To assign a client to a partition:

1. Launch LunaSH and login as the HSM SO.

2. Enter the following command to assign a client to a partition:

   client assignpartition -client <clientname> **-partition** <partition_label>

   For example:

```
lunash:> client assignPartition -client ntls_client -partition ntls_partition

 'client assignPartition' successful.

Command Result : 0 (Success)
```

3. Enter the following command to verify that the HSM Partition is assigned to the client:

    client show -client <clientname>

    For example:

    ```
    lunash:> client show -client ntls_client

    ClientID:     ntls_client
    Hostname:     Luna_Client
    OTT Expiry:   n/a
    Partitions:   ntls_partition
    ```

4. If you registered your client by host name, the appliance will need to use a DNS server to look up the device IP address. To ensure that the client is reachable in the event of a DNS failure, you can use the following command to map the client host name to its IP address, and save the mapping locally on the appliance.

    client hostip map -client <client_name> **-ip** <client_IP_address>

    For example:

    ```
    lunash:> client hostip map -client ntls_client -ip 192.20.11.21

    Command Result : 0 (Success)

    lunash:>client hostip show

    Client Name          Host Name                      Host IP
    ------------------------------------------------------------------
    ntls_client          ntls_client                    192.20.11.21

    Command Result : 0 (Success)
    ```

5. Hand off possession of the partition to its new owner by providing the contact information (IP address and partition name) and any necessary instructions. The receiving person will become the Partition SO and begin configuring the partition for its application.

Verifying Your Setup

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

This task is performed by the partition owner, from the SafeNet Luna HSM client workstation used to deploy the partition.

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

2. Go to the software directory (**c:\Program Files\SafeNet\LunaClient** for Windows, or **/usr/safenet/lunaclient** for Linux, and type **vtl verify**.

3. The response should be similar to:

    ```
    Slot    Serial #            Label
    ====    ============        =====
       0         2279315
    ```

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

At this point, the client and HSM are configured and registered with each other. You can now begin to use the SafeNet Luna Network HSM with your application. You can use the **partition list** command for a list of HSM Partitions on the HSM, and the **client list** command for a list of the clients assigned to an HSM Partition.

4. Setup is complete. We suggest that you browse the *Administration Guide* to develop a deeper understanding of the options and capabilities of your SafeNet Luna Network HSM partition, and of the housekeeping tasks and utilities that you might need.

Client Connection Limits

See "Connections to the Appliance - Limits" on page 1 for a discussion of the limits for client connections to a SafeNet Luna Network HSM appliance and HSM.

Applications and Integrations

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

Creating an STC Link Between a Client and a Partition

If you require a higher level of security for your network links than is offered by NTLS, such as in cloud environments, or in situations where message integrity is paramount, you can use Secure Trusted Channel (STC) to provide very secure client-partition links. STC offers the following features to ensure the security and integrity of your client-partition communications:

*   All data is transmitted using symmetric encryption; only the end-points can decrypt messages

*   Message authentication codes prevent an attacker from intercepting and modifying any command or response

*   Bi-directional authentication of both the HSM and the end-point ensure that only authorized entities can establish an STC connection

See "Secure Trusted Channel (STC)" on page 1 in the *Administration Guide* for more information. You can configure your SafeNet Luna Network HSM so that some partitions use STC and others use NTLS.

> 🖉   **Note:** The SafeNet Luna Network HSM can create STC and NTLS channels to different clients as required. The client can also support both STC and NTLS links. However, all links from a specific client to a specific SafeNet Luna Network HSM appliance must be either STC or NTLS.

> 🖉   **Note:** STC links are not supported over an IPv6 network. You must use NTLS to make partition-client connections via IPv6.

This section describes how to establish an STC connection between a client and a new partition. The procedure consists of the following major steps:

*   "Prerequisites" on the next page

*   "Step 1: Create the Client Token and Identity" on page 78

- "Step 2: Register the Partition Identity Public Key to the Client" on page 79

- "Step 3: Enable and Verify the STC Link" on page 80

The following optional procedures are also described:

- "Registering a Single STC Partition to Multiple Clients" on page 81

- "Converting an Initialized NTLS Partition-Client Connection to STC" on page 85

Figure 1: Creating an STC Link Between a Client and a Partition
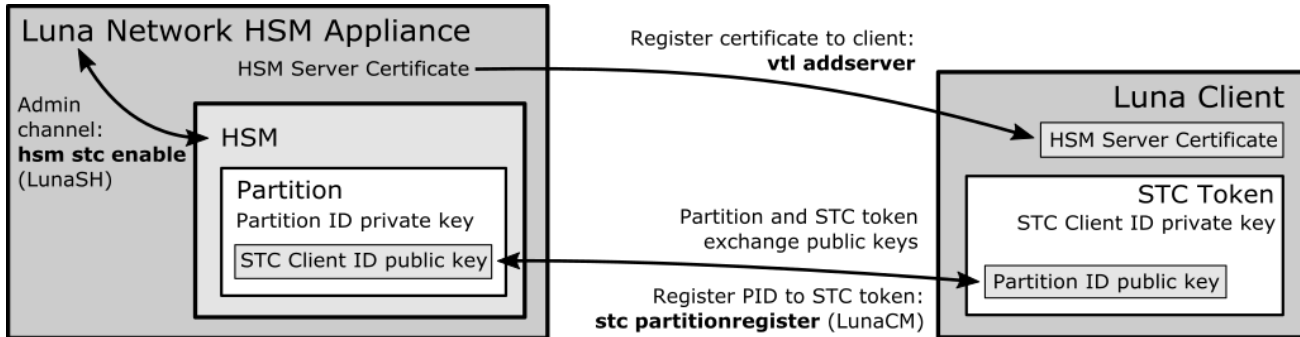
Prerequisites

You must complete these procedures before establishing a partition-client STC connection. The instructions are divided into tasks performed by the HSM SO and the Client Administrator.

- "HSM SO Prerequisites" below

- "Enabling STC on the Admin Channel (Optional)" on the next page

- "Client Administrator Prerequisites" on page 78

HSM SO Prerequisites

To prepare the HSM to use STC, the HSM SO must complete the following prerequisites. If you have Administrator access to the client workstation, you can use **scp** or **pscp** to transfer the server and partition public keys directly from the SafeNet Luna Network HSM. Otherwise, you must provide these keys to the client by other secure means.

1. Enable HSM Policy 39: Allow Secure Trusted Channel on the appliance.

    a. Log in as HSM SO using LunaSH.

        hsm login

    b. Use the following command to set Policy 39 to **1** (Enabled):

        hsm changepolicy -policy 39 -value 1

    c. Confirm that HSM Policy 39 is enabled:

        hsm showpolicies

2. Use the following command to create one or more new partitions for the client:

    > **Note:** Each client identity registered to a partition uses 2392 bytes of storage on the partition. Ensure that you create partitions large enough to store the identity of every client workstation that will access the partition, in addition to cryptographic objects.

partition create -partition <partition_name> [**-size** <bytes>]

When you create a partition, a partition identity key pair is automatically created.

3. For each partition you created, export the partition identity public key to the SafeNet Luna Network HSM file
    system. The file will be named with the partition's serial number. You can check the key's filename with **my file
    list**.

    stc partition export -partition <partition_name>

    my file list

    For example:

    ```
    lunash:>stc partition export -partition app_par1
    Successfully exported partition identity for partition app_par1 to file: 154438865304.pid

    lunash:>my file list
    515 Mar  6 17:38 154438865304.pid
    4409 Mar  6 10:44 firstboot.log
    ```

4. You can use the following command to display the partition identity public key hash. It is recommended that you
    provide it to the client along with the partition identity public key, so that the Partition SO can verify the key's
    integrity as described in "Step 3: Enable and Verify the STC Link" on page 80.

    stc partition show -partition <partition_name>

    For example:

    ```
    lunash:>stc partition show -partition app_par1

    Partition Serial Number:               154438865304
    Partition Identity Public Key SHA1 Hash: 477ad2869ad892ebdd5007aa54fae3745fa175e2
    ```

5. The client will require the following files/information to establish the STC connection. The SafeNet Luna Network
    HSM client software package includes the **scp** (Linux) and **pscp** (Windows) tools for securely transferring files (see
    "SCP and PSCP" on page 1 for syntax). If you do not have access to the client workstation, or a firewall prevents
    you from using **scp** or **pscp**, you must transfer these files from the HSM and provide them to the client by other
    secure means:

    –   The HSM Server Certificate (**server.pem**) from the SafeNet Luna Network HSM. If you have already
        established an NTLS connection between the appliance and the client, as detailed in "Create a Network Trust
        Link Between the Client and the Appliance" on page 67, you do not need to send this certificate.

    –   The partition identity public key for each partition to be assigned to the client (**154438865304.pid** in the
        example above).

    –   The partition identity public key hash for each partition to be assigned to the client. This is recommended so
        that the client can verify the key's integrity before using the partition. Do not send the hash by the same means
        as the certificates.

Enabling STC on the Admin Channel (Optional)

For added security, you can use STC to secure communications between the SafeNet Luna Network HSM appliance
and the HSM Admin partition. This procedure is performed by the HSM SO using LunaSH. You must be logged in as
HSM SO to enable or disable this feature. You must restart the STC service after enabling STC on the Admin channel.

> **Note:** Enabling STC on the Admin channel is performance-affecting. For more information, see "Establishing and Configuring the STC Admin Channel on a SafeNet Luna Network HSM Appliance" on page 1.

To enable STC on the admin channel:

1. Enable STC by entering the following command in LunaSH:

    hsm stc enable

2. Restart the STC service on the HSM.

    service restart stc

Client Administrator Prerequisites

To prepare the client to access a partition on the SafeNet Luna Network HSM, you must first establish a Network Trust Link to the appliance using the HSM Server Certificate (**server.pem**) you received from the HSM SO. You must have Administrator privileges on the client.

1. Open a command line (as Administrator) on the client and navigate to the LunaClient install directory.

2. Register the SafeNet Luna Network HSM appliance with the client by entering the following command:

    vtl addserver -n <server_IP_or_hostname> **-c** <server_certificate_filename>

    See "Create a Network Trust Link Between the Client and the Appliance" on page 67 for more detailed instructions.

3. To check that you have successfully registered the appliance with the client, run LunaCM and enter the following command to see a list of registered servers:

    clientconfig listservers

Step 1: Create the Client Token and Identity

This procedure is completed by an Administrator on the client workstation, using LunaCM.

> **CAUTION:** This step is not required if you have already created a client token and identity. Verify using **stc identityshow**. If you recreate the client identity, you will have to re-register any existing STC partitions.

To create the client token and identity:

1. Open a SafeNet Luna HSM client session:

    a. Open a command prompt or terminal window.

    b. Launch LunaCM:

Windows	C:\Program Files\SafeNet\LunaClient\lunacm
Linux	/usr/safenet/lunaclient/data/bin/lunacm

2. Initialize the STC client software token, or insert the STC client hardware token (SafeNet eToken 7300) you have prepared for this client:

    – If you are using an STC client software token, enter the following command to initialize the STC client token.

    stc tokeninit -label <token_label>

For example:

```
lunacm:> stc tokeninit -label mySTCclientToken

Successfully initialized the client token.
```

- – If you are using an STC client hardware token (SafeNet eToken 7300), insert the token into an available USB port. Before you can use a hardware token, the token must be initialized using the SafeNet Authentication Client on a Windows workstation, as described in "Using a Hard Token to Store the STC Client Identity" on page 1 in the *Administration Guide*.

  You must also install the SafeNet Authentication Client software (8.3 or higher) on the client workstation and add the following line to the **Secure Trusted Channel** section of the **crystoki.ini** (Windows) or **Chrystoki.conf** (UNIX/Linux) file, to specify the path to the SafeNet Authentication Client eToken library:

Windows	**ClientTokenLib=C:\Windows\System32\eToken.dll**
Linux	**ClientTokenLib=<path_to_libeToken.so>** For example, on CentOS, the path is **/usr/lib/libeToken.so**

3. Enter the following command to create a client identity on the token. The STC client identity public key is automatically exported to the <luna_client_root_dir>**/data/client_identities** directory:

stc identitycreate -label <client_identity>

For example:

```
lunacm:> stc identitycreate -label mySTCclientID

Client identity successfully created and exported to file /us-
r/safenet/lunaclient/data/client_identities/mySTCclientID
```

Step 2: Register the Partition Identity Public Key to the Client

This step requires the partition identity public key file created by the HSM SO in "Prerequisites" on page 76 (**154438865304.pid** in the example).

To register the partition identity public key to the client:

1. Enter the following command in LunaCM:

stc partitionregister -file <partition_identity> [**-label** <partition_label>]

For example:

```
lunacm:> stc partitionregister -file /usr/safenet/lunaclient/partition_iden-
tities/154438865304.pid -label app_par1

Partition identity 154438865305 successfully registered.
```

Repeat this step for each partition identity public key you wish to register to this client.

2. If you were provided with the partition identity public key hash, enter the following command to verify that the hashes match:

stc identityshow

For example:

```
lunacm:> stc identityshow

Client Identity Name:        mySTCclientID
```

```
Public Key SHA1 Hash:              1b8e783c5cc3bb6a79e5d4a4026258a0f34ef7f6
List of Registered Partitions:

Partition Identity      Partition               Partition Public Key SHA1 Hash
Label                   Serial Number
_____
 app_par1               154438865304     6916eca3751173f7cf903ab60b9bf1bf35088271
```

If the hashes do not match, enter the following command to deregister the partition identity public key, and contact your HSM SO.

stc partitionderegister -serial <partition_serial_number>

Step 3: Enable and Verify the STC Link

> ⚠ **CAUTION:** When you enable STC on the client, you must specify the SafeNet Luna Network HSM appliance that hosts the partition you want to link to. This forces the client to use STC for all links to the specified SafeNet Luna Network HSM appliance. Any existing NTLS connections to the specified SafeNet Luna Network HSM appliance will be terminated. Ensure you have registered the partition identity for each partition on this HSM before continuing.

To enable and verify the STC link:

1. Enter the following command in LunaCM to determine the server ID of the SafeNet Luna Network HSM appliance that hosts the partition:

    clientconfig listservers

2. Enter the following command to enable the STC link:

    stc enable -id <server_id>

    For example:

```
lunacm:> stc enable -id 0

        You are about to enable STC to server 192.20.11.78.
        This will initiate an automatic restart of this application. All sessions
        logged in through the application will be closed.

        Are you sure you wish to continue?

        Type 'proceed' to continue, or 'quit' to quit now -> proceed

        Successfully enabled STC to connect to server 192.20.11.78.
```

At this point, LunaCM restarts. If successful, the partition appears in the list of available HSMs. The slot for the partition is easily identified because it does not have a label, since it is not yet initialized. In the following example, the uninitialized SafeNet Luna Network HSM partition is in slot 1:

```
        Available HSMs:

        Slot Id ->             0
        Label ->               stc_legacy
        Serial Number ->       359693009024
        Model ->               K6 Base
        Firmware Version ->     6.22.0
        Configuration ->       Luna User Partition, No SO (PW) Signing With Cloning Mode
        Slot Description ->     Net Token Slot
```

```
Slot Id ->              1
Label ->
Serial Number ->        154438865304
Model ->                LunaSA
Firmware Version ->      7.0.1
Configuration ->        Luna User Partition, No SO (PW) Signing With Cloning Mode
Slot Description ->      Net Token Slot
```

3. Enter the following command to set the current slot to the slot containing the new partition:

    slot set -slot <slot>

    For example:

    ```
    lunacm:> slot set -slot 1
    ```

4. Enter the following command to verify the link:

    stc status

    For example:

    ```
    lunacm:> stc status

    Enabled:       Yes
    Status:        Connected
    Channel ID:    2
    Cipher Name:   AES 256 Bit with Cipher Block Chaining
    HMAC Name:     HMAC with SHA 512 Bit
    ```

The Partition SO can now initialize the partition on the client workstation. See "Configure Application Partitions" on page 88. When the partition is initialized, the following actions are performed automatically:

- The client identity public key is registered to the partition.

- Partition policy 37: Force Secure Trusted Channel is enabled on the partition.

Registering a Single STC Partition to Multiple Clients

After the client-partition STC connection is established, you may want other clients to have access to the same partition. This allows the Partition SO, Crypto Officer, and Crypto User to access the partition from their own client workstations.

In the following procedure, Client 2 will register the HSM Server Certificate and the partition identity public key(s), and Client 1 will register Client 2's identity public key.

This procedure is completed by the Partition SO (Client 1) and the Client 2 Administrator.

Figure 2: Registering Two Clients to a Single Initialized Partition
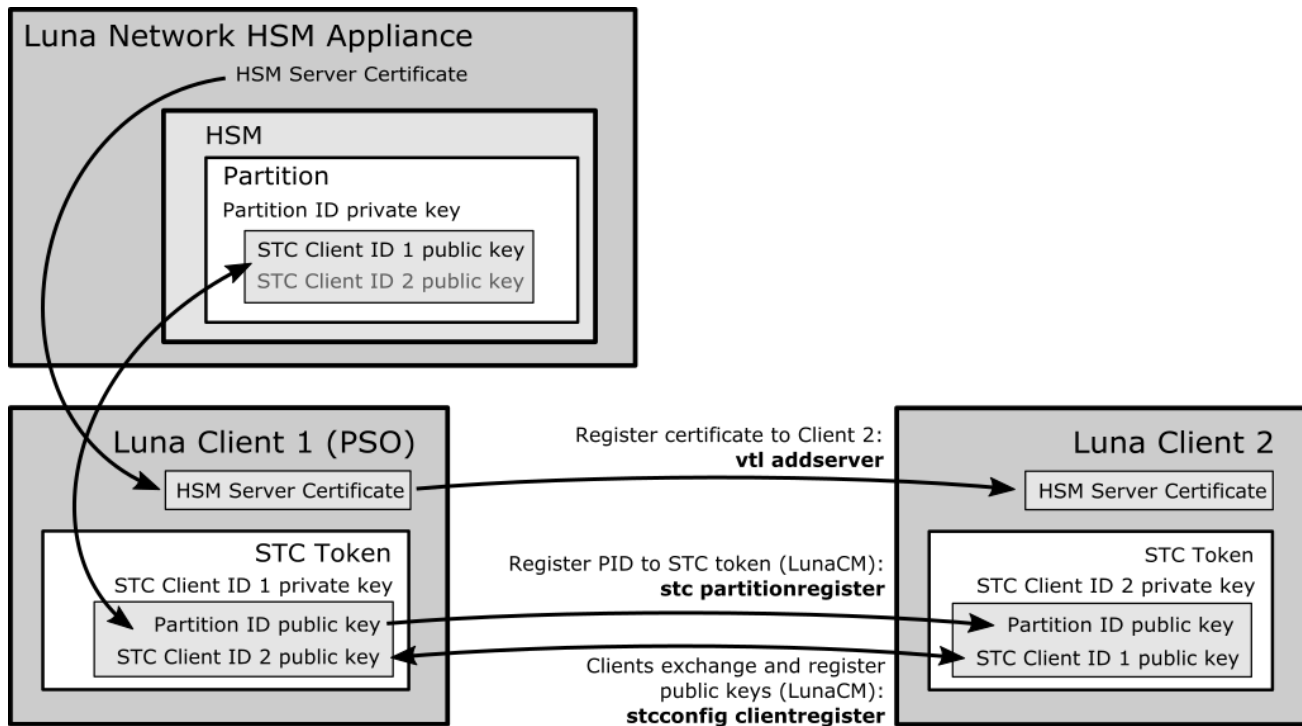
Partition SO (Client 1) Prerequisites:

You must provide the same files/information to the Client 2 Administrator that you received from the HSM SO. The SafeNet Luna Network HSM client software package includes the **scp** (Linux) and **pscp** (Windows) tools for securely transferring files (see "SCP and PSCP" on page 1 for syntax). If you do not have access to the client workstation, or a firewall prevents you from using **scp** or **pscp**, you must provide the following to the Client 2 Administrator by other secure means:

- The HSM Server Certificate (originally **server.pem**) from the SafeNet Luna Network HSM. Alternatively, the Client 2 Administrator can obtain it from the HSM SO.

- The partition identity public key for each partition you want to register to Client 2. You can use the original ***.pid** file supplied by the HSM SO, or export a copy to the client system using the following LunaCM commands:

role login -name po

stcconfig partitionidexport

For example:

```
lunacm:> stcconfig partitionidexport

Successfully exported partition identity for the current slot to /us-
r/safenet/lunaclient/partition_identities/154438865305.pid
```

- The partition identity public key hash for each partition to be registered to Client 2. This is recommended so that the Client 2 Administrator can verify the key's integrity before using the partition. You should not send the hash by the same means as the certificates. Enter the following command in LunaCM to view the hash:

stc identityshow

For example:

```
lunacm:> stc identityshow
```

```
Client Identity Name:        mySTCclientID
Public Key SHA1 Hash:        1b8e783c5cc3bb6a79e5d4a4026258a0f34ef7f6
List of Registered Partitions:

 Partition Identity   Partition           Partition Public Key SHA1 Hash
 Label                Serial Number
_____
 app_par1             154438865304        6916eca3751173f7cf903ab60b9bf1bf35088271
```

Client 2 Prerequisites:

1. This step is not required if you have already created a client token and identity. Verify using **stc identityshow**. If you recreate the client identity, you will have to re-register any existing STC partitions.

   Run LunaCM and execute the following commands to create the client token and identity:

   stc tokeninit -label <token_label>

   stc identitycreate -label <client_identity>

   For a more detailed description of this step, see "Step 1: Create the Client Token and Identity" on page 78.

2. Provide the following files/information to the Partition SO. The SafeNet Luna Network HSM client software package includes the **scp** (Linux) and **pscp** (Windows) tools for securely transferring files (see "SCP and PSCP" on page 1 for syntax). If you do not have access to the client workstation, or a firewall prevents you from using **scp** or **pscp**, you must provide the client identity to the Partition SO by other secure means.

   – The client 2 identity public key

   – The client 2 identity public key hash. This is recommended so that the Partition SO can verify the key's integrity before allowing access to the partition. You should not send the hash by the same means as the client identity public key. Enter the following command in LunaCM to view the hash:

     stc identityshow

     For example:

     ```
     lunacm:> stc identityshow

     Client Identity Name:        Client2
     Public Key SHA1 Hash:        cd5ca1c094acfe44803a9ef4b412fc4087a16c32
     List of Registered Partitions: None
     ```

Client 2 Administrator:

1. Ensure that you have received the necessary certificates/information from the Partition SO:

   – HSM Server Certificate (***.pem**)

   – Partition identity public key (***.pid**) for each partition to be registered

   – Partition identity public key hash for each partition

2. Open a command prompt or terminal window and navigate to the SafeNet Luna Network HSM client installation directory.

3. Use the **vtl** utility to register the HSM Server Certificate (**192.20.11.78Cert.pem** in the example below) to the client:

   vtl addserver -n <HSM_hostname_or_IP> **-c** <server_certificate>

   For example:

   ```
   >vtl addserver -n 192.20.11.78 -c ./cert/server/192.20.11.78Cert.pem
   ```

```
New server 192.20.11.78 successfully added to server list.
```

4. Launch LunaCM and use the following commands to register the partition identity public key to Client 2 and view the partition hash:

    stc partitionregister -file <partition_identity> [**-label** <partition_label>]

    stc identityshow

    Repeat for each partition you want to register. For a more detailed description of this step, see .

5. Find the correct server ID for the SafeNet Luna Network HSM hosting the partition and enable its STC connection. You will be prompted to restart LunaCM and all current sessions will be closed.

    > ⚠ **CAUTION:** This forces the client to use STC for all links to the specified appliance. Any remaining NTLS links from this client to the appliance will be terminated. Ensure you have registered the partition identity for each partition on this HSM before continuing.

    lunacm:>**clientconfig listservers**

    lunacm:>**stc enable -id** <server_ID>

    If the partition is not visible as a slot when LunaCM restarts, wait until the Partition SO completes the final procedure and activates Partition Policy 37. For a more detailed version of this step, see .

Partition SO (Client 1):

1. Ensure that you have received the necessary certificates/information from the Client 2 Administrator:

    –   Client 2 identity public key

    –   Client 2 identity public key hash

2. Launch LunaCM, change the active slot to the partition, and login as Partition SO:

    slot set -slot <slotnum>

    role login -name po

3. Use the following command to register the Client 2 identity public key (**Client2** in the example below):

    stcconfig clientregister -label <client_label> **-file** <client_identity>

    For example:

    ```
    lunacm:> stcconfig clientregister -l Client2 -f /usr/safenet/lunaclient/client_iden-
    tities/Client2

    Successfully registered the client Client2 to the current slot.
    ```

4. Enter the following command to view the hash for the **Client2** identity:

    stcconfig clientlist

    For example:

    ```
    lunacm:> stcconfig clientlist

     Client Name                      Client Public Key SHA1 Hash
    ```

```
Client2                          cd5ca1c094acfe44803a9ef4b412fc4087a16c32

Partition SO                     1b8e783c5cc3bb6a79e5d4a4026258a0f34ef7f6
```

If the displayed hash does not match the hash you received from the Client 2 Administrator, enter the following command to deregister the client identity, and contact the Client 2 Administrator:

stcconfig clientdelete -label <client_label>

5. You can now initialize the Crypto Officer role (or the CO can initialize the Crypto User role) and provide the password to the Client 2 Administrator by secure means. See "Configure Application Partitions" on page 88.

The Partition SO can register additional clients to the same partition by repeating the process above.

Figure 3: Registering Multiple Clients to a Single Partition
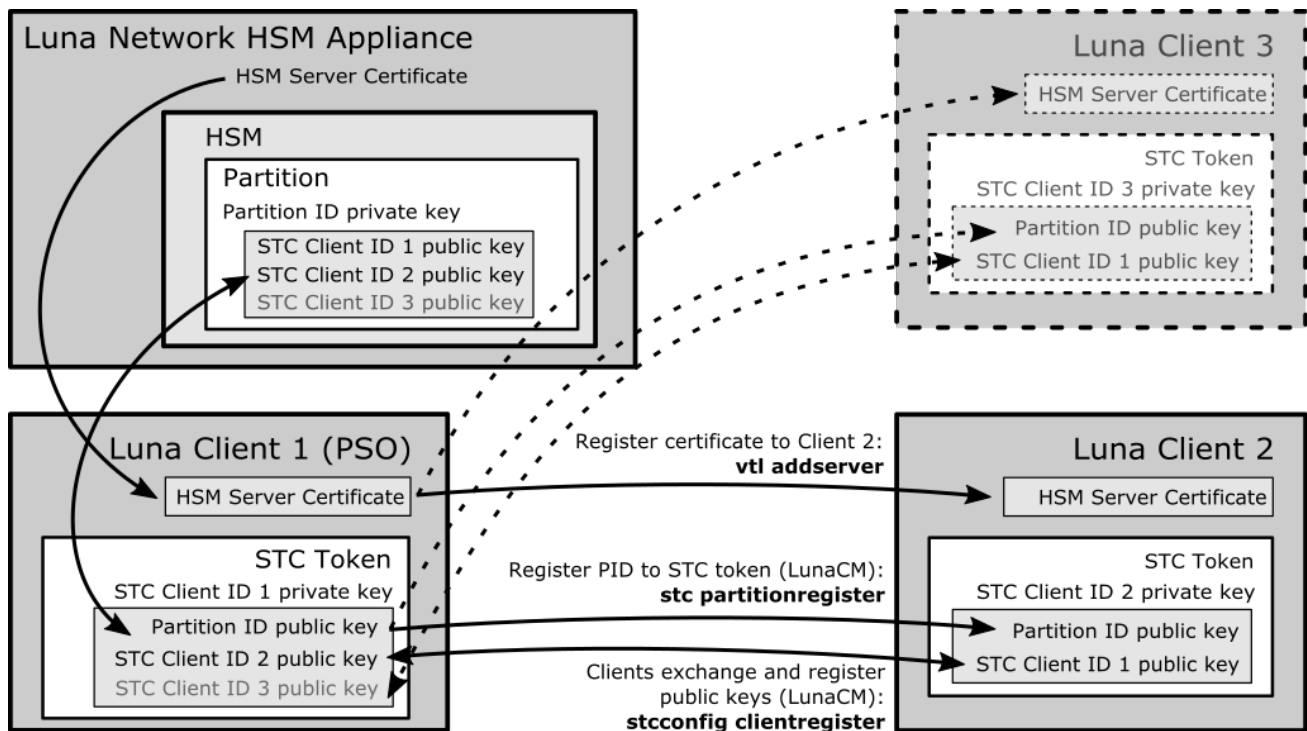
Converting an Initialized NTLS Partition-Client Connection to STC

If you have initialized partitions already assigned to a client using NTLS, you can use the following procedure to switch to a more secure STC connection. All of the client's assigned partitions on the specified SafeNet Luna Network HSM will be converted. It is not possible for a client to connect to multiple partitions on a single SafeNet Luna Network HSM using a combination of NTLS and STC.

> **Note:** The HSM SO must first enable HSM Policy 39: Allow Secure Trusted Channel on the SafeNet Luna Network HSM (see "Prerequisites" on page 76).

The Partition SO must complete this procedure.

To convert an NTLS partition-client connection to STC:

1. This step is not required if you have already created a client token and identity. Verify using **stc identityshow**. If

you recreate the client identity, you will have to re-register any existing STC partitions.

Run LunaCM and execute the following commands to create the client token and identity:

stc tokeninit -label <token_label>

stc identitycreate -label <client_identity>

For a more detailed description of this step, see "Step 1: Create the Client Token and Identity" on page 78.

2. Login to the partition as Partition SO and use the following command to export the existing partition ID:

slot set -slot <slotnum>

role login -name po

stcconfig partitionidexport

For example:

```
lunacm:> stcconfig partitionidexport

Successfully exported partition identity for the current slot to /us-
r/safenet/lunaclient/partition_identities/1238700701520.pid
```

3. Enter the following command to register the partition's public key with the client identity:

stc partitionregister -file <partition_identity> [**-label** <partition_label>]

For example:

```
lunacm:> stc partitionregister -file /usr/safenet/lunaclient/partition_iden-
tities/1238700701520.pid

Partition identity 1238700701520 successfully registered.
```

4. Enter the following command to register the client identity to the partition:

> 📝 **Note:** Each client identity registered to a partition uses 2392 bytes of storage on the partition. Ensure that there is enough free space before registering a client identity.

stcconfig clientregister -label <client_label> **-file** <client_identity>

For example:

```
lunacm:> stcconfig clientregister -label mySTCclientID -file /usr/safenet/lunaclient/client_
identities/mySTCclientID

Successfully registered the client mySTCclientID to the current slot.
```

5. Enter the following command to enable partition policy 37: Force STM Connection.

partition changepolicy -slot <slotnum> **-policy 37 -value 1**

Repeat steps 2-5 for each NTLS partition on the same SafeNet Luna Network HSM you want to register to this client.

> 📝 **Note:** If this command returns an error, ensure that the HSM SO has enabled HSM Policy 39 on the appliance.

6. Find the correct server ID for the SafeNet Luna Network HSM hosting the partition and enable its STC connection. You will be prompted to restart LunaCM and all current sessions will be closed.

> ⚠️ **CAUTION:** This forces the client to use STC for all links to the specified appliance. Any remaining NTLS links from this client to the appliance will be terminated. Ensure that you have completed steps 2-5 for each of this client's partitions before continuing.

clientconfig listservers

stc enable -id <server_ID>

If a partition is not visible as a slot when LunaCM restarts, disable STC for the server using **stc disable -id** <server_ID>, and ensure that you have activated Partition Policy 37. For a more detailed version of this step, see "Step 3: Enable and Verify the STC Link" on page 80.

Configure Application Partitions

This chapter describes how the Partition Security Officer (SO) configures a partition after receiving it from the HSM SO. The configuration tasks you need to perform depend on whether the partition is password-authenticated or PED-authenticated as follows:

Authentication	Tasks
Password	1. "Initialize the Partition SO and Crypto Officer Roles on a PW-Auth Partition" below 2. "Initialize the Crypto User Role on a PW-Authenticated Partition" on the next page
PED	1. "Initialize the Partition SO and Crypto Officer Roles on a PED-Auth Partition" on page 91 2. "Initialize the Crypto User Role on a PED-Authenticated Partition" on page 92 3. "Activate a PED-Authenticated Partition" on page 95

Initialize the Partition SO and Crypto Officer Roles on a PW-Auth Partition

These instructions assume a password-authenticated SafeNet Luna Network HSM has been initialized, and an application partition has been created.

Step 1: Initialize the Partition SO role

This step is performed by an Administrator user on the SafeNet Luna Network HSM client workstation. If you are using STC to provide the client-partition link, do not perform this procedure, since you already initialized the partition when configuring the STC link. See "Creating an STC Link Between a Client and a Partition" on page 75 for more information.

1. Set the active slot to the uninitialized application partition:

   Type **slot set -slot** <slotnum>

   ```
   lunacm:> slot set -slot 0

           Current Slot Id:    0     (Luna User Slot 7.0.1 (PW) Signing With Cloning Mode)

   Command Result : No Error
   ```

2. Initialize the application partition, to create the partition's Security Officer (SO), and set the initial password and cloning domain.

   partition init -label <par_label>

   ```
   lunacm:>par init -label myLunapar

           You are about to initialize the partition.
           All contents of the partition will be destroyed.

           Are you sure you wish to continue?
   ```

```
            Type 'proceed' to continue, or 'quit' to quit now ->proceed

            Enter password for Partition SO: ********
            Re-enter password for Partition SO: ********

            Option -domain was not specified.  It is required.

            Enter the domain name: *********
            Re-enter the domain name: *********

    Command Result : No Error
```

Step 2: Initialize the Crypto Officer role

The SO of the application partition can now assign the first operational role within the new partition.

1. First, login as Partition SO. You can also use the shortcut **po**.

    role login -name Partition SO

2. Initialize the Crypto Officer role and set the initial password. You can also use the shortcut **co**.

    role init -name Crypto Officer

```
    lunacm:>role init -name co

            enter new password: ********
            re-enter new password: ********

    Command Result : No Error
```

3. The Partition SO can create the Crypto Officer, but only the Crypto Officer can create the Crypto User. Therefore, you must log out to allow the Crypto Officer to log in with the newly-set password.

    role logout

> **Note:** The password for the Crypto Officer role is valid for the initial login only. The CO must change the initial password using the command **role changepw** during the initial login session, or a subsequent login. Failing to change the password will result in a CKR_PIN_EXPIRED error when they perform role-dependent actions.

Once the Crypto Officer logs in and changes the initial credential set by the Partition SO, applications using the CO's challenge secret/password can perform cryptographic operations in the partition. The Crypto Officer can create, modify and delete crypto objects within the partition, and use existing crypto objects (sign/verify). You can also create a limited-capability role called Crypto User that can use the objects created by the Crypto Officer, but cannot modify them. The separation of roles is important in some security regimes and operational situations, and where you might be required to satisfy audit criteria for industry or government oversight.

The next sequence of configuration actions is performed by the Crypto Officer, just created for the application partition. See "Initialize the Crypto User Role on a PW-Authenticated Partition" below.

Initialize the Crypto User Role on a PW-Authenticated Partition

These instructions assume:

- A password-authenticated SafeNet Luna Network HSM has been initialized

- An application partition has been created

- A Crypto Officer has been created for the partition

- The Crypto Officer password has been conveyed to the person responsible for the Crypto Officer role. See .

As Crypto Officer, you can:

- Create a Crypto User (limited access user) for the application partition.

- Create, delete, change and manipulate cryptographic objects on the application partition, either for your own use or for use by the Crypto User.

To initialize the Crypto User role

1. Set the active slot to the desired application partition, where the Crypto Officer was just created.

   slot set -slot <slotnum>

   ```
   lunacm:> slot set -slot 0

           Current Slot Id:   0     (Luna User Slot 7.0.0 (PW) Signing With Cloning Mode)

   Command Result : No Error
   ```

2. Log in as the Crypto Officer. You can also use the shortcut **co**.

   role login -name Crypto Officer

   ```
   lunacm:>role login -name co

           enter password: ********

   Command Result : No Error
   ```

   > **Note:** The password for the Crypto Officer role is valid for the initial login only. You must change the initial password using the command **role changepw** during the initial login session, or a subsequent login. Failing to change the password will result in a CKR_PIN_EXPIRED error when you perform role-dependent actions.

3. If you have not already done so, change the initial password set by the Partition SO.

   role changepw -name Crypto Officer

   ```
   lunacm:>role changepw -name co

           enter existing password: ********
           enter new password: ********
           re-enter new password: ********

   Command Result : No Error
   ```

4. Create the Crypto User. You can also use the shortcut **cu**.

   role init -name Crypto User

   ```
   lunacm:>role init -name cu

           enter new password: ********
   ```

```
        re-enter new password: ********

Command Result : No Error
```

> **Note:** The password for the Crypto User role is valid for the initial login only. The CU must
> change the initial password using the command **role changepw** during the initial login session,
> or a subsequent login. Failing to change the password will result in a CKR_PIN_EXPIRED
> error when they perform role-dependent actions.

The Crypto Officer can now login with the credentials provided by the Crypto Officer, and change the initial password.
The Crypto User can now use applications to perform cryptographic operations using keys and objects created in the
partition by the Crypto Officer.

Initialize the Partition SO and Crypto Officer Roles on a PED-Auth Partition

These instructions assume a PED-authenticated SafeNet Luna Network HSM has been initialized, and an application
partition has been created.

You will need:

- Luna PED and PED keys with labels. These instructions assume that your Luna PED is available locally, but has a
  working Remote PED connection to the SafeNet Luna Network HSM.

These instructions assume that you have already made your decisions whether to use all-new, blank PED keys, or to
re-use any existing, imprinted PED keys for any of the steps.

Step 1: Initialize the Partition SO role

This step is performed by an administrative user on the SafeNet Luna Network HSM client workstation. If you are using
STC to provide the client-partition link, do not perform this procedure, since you already initialized the partition when
configuring the STC link. See "Creating an STC Link Between a Client and a Partition" on page 75 for more information,
and skip ahead in this page to "Step 2: Initialize the Crypto Officer role" on the next page.

Have a blue HSM SO PED key and a red Domain PED key ready.

1. Set the active slot to the uninitialized application partition:

   Type **slot set -slot** <slotnum>

```
lunacm:> slot set -slot 0

        Current Slot Id:    0      (Luna User Slot 7.0.1 (PW) Signing With Cloning Mode)

Command Result : No Error
```

2. Initialize the application partition, to create the partition's blue Security Officer (SO) PED key and the red cloning
   domain PED key.

   partition init -label <par_label>

```
lunacm:>par init -label myLunapar

        You are about to initialize the partition.
        All partition objects will be destroyed.
```

```
            Are you sure you wish to continue?

            Type 'proceed' to continue, or 'quit' to quit now -> proceed

            Please attend to the PED.
```

Respond to Luna PED prompts...

```
Command Result : No Error
```

Step 2: Initialize the Crypto Officer role

The SO of the application partition can now assign the first operational role within the new partition. Have a black Crypto Officer PED key ready.

1. First, login as Partition SO. You can also use the shortcut **po**.

    role login -name Partition SO

2. Type **role init -name co**.

    ```
    lunacm:> role init -name Crypto Officer

            Please attend to the PED.
    ```

    Respond to Luna PED prompts...

    ```
    Command Result : No Error
    ```

3. The Partition SO can create the Crypto Officer, but only the Crypto Officer can create the Crypto User. Therefore, you must log out to allow the Crypto Officer to log in.

    role logout

    > ☑ **Note:** The black Crypto Officer PED key is valid for the initial login only. The CO must change the initial credential on the key using the command **role changepw** during the initial login session, or a subsequent login. Failing to change the credential will result in a CKR_PIN_ EXPIRED error when they perform role-dependent actions.

Once the Crypto Officer logs in and changes the initial credential set by the Partition SO, applications using the CO's challenge secret/password can perform cryptographic operations in the partition. The Crypto Officer can create, modify and delete crypto objects within the partition, and use existing crypto objects (sign/verify). You can also create a limited-capability role called Crypto User that can use the objects created by the Crypto Officer, but cannot modify them. The separation of roles is important in some security regimes and operational situations, and where you might be required to satisfy audit criteria for industry or government oversight.

The next sequence of configuration actions is performed by the Crypto Officer, just now created for the application partition. See "Initialize the Crypto User Role on a PED-Authenticated Partition" below.

Initialize the Crypto User Role on a PED-Authenticated Partition

These instructions assume

- A PED-authenticated SafeNet Luna Network HSM has been initialized

- An application partition has been created

- A Crypto Officer has been created for the partition

- The Crypto Officer PED key has been conveyed to the person responsible for the Crypto Officer role. See "Initialize the Partition SO and Crypto Officer Roles on a PED-Auth Partition" on page 91.

As Crypto Officer, you can:

- Create a Crypto User (limited access user) for the application partition.

- Create, delete, change and manipulate cryptographic objects on the application partition, either for your own use or for use by the Crypto User.

- Activate the partition for use by applications.

To create a Crypto User for the partition, you will need:

- Luna PED and the black Crypto Officer PED key(s) assigned to you by the SO.

- Blank PED key(s) with labels for the Crypto User that you are about to create.

- A local PED connection.

These instructions assume that you have already made your decisions whether to use all-new, blank PED keys, or to re-use any existing, imprinted PED keys for any of the steps.

To create the Crypto User role on a PED-authenticated application partition:

1. Set the active slot to the desired application partition, where the Crypto Officer was just created.

   Type **slot set -slot** <slotnum>

```
lunacm:> slot set -slot 0

       Current Slot Id:   0    (Luna User Slot 7.0.0 (PED) Signing With Cloning Mode)

Command Result : No Error
```

2. Log in as the Crypto Officer. You can also use the shortcut **co**.

   role login -name Crypto Officer

```
lunacm:>role login -name co

       Please attend to the PED.
```

   Respond to Luna PED prompts...

```
Command Result : No Error
```

> **Note:** The black Crypto Officer PED key is valid for the initial login only. You must change the initial credential on the key using the command **role changepw** during the initial login session, or a subsequent login. Failing to change the credential will result in a CKR_PIN_EXPIRED error when you perform role-dependent actions.

3. If you have not already done so, change the initial credential set by the Partition SO.

   role changepw -name Crypto Officer

```
lunacm:>role changepw -name co

       Please attend to the PED.
```

Respond to Luna PED prompts. You must first present the black Crypto Officer key and PIN created by the Partition SO. When you are prompted to present a new black CO key, you can create a new key, or overwrite the original PED key by:

a.   Replying **No** to "Would you like to reuse an existing keyset?"

b.   Pressing **Enter** (without removing the key) when prompted to present a new black PED key

c.   Replying **Yes** when asked if you want to overwrite the original key.

```
Command Result : No Error
```

4.   Create the Crypto User. You can also use the shortcut **cu**. Have a gray Crypto User PED key ready.

role init -name Crypto User

```
lunacm:> role init -name Crypto User

        Please attend to the PED.
```

Respond to Luna PED prompts...

```
    Command Result : No Error
```

> ✎   **Note:** The gray Crypto User PED key is valid for the initial login only. The CU must change the initial credential on the key using the command **role changepw** during the initial login session, or a subsequent login. Failing to change the credential will result in a CKR_PIN_EXPIRED error when they perform role-dependent actions.

The Crypto User can now log in to use applications to perform cryptographic operations using keys and objects created in the partition by the Crypto Officer.

It is possible for all three of Partition SO, Crypto Officer, and Crypto User to perform their functions against a SafeNet Luna Network HSM partition, from the same SafeNet Luna HSM Client host computer, simply taking turns at the keyboard and the Luna PED. It is also possible to work from different computers, as long as any such computer is a registered user of the partition - that is, a working network trust link (NTL) connection is required for each.

In addition, if those persons and their respective SafeNet Luna HSM Client host computers are not co-located, then they must arrange to manage their sharing of the Remote PED. Either

•   One person must maintain the single Remote PED setup, and the others must coordinate closely with the PED-keeper when authentication to the HSM is required,

    or

•   All three can have their own separate PEDs and PedServer instances, but they must coordinate with the appliance administrator to **hsm ped disconnect** any current Remote PED channel before **hsm ped connect -ip <new-ip> -port <new-port>** to establish a Remote PED session with one of the other PedServers.

Crypto Officer or Crypto User Must Remain Logged In

At this point, the Crypto User, or an application using the CU's challenge secret/password can perform cryptographic operations in the partition, as soon as the Crypto User logs in with **role login -name cu**. However, any event that causes that session to close, including action by the application, requires that the CU must log in again (with the gray PED key) before the application partition can be used again. For an application that maintains an open session, that is not a handicap. For an application that opens a session for each action, performs the cryptographic action, then closes the session, the CU must be constantly logging in and using the PED and PED key.

To bypass this limitation, use the Activation feature. See "Activate a PED-Authenticated Partition" below or "SO and CU Activate PED-authenticated PSO Application Partition " on page 1.

Activate a PED-Authenticated Partition

In this section, the Partition SO configures the partition to allow Activation (caching of the authentication credential). Once the Activation policy is set, credentials will be cached the next time the Crypto Officer or Crypto User logs in. This allows the Crypto Officer or Crypto User to log in once using their PED key, and open and close subsequent sessions using only a challenge secret (password). The Partition SO can optionally allow Auto-Activation, which preserves the cached PED credentials in the event of a restart or a brief power outage (up to 2 hours). For more information, see "Activation and Auto-Activation on PED-Authenticated Partitions" on page 1 in the *Administration Guide*.

The Partition SO must set an initial challenge secret for the Crypto Officer, and the Crypto Officer must set one for the Crypto User. See the correct section below for your user role:

- "Partition Security Officer" below
- "Crypto Officer" on the next page
- "Crypto User [Optional]" on page 97

Partition Security Officer

These instructions are for the Partition SO. They assume that:

- You are running LunaCM on a SafeNet Luna HSM Client host computer containing, or connected to, an HSM with an application partition.
- The partition has at least a Crypto Officer role initialized. If the Crypto User role is also initialized, activation will be enabled for both roles.

To enable activation of a PED-authenticated application partition:

1. Set the active slot to the desired application partition.

   slot set -slot <slotnum>

   ```
   lunacm:> slot set -slot 0

           Current Slot Id:    0     (Luna User Slot 7.0.0 (PED) Signing With Cloning Mode)

   Command Result : No Error
   ```

2. Log in as the Partition Security Officer.

   role login -name po

3. Set **partition policy 22: Allow activation** for the partition.

   partition changepolicy -policy 22 -value 1

   ```
   lunacm:> partition changePolicy -policy 22 -value 1

   Command Result : No Error
   ```

4. [Optional] Set **partition policy 23: Allow auto-activation** for the partition.

   partition changepolicy -policy 23 -value 1

   ```
   lunacm:> partition changePolicy -policy 22 -value 1
   ```

```
Command Result : No Error
```

5. Create an initial challenge secret for the Crypto Officer.

    role createchallenge -name co

    ```
    lunacm:>role createchallenge -name co

            Please attend to the PED.

            enter new challenge secret: ********
            re-enter new challenge secret: ********

    Command Result : No Error
    ```

6. Provide the initial challenge secret to the Crypto Officer by secure means. The CO will need to change the challenge secret before using the partition for any crypto operations.

7. Log out as Partition SO.

    role logout

Once policy 22 is set, the black CO PED key credential will be cached the next time the CO logs in. From that point on, only the CO partition challenge secret is required to access the partition. The CO credential remains cached until the HSM loses power, or the role is explicitly deactivated using the command **role deactivate**. The credential is re-cached the next time the CO logs in.

> **Note:** The Partition SO can stop automatic caching of the CO and CU credentials at any time by disabling **partition policy 22: Allow activation** (setting its value to 0).

Crypto Officer

These instructions are for the Crypto Officer. Ensure that you have the initial challenge secret password provided by the Partition SO.

To activate the Crypto Officer role on an application partition:

1. Login to the partition as the Crypto Officer. When prompted, enter the initial challenge secret.

    role login -name co

    ```
    lunacm:>role login -n co

            enter password: ********

            Please attend to the PED.

    Command Result : No Error
    ```

    The Crypto Officer PED secret is cached, and the role is now activated.

2. Change the initial CO challenge secret. You must include the **-oldpw** option to indicate that you wish to change the challenge secret (referred to as the secondary credential), rather than the black PED key (primary credential).

    role changepw -name co -oldpw <initial_challenge> **-newpw** <new_challenge>

    ```
    lunacm:>role changepw -name co -oldpw password -newpw Pa$$w0rd

            This role has secondary credentials.
    ```

```
             You are about to change the secondary credentials.
             Are you sure you wish to continue?

             Type 'proceed' to continue, or 'quit' to quit now ->proceed

             Please attend to the PED.

     Command Result : No Error
```

3.   [Optional] Create an initial challenge secret for the Crypto User.

     role createchallenge -name cu

```
     lunacm:>role createchallenge -name cu

             Please attend to the PED.

             enter new challenge secret: ********
             re-enter new challenge secret: ********

     Command Result : No Error
```

4.   [Optional] Provide the initial challenge secret to the Crypto User by secure means. The CU will need to change the challenge secret before using the partition for any crypto operations.

5.   Log out as Crypto Officer.

     role logout

With activation in place, you can log in once and put your black CO PED key away in a safe place. The cached credentials will allow your application(s) to open and close sessions and perform their operations within those sessions.

Crypto User [Optional]

These instructions are for the Crypto User. Ensure that you have the initial challenge secret password provided by the Crypto Officer.

To activate the Crypto User role on an application partition:

1.   Login to the partition as the Crypto User. When prompted, enter the initial challenge secret.

     role login -name cu

```
     lunacm:>role login -n cu

             enter password: ********

             Please attend to the PED.

     Command Result : No Error
```

2.   Change the initial CU challenge secret. You must include the **-oldpw** option to indicate that you wish to change the challenge secret (referred to as the secondary credential), rather than the gray PED key (primary credential).

     role changepw -name cu -oldpw <initial_challenge> **-newpw** <new_challenge>

```
     lunacm:>role changepw -name cu -oldpw password -newpw Pa$$w0rd

             This role has secondary credentials.
             You are about to change the secondary credentials.
             Are you sure you wish to continue?
```

```
        Type 'proceed' to continue, or 'quit' to quit now ->proceed

        Please attend to the PED.

   Command Result : No Error
```

With activation in place, you can log in once and put your gray CO PED key away in a safe place. The cached credentials will allow your application(s) to open and close sessions and perform their operations within those sessions.

Set Partition Policies

At this point, you should have initialized the partition and created the Crypto Officer role. All administration of an initialized partition is carried out by the Partition SO, via LunaCM, from a registered client computer. Before deploying the partitions, review and set the policies constraining the use of the partition by clients, as described in the following sections:

- "Displaying the Current Partition Policy Settings" below

- "Changing the Partition Policy Settings" on the next page

- "RSA Blinding Mode" on page 101

Displaying the Current Partition Policy Settings

First, display the policies (default) of the application partition. You can run the **partition showpolicies** command without logging in. The Partition SO must be logged in to change partition policy settings.

To display the current partition policy settings:

1. Open a LunaCM session.

2. Enter the following command to display current partition capability and policy settings. Capabilities are factory settings. Policies are the means of modifying the adjustable capabilities:

partition showpolicies [**-slot** <slotnum>]

For example:

```
lunacm:> partition showpolicies
        Partition Capabilities
                0: Enable private key cloning : 1
                1: Enable private key wrapping : 0
                2: Enable private key unwrapping : 1
                3: Enable private key masking : 0
                4: Enable secret key cloning : 1
                5: Enable secret key wrapping : 1
                6: Enable secret key unwrapping : 1
                7: Enable secret key masking : 0
               10: Enable multipurpose keys : 1
               11: Enable changing key attributes : 1
               15: Allow failed challenge responses : 1
               16: Enable operation without RSA blinding : 1
               17: Enable signing with non-local keys : 1
               18: Enable raw RSA operations : 1
               20: Max failed user logins allowed : 10
               21: Enable high availability recovery : 1
               22: Enable activation : 0
               23: Enable auto-activation : 0
               25: Minimum pin length (inverted: 255 - min) : 248
               26: Maximum pin length : 255
               28: Enable Key Management Functions : 1
```

```
                29: Enable RSA signing without confirmation : 1
                31: Enable private key unmasking : 1
                32: Enable secret key unmasking : 1
                33: Enable RSA PKCS mechanism : 1
                34: Enable CBC-PAD (un)wrap keys of any size : 1
                35: Enable private key SFF backup/restore : 0
                36: Enable secret key SFF backup/restore : 0
                37: Enable Secure Trusted Channel : 1
                38: Enable  Fast-Path : 0
                39: Enable  Start/End Date Attributes : 1

        Partition Policies
                 0: Allow private key cloning : 1
                 1: Allow private key wrapping : 0
                 2: Allow private key unwrapping : 1
                 3: Allow private key masking : 0
                 4: Allow secret key cloning : 1
                 5: Allow secret key wrapping : 1
                 6: Allow secret key unwrapping : 1
                 7: Allow secret key masking : 0
                10: Allow multipurpose keys : 1
                11: Allow changing key attributes : 1
                15: Ignore failed challenge responses : 1
                16: Operate without RSA blinding : 1
                17: Allow signing with non-local keys : 1
                18: Allow raw RSA operations : 1
                20: Max failed user logins allowed : 10
                21: Allow high availability recovery : 1
                22: Allow activation : 0
                23: Allow auto-activation : 0
                25: Minimum pin length (inverted: 255 - min) : 248
                26: Maximum pin length : 255
                28: Allow Key Management Functions : 1
                29: Perform RSA signing without confirmation : 1
                31: Allow private key unmasking : 1
                32: Allow secret key unmasking : 1
                33: Allow RSA PKCS mechanism : 1
                34: Allow CBC-PAD (un)wrap keys of any size : 1
                35: Allow private key SFF backup/restore : 0
                36: Allow secret key SFF backup/restore : 0
                37: Force Secure Trusted Channel : 0
                38: Allow Fast-Path : 0
                39: Allow Start/End Date Attributes : 0

    Command Result : No Error
```

Changing the Partition Policy Settings

Having viewed the Policy settings, you can now modify a Partition Policy for a given partition.

To change a partition policy:

1. Open a LunaCM session, select the partition slot, and login as Partition SO.

    slot set slot <slotnum>
    role login -name po

2. Enter the following command to change a Partition Policy:

    partition changepolicy -policy <policy_id> **-value** <policy_value>

RSA Blinding Mode

Blinding is a technique that introduces random elements into the signature process to prevent timing attacks on the RSA private key. Use of this technique may be required by certain security policies, but it does reduce performance.

The Partition Security Officer can turn this feature on or off.

If RSA blinding is enabled in Capabilities and allowed in Policies, the partition will always run in RSA blinding mode; performance will be lower than SafeNet published performance figures. This is because the deliberate introduction of random elements causes the average signature to take longer to complete.

For maximum performance, you can switch RSA blinding mode off, at the cost of additional risk of timing attacks on your keys. It is your decision whether your network and other security measures are sufficiently rigorous that blinding is not needed.

SafeNet Luna HSMs are normally shipped with the Capability set to allow switching blinding on or off, and with the Policy set to not use blinding, by default.

Optional Configuration Tasks

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

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

You can synchronize a SafeNet Luna Network HSM appliance with a network time protocol (NTP) server. NTP provides a reliable, consistent, and accurate timing mechanism for the appliance using Coordinated Universal Time (UTC), and is the recommended option for providing an accurate date and time for the appliance. SafeNet Luna Network HSM also provides secure NTP. See "Timestamping – NTP and Clock Drift" on page 1 in the *SafeNet Luna Network HSM Appliance Administration Guide.*

Configure multiple HSMs to operate in high-availability (HA) mode

High Availability (HA) mode allows you to automatically replicate the data on a HSM/partition over two or more physical HSMs to provide redundancy and load balancing. Applications using an HA HSM/partition do not access it directly. Instead, the HA software creates a virtual slot for the partition and manages which physical HSM is actually used when responding to an application request. See "High-Availability (HA) Configuration and Operation" on page 1 in the *Administration Guide*.

Configure SNMP

You can use the SafeNet SNMP MIB to monitor the performance of your HSMs. See "SNMP Monitoring" on page 1 in the *Administration Guide*.

Configure a remote PED

If you are configuring a PED-authenticated HSM, you can configure it to use a remote PED, which allows you to authenticate to the HSM from a remote location. See "About Remote PED" on page 1 in the *Administration Guide*.

Configure for RADIUS Authentication

RADIUS (Remote Authentication Dial-In User Service) is a client/server protocol providing authentication, authorization, and accounting service to configured clients. The client passes user information to configured, designated RADIUS servers, and acts on the returned response. A RADIUS server receives user connection requests, authenticates the user if that user's profile exists on the server, and then returns the configuration information according to which the client can deliver service to the user.

While a proposal is being considered (by the custodians of the RADIUS standard) to switch to TLS communication protocol, RADIUS interaction currently takes place over UDP (User Datagram Protocol).

RADIUS Configuration Summary

Configuration and identification must take place at both ends of the RADIUS transaction. These actions include:

On the RADIUS Server Side

- Identify the client systems from which this server will accept requests and return service (this is recorded in the RADIUS server's configuration file).

- Identify the users who will be covered by the service.

On the RADIUS Client Side (Your SafeNet Luna Network HSM)

- Enable RADIUS.

- Add a RADIUS server, specifying its IP address, and providing the access secret for that server.

- Check the status of SafeNet Luna Network HSM appliance users.

- Add desired SafeNet Luna Network HSM appliance users to the RADIUS list, enabling RADIUS authentication for those users.

- Verify that RADIUS is enabled for any user on your SafeNet Luna Network HSM that needs to use RADIUS.

Configuring RADIUS with Your SafeNet Appliance

Follow these steps on the RADIUS Server:

You can use any standards-compliant RADIUS server, either a commercial server or one of the free/open-source servers, like freeRADIUS or openRADIUS.

1. Add the client to the RADIUS server's configuration file, specifying:

   – The address of the SafeNet Luna Network HSM appliance.

   – The secret or password that the client will use when connecting.

   – A short, user-friendly or business-relevant name for the client.

   You can edit the file directly, for some RADIUS implementations, or use the provided interface.

   ```
   /etc/raddb/clients.conf:

   client 192.20.17.174 {
           ipaddr          = 192.20.17.174
           secret          = testing123
           nas             = other
           shortname       = sa174
   }
   client 192.20.22.106 {
           ipaddr          = 192.20.22.106
           secret          = testing321
           nas             = other
           shortname       = sa22106
   }
   ```

2. For each client, add the user name and the password for that user to the "users" file of the RADIUS server.

   ```
       /etc/raddb/users:

   sauser162       Cleartext-Password := "userpw654"
   sauser171       Cleartext-Password := "userpw987"
   sauser172       Cleartext-Password := "userpw789"
   sauser173       Cleartext-Password := "userpw456"
   sauser174       Cleartext-Password := "userpw321"
   nagios          Cleartext-Password := "nagiospw"
   audit           Cleartext-Password := "userpin"
   ```

```
someguy              Cleartext-Password := "userpw"
sauser106            Cleartext-Password := "userpw123"
```

A user can use RADIUS for a SafeNet Luna Network HSM, only if that SafeNet Luna Network HSM is registered as a client, and if that user is registered as a user in the appropriate files on the RADIUS server.

Follow these steps on the SafeNet Luna Network HSM appliance:

> **Note:** Without RADIUS, use the command **user add user somename** to add an appliance administrative user on SafeNet Luna Network HSM.
>
> With RADIUS, use the command **user radiusAdd -u somename** to both create the user on the appliance and add that user to the RADIUS list. You cannot use **user radiusAdd** to convert an existing user from non-RADIUS to RADIUS.

1. On the SafeNet Luna Network HSM appliance, enable RADIUS with the command **sysconf radius enable**.

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

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

   Enter the server secret:
   Re-enter the server secret:
   Command Result : 0 (Success)
   ```

3. Verify that the desired server has been added.

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

   RADIUS for SSH is enabled with the following deployed servers:

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


   Command Result : 0 (Success)
   ```

4. Check the user list to see which users exist, are enabled on the SafeNet appliance, and are RADIUS enabled.

   ```
   [1722022106] lunash:>user list

               Users        Roles      Status      RADIUS
   -------------------    --------    --------    --------
               admin         admin     enabled          no
               audit         audit     enabled          no
             monitor       monitor    disabled          no
            operator      operator    disabled          no

   Command Result : 0 (Success)
   ```

5. Add a user, by name, as a RADIUS user.

   ```
   [1722022106] lunash:>user radiusAdd -u someguy

   Creating mailbox file: File exists
   Stopping sshd:                                            [  OK  ]
   Starting sshd:                                            [  OK  ]
   ```

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

6. Add the user's appliance role (in this example, we are giving him admin-level access).

```
[1722022106] lunash:>user role add -u someguy -r admin

User someguy was successfully modified.

Command Result : 0 (Success)
```

7. Verify that the user exists, has the correct role on the SafeNet appliance, and is a RADIUS user for this appliance.

```
[1722022106] lunash:>user list

              Users       Roles      Status     RADIUS
    --------------------  --------   --------   --------
                 admin      admin    enabled         no
                 audit      audit    enabled         no
               someguy      admin    enabled        yes
               monitor    monitor   disabled         no
              operator   operator   disabled         no

Command Result : 0 (Success)
[1722022106] lunash:>
```