# THALES

# Luna HSM Client 10.2
# for SafeNet Luna Network HSM

## PRODUCT OVERVIEW

## Document Information

| | |
|---|---|
| **Product Version** | 10.2 |
| **Document Part Number** | 007-000553-002 |
| **Release Date** | 15 June 2020 |

## Revision History

| Revision | Date | Reason |
|---|---|---|
| Rev. A | 15 June 2020 | Initial release |

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.

Thales Group 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 Thales Group be held liable for any third party actions and in particular in case of any successful attack against systems or equipment incorporating Thales Group products. Thales Group 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 Thales Group.

## 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 Thales-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 Product Overview

For an overview of new features in this release, see "New Features and Enhancements" on page 19.

This document provides an overview of the SafeNet Luna HSM suite of products. It contains the following chapters:

The preface includes the following information about this document:

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.thalesgroup.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 Thales Group 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:<br>> Command-line commands and options (Type **dir /p**.)<br>> Button names (Click **Save As**.)<br>> Check box and radio button names (Select the **Print Duplex** check box.)<br>> Dialog box titles (On the **Protect Document** dialog box, click **Yes**.)<br>> Field names (**User Name**: Enter the name of the user.)<br>> Menu names (On the **File** menu, click **Save**.) (Click **Menu** > **Go To** > **Folders**.)<br>> 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**]<br>[<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}<br>{<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]<br>[<a>\|<b>\|<c>] | Represent optional alternate keywords or variables in a command line description. Choose one command line argument enclosed within the braces, if desired. Choices are separated by vertical (OR) bars. |

# Support Contacts

If you encounter a problem while installing, registering, or operating this product, please refer to the documentation before contacting support. If you cannot resolve the issue, contact your supplier or Thales Customer Support.

Thales Customer Support operates 24 hours a day, 7 days a week. Your level of access to this service is governed by the support plan arrangements made between Thales and your organization. Please consult this support plan for further information about your entitlements, including the hours when telephone support is available to you.

## Customer Support Portal

The Customer Support Portal, at https://supportportal.thalesgroup.com, is where you can find solutions for most common problems. The Customer Support Portal is a comprehensive, fully searchable database of support resources, including software and firmware downloads, release notes listing known problems and workarounds, a knowledge base, FAQs, product documentation, technical notes, and more. You can also use the portal to create and manage support cases.

> **NOTE**  You require an account to access the Customer Support Portal. To create a new account, go to the portal and click on the **REGISTER** link.

## Telephone

The support portal also lists telephone numbers for voice contact (Contact Us).

# CHAPTER 1:   SafeNet Luna Hardware Security Modules

Hardware Security Modules (HSMs) are dedicated systems that physically and logically secure cryptographic keys and cryptographic processing. The purpose of an HSM is to protect sensitive data from being stolen by providing a highly secure operation structure. HSMs are fully contained and complete solutions for cryptographic processing, key generation, and key storage. They are purpose-built appliances that automatically include the hardware and firmware (i.e., software) necessary for these functions in an integrated package.

An HSM manages cryptographic keys used to lock and unlock access to digitized information over their life-cycle. This includes generation, distribution, rotation, storage, termination, and archival functions. An HSM also engages in cryptographic processing, which produces the dual benefits of isolation and offloading cryptographic processing from application servers.

HSMs are available in the following forms:

> Standalone network-attached appliances, as described in "SafeNet Luna Network HSM" below.

> Hardware cards that plug into existing network-attached systems, as described in "SafeNet Luna PCIe HSM" on page 14.

> USB-connected backup HSMs, as described in "SafeNet Luna Backup HSM" on page 15

See the following topics for a comparison of the PCIe and Network HSMs, and for a description of the available HSM models:

> "Comparing the SafeNet Luna Network HSM Appliance and PCIe HSM" on page 15

> "SafeNet Luna HSM Models" on page 15

For a high level overview of the distinctive features of the SafeNet Luna Network HSM and SafeNet Luna PCIe HSM, see "SafeNet Luna HSM Features" on page 17.

## SafeNet Luna Network HSM

SafeNet Luna Network HSM stores, protects, and manages sensitive cryptographic keys in a centralized, high-assurance appliance, providing a root of trust for sensitive cryptographic data transactions. Deployed in more public cloud environments than any other HSM, SafeNet Luna Network HSM works seamlessly across your on-premises, private, public, hybrid, and multi-cloud environments. SafeNet Luna Network HSM is the most trusted general purpose HSM on the market, and with market leading performance, true hardware-based security, and the broadest ecosystem available, SafeNet Luna Network HSM is at the forefront of HSM innovation.

## Ethernet-attached

An Ethernet-attached HSM, SafeNet Luna Network HSM is designed to protect critical cryptographic keys and accelerate sensitive cryptographic operations across a wide range of security applications. It includes many features that increase security connectivity and ease-of-administration in dedicated and shared security applications.

## Integrated Cryptographic Engine

The SafeNet Luna Network HSM can be shared between multiple applications or clients connected to it through a network. In the same way that mail and web servers provide email or web pages to authenticated clients, the SafeNet Luna Network HSM offers powerful key management and high-performance cryptographic processing to clients on the network. To achieve this, the SafeNet Luna Network HSM includes an integrated FIPS 140-2- validated HSM and the Cryptographic Engine, which offers the same high level of security as traditional HSMs. Additionally, the SafeNet Luna Network HSM adds a secure service layer that allows the Cryptographic Engine to be shared between network clients.

## Partitions

The SafeNet Luna Network HSM also introduces the concept of HSM partitions, a feature that allows the SafeNet Luna Network HSM's single physical HSM to be divided into several logical HSM partitions, each with independent data, access controls, and administrative policies. HSM partitions can be thought of as 'safety deposit boxes' that reside within the Cryptographic Engine's 'vault'. The vault itself offers an extremely high level of security for all the contents inside, while the safety deposit boxes protect their specific contents from people who have access to the vault. HSM partitions allow separate data storage and administration policies to be maintained by multiple applications sharing one HSM without fear of compromise from other partitions residing on it. Each HSM partition has a special access control role who manages it. Depending on the configuration, each SafeNet Luna Network HSM can contain up to 100 partitions.

## Dedicated Clients

HSM partitions can be dedicated to a single Client, or multiple Clients that share access to a single HSM partition. Clients are applications, or application servers, that connect to the SafeNet Luna Network HSM. Examples of possible clients are an encrypted database, a secure web server, or a Certificate Authority (CA); all these applications require the storage of sensitive cryptographic data or can benefit from the increased security and cryptographic performance offered by the SafeNet Luna Network HSM. Each Client is assigned to one or more specific HSM partitions. Clients authenticate to the SafeNet Luna Network HSM with a digital certificate and unique HSM partition challenge.

## Employ the HSM as a Service

SafeNet Luna Network HSM empowers organizations to take a best practices approach to cryptographic key security by offloading cryptographic processes to a centralized, high-assurance key vault that can be deployed as a service. Only the SafeNet Luna Network HSM is able to provide trusted key owner ship and control, with full multi-tenancy across on-premises, private, public, hybrid, and multi-cloud environments.

## Sample Deployment Architecture

The following sample architecture illustrates potential connections between your SafeNet Luna HSM(s), server(s), and workstation(s). Some of the elements are optional configuration items, and might not be present in your system.

**Figure 1: Network HSM Connections**
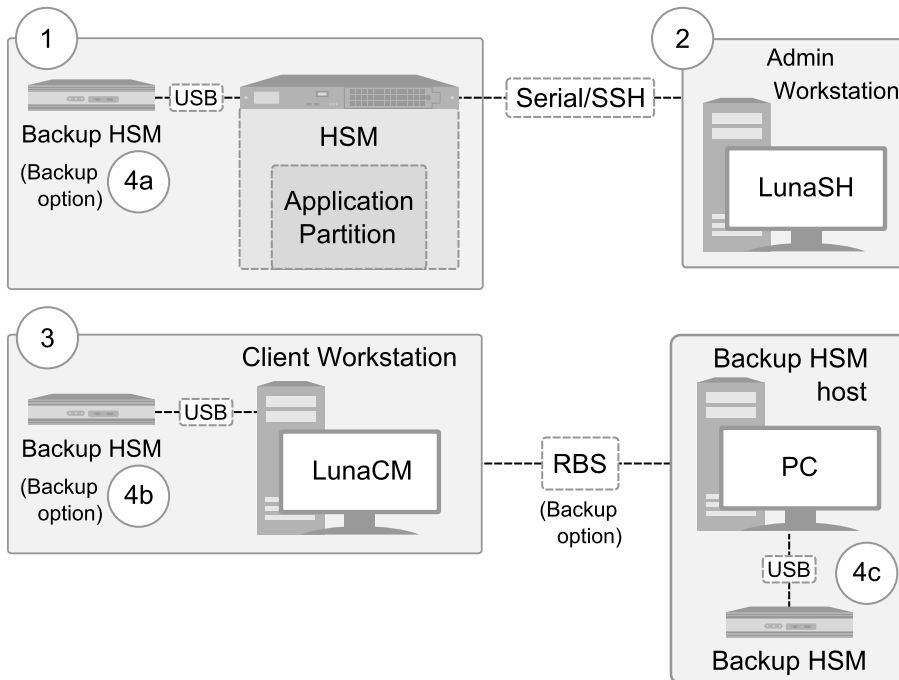


1. Within your SafeNet appliance lies an HSM. That HSM holds one or more application partitions (independent virtual HSMs) that different users or clients can access.

2. Initial setup of your HSM requires you to connect directly to it via serial cable. Post-setup, you can use SSH to remotely access your HSM. Both of these connections use LunaSH, the command-line interface or shell for appliance and HSM configuration and management.

3. To perform cryptographic operations with your HSM or Partition, you must login remotely through the Luna HSM Client at your workstation. The client uses LunaCM for the configuration and administration of your Partition, and uses cryptographic APIs such as PKCS#11, Java, JCPROV, CSP, and KSP to perform significant cryptographic operations.

4. Backup HSMs are used exclusively to securely backup sensitive material from SafeNet Luna HSMs, and to restore backed-up material to SafeNet Luna HSMs. The SafeNet Luna Backup HSM can be connected using any of the following methods:

   • To the appliance containing the primary HSM or

   • To a client workstation that can access the HSM

   • Via Remote Backup Service (RBS) to a separate Backup HSM host, which allows you to further remove your backup to a more remote location.

# SafeNet Luna PCIe HSM

SafeNet Luna PCIe HSM stores, protects, and manages sensitive cryptographic keys in a small form factor PCIe card, providing a root of trust for sensitive cryptographic data transactions. With SafeNet Luna PCIe HSM cryptographic processes are offloaded to a high-performance cryptographic processor. SafeNet Luna PCIe HSM easily embeds in servers and security appliances for an easy-to-integrate and cost-efficient solution for FIPS 140-2 validated key security. SafeNet Luna PCIe HSM benefits from a diverse feature set that enables greater centralized control through secure remote management, transport, and backup.

## Single-partition

The SafeNet Luna PCIe HSM is a single-partition HSM card that you can embed in a pre-existing network-attached system. Access to the partition is managed by a special access control role. The SafeNet Luna PCIe HSM offers hardware accelerated ECC algorithms that can be used in the development of solutions for resource constrained environments (devices like smart phones, tablets, etc.), without the need to purchase additional licenses. ECC offers high key strength at a greatly reduced key length compared to RSA keys; higher security with fewer resources.

## Cost Effective

Like in the SafeNet Luna Network HSM, the SafeNet Luna PCIe HSM securely stores cryptographic keys in its hardware; sensitive information never leaves the HSM protection. The SafeNet Luna PCIe HSM provides PKCS#11-compliant cryptographic services for applications running on the server in a secure and tamper-proof hardware package. Leveraging a SafeNet Luna PCIe HSM in your appliance or service represents a cost effective way to bring FIPS 140-2 and Common Criteria validated solutions to market.

SafeNet Luna PCIe HSM empowers organizations to take a best practices approach to cryptographic key security by offloading cryptographic processes to a dedicated small form factor cryptographic processor. SafeNet Luna PCIe HSM is the highest performing embedded HSM on the market.

## Sample Deployment Architecture

The following sample architecture illustrates potential connections between your SafeNet Luna HSM(s), server (s), and workstation(s). Some of the elements are optional configuration items, and might not be present in your system.
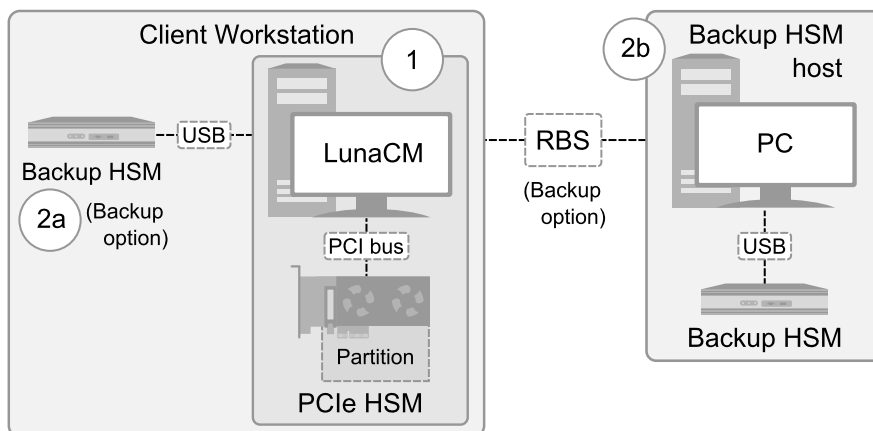
1. The PCIe HSM is a small card that fits in your system's connector slots, and it is accessed directly through the Luna HSM Client at your workstation. The client uses LunaCM for the configuration and administration of your PCIe HSM, and uses cryptographic APIs to perform cryptographic operations requested by your applications.

2. Backup HSMs are used exclusively to securely backup sensitive material from SafeNet Luna HSMs, and to restore backed-up material to SafeNet Luna HSMs. The SafeNet Luna Backup HSM can be connected using any of the following methods:

   - To the client host containing the primary HSM
   - Via Remote Backup Service (RBS) to a separate Backup HSM host, which allows you to further remove your backup to a more remote location.

# SafeNet Luna Backup HSM

The SafeNet Luna Backup HSM allows you to backup the objects in your Network or PCIe user partitions and store the object archive in a secure HSM. Backup HSMs are able to store objects only. They do not provide the ability to access the objects to perform cryptographic operations. See "Flexible Backups" on page 59 for more information.

Two versions are available, as detailed in "Backup HSM Models" on page 17.

# Comparing the SafeNet Luna Network HSM Appliance and PCIe HSM

| SafeNet Luna Network HSM Appliance | SafeNet Luna PCIe HSM |
| --- | --- |
| > Field-upgradable to 100 partitions <br> > Includes hardened OS <br> > High security, stable networking, and environmental protection via built-in chassis <br> > Routine firmware and software updates <br> > Automatic system logging | > Limited to 1 partition <br> > Compatible with external OS: Windows, Linux <br> > Allows custom and flexible chassis intrusion security <br> > Routine firmware updates <br> > Light and low-cost |

A database server using an HSM would require one HSM, while a secure website using SSL on the same network would require a second, separate HSM. As the number of secure applications requiring an HSM grows, so does the number of ordinary HSMs deployed. The SafeNet Luna Network HSM bypasses this limitation by implementing multiple virtual HSMs, or HSM Partitions on a single HSM server. A PCIe HSM is useful for cases that need limited, but highly secure, data protection. A Network HSM and its appliance are useful for cases that require a more complex security infrastructure, like cloud computing.

# SafeNet Luna HSM Models

Both the SafeNet Luna Network HSM and the SafeNet Luna PCIe HSM come in different models with different performance capabilities. Which one you choose to use will depend on your organization's security needs.

> **NOTE** The FIPS levels below indicate the standard to which the product is designed. Always confirm the HSM certification status before deploying an HSM in a regulated environment.

## Luna A (Password-authenticated, FIPS Level 3) Models

Luna A models offer secure storage of your cryptographic information in a controlled and easy-to-manage environment. Luna A models protect your proprietary information by using password authentication. Depending on your needs, Luna A models are available at several performance levels, as follows:

| Model | SafeNet Luna Network HSM | SafeNet Luna PCIe HSM |
|-------|--------------------------|------------------------|
| **Luna A700** | > Standard performance<br>> 2MB memory<br>> Password-based authentication<br>> 5 partitions | > Standard performance<br>> 2MB memory<br>> Password-based authentication |
| **Luna A750** | > Enterprise-level performance<br>> 16MB memory<br>> Password-based authentication<br>> 5 partitions, upgradable to 20 | > Enterprise-level performance<br>> 16MB memory<br>> Password-based authentication |
| **Luna A790** | > Maximum performance<br>> 32MB memory<br>> Password-based authentication<br>> 10 partitions, upgradable to 100 | > Maximum performance<br>> 32MB memory<br>> Password-based authentication |

## Luna S (PED-authenticated, FIPS Level 3) Models

Luna S models offer secure storage of your cryptographic information in a controlled and highly secure environment. Luna S models protect your proprietary information by using multifactor (PED) authentication. Depending on your needs, Luna S models are available at several performance levels, as follows:

| Model | SafeNet Luna Network HSM | SafeNet Luna PCIe HSM |
|-------|--------------------------|------------------------|
| **Luna S700** | > Standard performance<br>> 2MB memory<br>> Multifactor authentication<br>> 5 partitions | > Standard performance<br>> 2MB memory<br>> Multifactor authentication |
| **Luna S750** | > Enterprise-level performance<br>> 16MB memory<br>> Multifactor authentication<br>> 5 partitions, upgradable to 20 | > Enterprise-level performance<br>> 16MB memory<br>> Multifactor authentication |

| Model | SafeNet Luna Network HSM | SafeNet Luna PCIe HSM |
|---|---|---|
| Luna S790 | > Maximum performance<br>> 32MB memory<br>> Multifactor authentication<br>> 10 partitions, upgradable to 100 | > Maximum performance<br>> 32MB memory<br>> Multifactor authentication |

## Backup HSM Models

Backup HSMs offer secure backups of your SafeNet Luna HSM user partitions. They can be initialized in either PED-authenticated or password-authenticated mode:

> PED-authenticated backup HSMs can backup PED-authenticated partitions.

> Password-authenticated backup HSMs can backup password-authenticated partitions.

Two versions are available:

> the G5-based desktop model.

> the G7-based hand-held model is available in the following models. Each model allows you to backup up to 100 partitions. In-field storage upgrades are not available.

| | |
|---|---|
| B700 | 32 MB storage. 100 partitions |
| B750 | 128 MB storage. 100 partitions |

# SafeNet Luna HSM Features

SafeNet Luna HSMs have a variety of features that distinguish them, as summarized below:

| Security | SafeNet Luna HSMs are manufactured to high security standards and are currently seeking FIPS Level 3 and Common Criteria certifications. SafeNet Luna HSMs protect your data from unwanted tampering with secure anti-intrusion and vulnerability detection mechanisms.<br>See "Security" on page 33 for details. |
|---|---|
| Redundancy | SafeNet Luna HSMs are equipped with physical features and configurations that enable auto-recovery of your HSMs.<br>See "Redundancy and Reliability" on page 38 for details. |
| Networking | SafeNet Luna HSMs support secure NTLS and STC network connections for client applications. The SafeNet Luna Network HSM appliance has multiple ports, allowing flexible network connections.<br>See "Networking" on page 41 for details. |
| Access control | SafeNet Luna HSM products offer multiple identities, some mandatory and some optional, that you can invoke in different ways to map to roles and functions in your organization.<br>See "User Access Control" on page 45 for details. |

| | |
|---|---|
| **Authentication** | SafeNet Luna HSMs are factory configured to be either<br><br>> password-authenticated (single-factor authentication) or<br><br>> PED-authenticated (multi-factor authentication with option for quorum authentication),<br><br>depending on the level of security and oversight with which you wish to protect your data.<br>See "Authentication" on page 48 for details. |
| **Administration** | The SafeNet Luna Network HSM appliance can be managed using several administrative interfaces.<br>See "Appliance Administration" on page 55 for details. |
| **Capabilities and policies** | SafeNet Luna HSMs, and partitions within them, are characterized by capabilities that are set at the factory or added by means of capability updates, and that are adjusted by means of settable policies that correspond to some of them.<br>See "Capabilities and Policies" on page 57 for details. |
| **Backups** | SafeNet Luna HSMs contain sensitive material that, if lost, could be detrimental. The SafeNet Luna Backup HSM and RBS securely back up and store such information that can be restored in case of failures in primary HSM functioning.<br>See "Flexible Backups" on page 59 for details. |
| **Logging and reporting** | SafeNet Luna HSMs are equipped with performance monitoring and audit logging features to monitor security and provide audits of HSM activity.<br>See "Logging and Reporting" on page 62 for details. |

# CHAPTER 2:   New Features and Enhancements

Thales Group has introduced many new features and enhancements to SafeNet Luna Network HSM 7 since the initial release, as described below.

## Luna HSM Client 10.2.0

### New Luna HSM Client Operating System Support

Luna HSM Client 10.2.0 can be installed on the following new operating systems:

> Windows Server Core 2016/2019

> Red Hat Enterprise Linux 8 (including variants like CentOS 8)

> AIX 7.2

### Support for New Mechanisms in Luna HSM Firmware 7.4.2

Luna HSM Client 10.2.0 includes support for Luna HSM firmware 7.4.2 mechanisms.

> 3GPP Mechanisms for 5G Mobile Networks

> SM2/SM4 Mechanisms

> SHA-3 Mechanisms

## Luna HSM Firmware 7.4.2

This release adds support for 3GPP, SM2/SM4, and SHA-3 cryptographic functions to SafeNet Luna Network HSMs. It consists of:

> Luna HSM firmware 7.4.2

> Luna HSM Client 7.4.0 software patch

## 3GPP Cryptography for 5G Mobile Networks

The new 3GPP crypto functions support the authentication and re-synchronization of a mobile device to the back-end authentication center (AUC). Milenage, Tuak and Comp128 algorithms are available and are relevant to 2/2.5G, 3G, 4G(LTE) and newer 5G mobile networks. The primary benefit of using the Luna HSM ensures that the subscribers key (Ki) is never exposed in the clear outside the security perimeter of a hardware security device. Optionally the Operators Variant string (OP) may also be encrypted under a storage key only found inside the HSM.

See 3GPP Mechanisms for 5G Mobile Networks.

## SM2/SM4 Support

SM2 is comparable to Elliptic Curve (EC) in terms of key structure though the signing algorithm is different. SM2 is required for sign/verify. There is a new key type CKK_SM2. SM4 is comparable to Advanced Encryption Standard (AES-128) in terms of key size though the encryption algorithm is different. SM4 is required for encrypt/decrypt (modes ECB, CBC, CBC-PAD). There is a new key type CKK_SM4.

See SM2/SM4 Mechanisms.

## SHA-3 Function Support

This provides a guide to using the SHA-3 crypto functions in the Luna HSM. The SHA-3 implementation conforms to the NIST publication FIPS PUB 202. The SHA-3 hash algorithm has been implemented in the K7 FW. This provides the ability to send message data to the Luna HSM in order to receive the SHA-3 digest of the data. The algorithm is implemented for digest bit lengths of 224, 256, 384 and 512 similar to the SHA-2 family of hash algorithms. Other mechanisms that make use of a digest include support for SHA-3 by either specifying the mechanism type or specifying mechanism parameters.

See SHA-3 Mechanisms.

# Luna HSM Client 10.1.0

This release consists of:

> Luna HSM Client 10.1.0

## Luna HSM Client 10.1 Supports Both Luna HSMs and DPoD HSM on Demand Services

Luna HSM Client can now be used with HSM on Demand services provided by SafeNet Data Protection on Demand. This allows you to migrate keys from a password-authenticated Luna HSM partition to an HSMoD service or vice-versa, set up High-Availability (HA) groups that include both password-authenticated Luna partitions and HSMoD services, and operate your local (Luna PCIe), remote (Luna Network), and cloud (HSMoD) HSM solutions on the same client workstation.

HSMoD client compatibility is limited to Windows and Red Hat Enterprise Linux 7-based operating systems in this release.

Refer to the following sections:

> Adding a DPoD HSM on Demand Service

> **>**   Cloning Keys Between Luna 6, Luna 7, and HSM on Demand

# G7-based SafeNet Luna Backup HSM
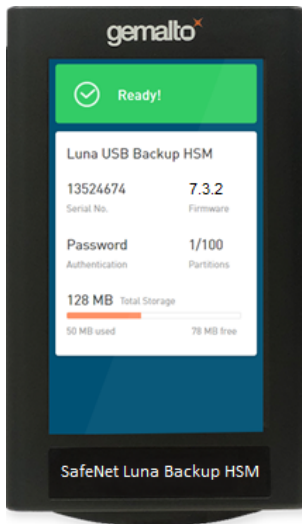
Thales is pleased to announce the availability of the G7-based SafeNet Luna Backup HSM – a full-featured, hand-held, USB-attached backup HSM that includes an informational full-color display.

You can use the SafeNet Luna Backup HSM to backup your Luna HSM 5.x, 6.x, and 7.x user partitions.

The SafeNet Luna Backup HSM connects easily to a client workstation using the included USB 3.0 Type C cable, and includes a universal 5V external power supply, which may be required to power the device in some instances.

> **NOTE**   The smart card slot located at the bottom front of the unit is reserved for future use and has been disabled in this release.

For detailed usage instructions, see Backing Up Partition Objects to a G7-based Backup HSM.

## Models

The G7-based SafeNet Luna Backup HSM is available in the following models. All models can be initialized in PED or password-authenticated mode for backing up either PED or password authenticated partitions. In-field storage upgrades are not available.

| | |
|---|---|
| **B700** | 32 MB storage. Up to 100 partitions of the same authentication type. |
| **B750** | 128 MB storage. Up to 100 partitions of the same authentication type. |

To use the G7-based SafeNet Luna Backup HSM, you must upgrade to Luna HSM Client 10.1, a client-only field update for Linux and Windows. Luna HSM Client 10.1 provides the drivers and software updates you need to use the G7-based SafeNet Luna Backup HSM.

# Remote PED Support on Linux

You can now host Remote PED services on a Linux workstation.

See Remote PED Setup.

# Client Certificates Signed by a Trusted Certificate Authority

Luna HSM Client 10.1 allows you to use client certificates signed by a trusted Certificate Authority (CA), which can be a commercial third-party CA or your organization's own signing station.

See Creating an NTLS Connection Using a Client Certificate Signed by a Trusted Certificate Authority.

## Windows Secure Boot Support

The drivers included with the Luna HSM Client software for Luna PCIe HSMs, Luna Backup HSMs, Luna USB HSMs, and Luna PEDs now support Windows Secure Boot.

# SafeNet Luna Network HSM Release 7.4

This release consists of:

> Luna HSM Client 7.4.0

> SafeNet Luna Network HSM appliance software 7.4.0

> Luna HSM firmware 7.4.0

## Functionality Modules

SafeNet Luna Network HSM 7.4 introduces Functionality Modules (FMs). FMs consist of your own custom-developed code, loaded and operating within the logical and physical security of a SafeNet Luna Network HSM as part of the HSM firmware. FMs allow you to customize your SafeNet Luna Network HSM's functionality to suit the needs of your organization. Custom functionality provided by your own FMs can include:

> new cryptographic algorithms, including Quantum algorithms

> security-sensitive code, isolated from the rest of the HSM environment

> keys and critical parameters managed by the FM, independent from standard PKCS#11 objects, held in tamper-protected persistent storage

To create FMs, you will need the Functionality Module Software Development Kit (SDK), which is included with the Luna HSM Client software. Applications that use FM functions are supported on Windows and Linux.

> **CAUTION!**  Enabling FMs (**HSM policy 50**) introduces changes to Luna HSM functionality, some of which are permanent; they cannot be removed by disabling the policy. FM-enabled status is **not** reversible by Factory Reset. Refer to "FM Deployment Constraints" on page 1 for details before enabling.

See "About the FM SDK Programming Guide" on page 1 and "Functionality Modules" on page 1 for details and procedures.

## View Utilization Metrics by Partition

Release 7.4 allows you to view utilization metrics for an individual partition or a specified list of partitions.

See "Partition Utilization Metrics" on page 1 for details.

## Ed25519ph Curve

SafeNet Luna Network HSM firmware version 7.4.0 includes support for the ed25519ph curve variant.

See "CKM_EDDSA" on page 1 for details.

# SafeNet Luna Network HSM Release 7.3

This release consists of:

> Luna HSM Client 7.3.0

> SafeNet Luna Network HSM appliance software 7.3.0

> Luna HSM firmware 7.3.0

## Appliance Re-Image

SafeNet Luna Network HSM 7.3 allows you to re-image the appliance to a pre-installed baseline version. This procedure formats the SafeNet Luna Network HSM file system, zeroizes the HSM, erases the appliance configuration, and resets the appliance software to Luna 7.2 and the HSM firmware to version 7.0.3. This capability is useful if you are re-purposing an HSM for a project that has standardized on an earlier software/firmware configuration, or if you need to format the appliance completely and remove all trace of its prior configuration (requires firmware 7.3.0).

See Re-Imaging the Appliance to Factory Baseline.

## Partition Utilization Metrics

SafeNet Luna Network HSM 7.3 allows the HSM SO to access utilization records for all partitions on the HSM. This information is restricted to operation counts, and shows which partitions are using the HSM's resources. Information about which keys are being used for which operation is still restricted to the Auditor (requires firmware 7.3.0).

See Partition Utilization Metrics.

## BIP32 Algorithm

SafeNet Luna Network HSM 7.3 includes new mechanisms that use the BIP32 cryptographic algorithm. This allows SafeNet Luna Network HSM to support applications that use Hierarchical Deterministic Wallets, used in Bitcoin and blockchain transactions (requires firmware 7.3.0).

## JavaSP support for ECC Curve 25519

The SafeNet Java Provider now includes support for mechanisms using ECC Curve 25519.

# SafeNet Luna Network HSM Release 7.2

This release consists of:

> Luna HSM Client 7.2.0

> SafeNet Luna Network HSM appliance software 7.2.0

> Luna HSM firmware 7.2.0

## 10 Gbps Optical NIC SafeNet Luna Network HSM Support

Thales is pleased to announce the availability of the 10 Gbps optical NIC SafeNet Luna Network HSM. This product variant provides two 10G optical network interfaces and two 1G copper network interfaces, as opposed to the standard 1G model which provides four 1G copper network interfaces.

The 10G SafeNet Luna Network HSM provides two 10G SFP optical Ethernet network interfaces (labeled 0 and 1), and two 1G copper RJ45 network interfaces (labeled 2 and 3), as illustrated below. You can optionally bond eth0 and eth1 to bond0, or eth2 and eth3 to bond1, to provide a redundant active/standby virtual interface.
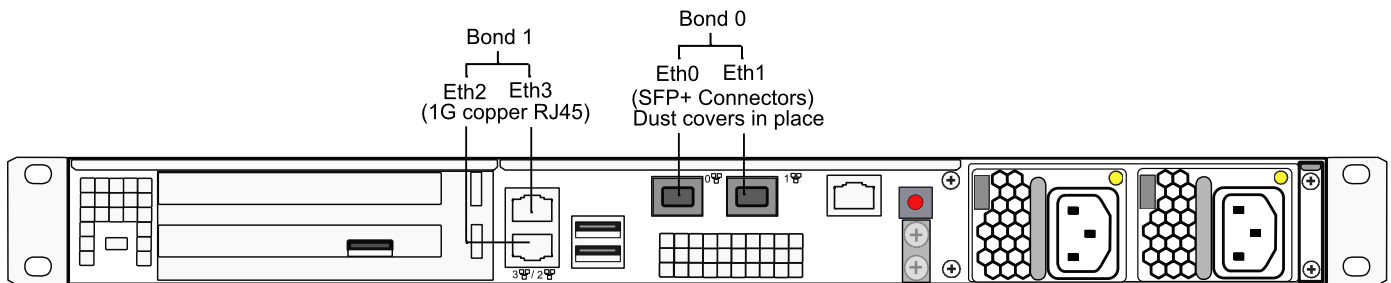


## Improved Luna HSM Client

Release 7.2 adds improvements to the Luna HSM Client software:

> **Enhanced Version Compatibility for Luna HSM Client** — Version 7.2 and newer Luna HSM Client can be used with HSMs running Luna 6.2.1 or higher, or any Luna 7 version, without conflict. Luna HSM Client 7.2 and newer versions can coexist in large deployments. You can schedule client roll-outs at your convenience, without need to match versions across your organization. Future HSM features that do not have client-version dependencies will function without issue.

> **Mixed-Version HA Groups** — HA groups containing both SafeNet Luna Network HSM 6 and 7 partitions are now supported using Luna HSM Client 7.2 or newer. This mixed-version configuration is useful for migrating keys to a new SafeNet Luna Network HSM 7, or to gradually upgrade your production environment from Luna 6 to Luna 7.

> **Improved Client Installer with User-Defined Install Paths (Windows)** — Luna HSM Client can be installed at user-selected locations (file paths with sufficient space), and installed Client software can be modified without uninstalling and reinstalling.

> **User-Defined Client Install Paths (Linux)** — Linux root-level users can install the Luna HSM Client software to an installation directory of their choice.

> **Minimal Client (Linux)** — The SafeNet Luna Minimal Client for Linux provides only the files needed to use an application with a partition on a SafeNet Luna Network HSM for deployment in Docker containers and similar microservice environments. The Luna Minimal Client can be installed on a workstation without root access.

## Configurable Cipher Suites

You can now configure the TLS cipher suites used by NTLS, STC, and PEDserver on the SafeNet Luna Network HSM. This new capability allows administrators to select and configure cipher strength to meet their internal security objectives and compliance requirements.

The cipher suites are configured using the new **sysconf tls cipher** LunaSH commands. The available set of ciphers is displayed in default order. Users can choose which ciphers from the set to use, as well as the order of preference for TLS cipher-suite negotiation. The modified cipher list and order can also be exported as a template; the template can then be used to configure TLS cipher suites on multiple HSMs.

## Customizable System Logging

You can now customize local and remote system logging according to message severity. There is no limit on the number of remote logging servers you can add, and you can configure the severity level for each server and log type independently. For example, you could send all log entries produced by the appliance to one remote server, and only entries marked **critical** or higher to another. Storing only the most severe (infrequent) entries locally on the appliance can prevent the syslog directory from filling up over time.

## Rename/Relabel Partitions

The HSM SO can now change the name assigned to a partition on creation. This does not affect the label set by the Partition SO during initialization and is only visible in LunaSH. This allows partitions to be created ahead of time and renamed to something more suitable later, when they are allocated for a particular purpose (Requires firmware 7.2.0).

The Partition SO can now change the label of an initialized partition (Requires firmware 7.2.0).

## Initialize the Orange RPV Key Remotely

You can now initialize the Remote PED Vector (orange key) using a Luna PED connected to a remote workstation running PEDserver. A one-time numeric password is used to authenticate the Remote PED to the HSM before initializing the RPV. This optional method is useful if the HSM SO only has remote SSH access to the appliance. The HSM must be in a zeroized state (uninitialized), for security. Your firewall settings must allow an HSM-initiated Remote PED connection (Requires firmware 7.2.0).

## Crypto User Can Clone Public Objects

The Crypto User (CU) role has always been able to create public objects, but not clone them. In HA mode, this would cause the replication and subsequent object creation operations to fail. Firmware 7.2.0 allows the CU to clone public objects, and therefore to perform operations on HA groups without Crypto Officer authentication (Requires firmware 7.2.0).

## Auto-Enabled HA Logging

Luna HSM Client now automatically enables HA logging, either when you create the first HA group, or when you update the Luna HSM Client to 7.2.0 and it detects a previously-configured HA group. If you manually turn HA logging off, logging is not auto-enabled for new HA groups.

## SCP03 Encoding

The SCP03 encoding scheme, as defined in NIST SP 800-108, is now supported for Global Platform.

## REST API 6.0

REST API 6.0 is included with the SafeNet Luna Network HSM 7.2 release. Customers who update their appliance software to version 7.2.0 will automatically receive the REST API 6.0 update. REST API 6.0 contains the following new features:

> **Appliance Upgrade Management** — Manage Thales Group Licensing Portal partition upgrade packs using REST API.

> **Package and Firmware Update Management** — Update, verify, list, and delete secure packages with REST API, including firmware updates.

> **Multi-Part Upload Requests** — Upgrade your HSMs via a single REST API call, improving performance and efficiency.

> **Configurable REST API Users and Roles** — Manage REST API users and roles (add, remove, modify, show, list) using REST API.

> **Configurable REST API Access Control List** -- Modify role access using REST API, by importing and exporting lists of available resources.

# SafeNet Luna Network HSM Release 7.1

This release consists of:

> Luna HSM Client 7.1.0

> SafeNet Luna Network HSM appliance software 7.1.0

> Luna HSM firmware 7.1.0

## Policy Templates

The HSM or Partition SO can save a copy of their organization's preferred HSM or partition policy settings to a template. They can then use this template to configure policy settings when initializing other HSMs or partitions.

This can save time and effort when deploying multiple HSMs or partitions. It also ensures consistency across your HSMs and partitions, which helps to simplify future audit and compliance requirements.

See Setting HSM Policies Using a Template and Setting Partition Policies Using a Template.

## Configurable Policies for Export of Private Keys

The Partition SO can use partition policies to control whether or not the private keys in a given partition can be exported off the HSM. The ability to export private keys is particularly useful in use cases such as smart card & identity issuance, secure manufacturing, etc.

This gives organizations the ability to support a wider variety of use cases with their HSM, and also provides Partition SOs with more flexibility overall.

See Configuring the Partition for Cloning or Export of Private Keys.

## Curve 25519 Available in FIPS Mode

Curve 25519 is now available for use in FIPS mode.

## REST API 5.0

REST API 5.0 is included with the SafeNet Luna HSM 7.1 release. Customers who upgrade their appliance to 7.1 will automatically receive the REST API 5.0 update as part of the upgrade.

REST API provides a set of web services which customers can use to communicate with and provision the HSM.

See REST API Reference.

# SafeNet Luna Network HSM Release 7.0

This release consists of:

> New SafeNet Luna Network HSM appliance

> Luna HSM Client 7.0.0

> SafeNet Luna Network HSM appliance software 7.0.0

> Luna HSM firmware 7.0.1

## New SafeNet Luna Network HSM Appliance

The SafeNet Luna Network HSM 7 has a new chassis and offers enhanced installation, maintenance, security, and usability features, including the following:

> Optional sliding mounting rails provide simplified installation and improved access for performing maintenance tasks and accessing the network ports.

> A locking faceplate bezel restricts access to the front of the appliance for enhanced security.

> A new LCD display provides a quick view of the appliance network configuration and overall health.

> Four 1GB Ethernet interface ports with port bonding (eth0 and eth1 to bond0 and/or eth2 and eth3 to bond1), for redundancy and enhanced reliability.

See Appliance Hardware Functions.

## Partition Security Officer

All application partitions now have a Partition Security Officer (PO) role that is completely distinct from the HSM Security Officer (HSM SO) role. In this security model, the HSM SO is responsible only for initializing the HSM, setting HSM-level security policies, and creating and deleting partitions. After creating the partitions, the HSM SO has no access to the contents of the partitions. Partitions are owned by the PO, who is responsible for initializing the partition, setting the partition-level security policies and initializing the cryptographic roles on the partition. This model permits a complete separation of roles on the HSM, providing a highly secure multi-tenant solution.

See Partition Roles.

## Best-in-Class Performance

SafeNet Luna Network HSM 7 provides cryptographic performance that is 10x faster than the release 5.x and 6.x SafeNet Luna HSMs.

## Industry-Leading Security

SafeNet Luna Network HSM 7 provides enhanced environmental failure protection and tamper resistance.

## Improved Random Number Generation

The performance of SafeNet Luna Network HSM 7's AES-256 CTR DRBG random number generation is significantly increased from previous versions. The RNG is fully compliant with the latest entropy standards:

> SP800-90B

> SP800-90C

> BSI DRG.4

## New Cryptographic Mechanism Support

SafeNet Luna Network HSM 7 adds support for the following cryptographic algorithms:

> SP800-108 HMAC (RSA & ECC)

> SP800-38F (KWP)

> Curve 25519

> AES-XTS - disk encryption standard

## Increased Key Storage Capacity

SafeNet Luna Network HSM 7 provides up to 32 MB of cryptographic object storage (depending on the model).

## Secure Transport Mode Redesigned

Secure Transport Mode (STM) in SafeNet Luna Network HSM 7 provides a simple, secure method for shipping an HSM to a new location and verifying its integrity upon receipt. When the HSM SO enables STM, it locks the HSM and its contents, and records the current configuration as a pair of unique strings. When the HSM is recovered from STM, the unique strings are redisplayed. If the strings match, the HSM has not been tampered or modified during transport.

See Secure Transport Mode.

## REST API

The SafeNet Luna Network HSM REST API web application allows you to use a set of scriptable REST APIs to perform some LunaSH functions.

See REST API Reference.

## IPv6

The SafeNet Luna Network HSM10.2 now supports IPv6, using static addressing, SLAAC, or DHCP.

See IPv6 Support and Limitations.

## Improved Serial Access

Serial access to the SafeNet Luna Network HSM is via an RJ45 serial port. A custom Prolific Technologies USB to RJ45 cable with a standard 8P8C modular connector is included. The cable requires the PL2303 driver, which you can download from http://www.prolific.com.tw.

See Opening a Serial Connection.

## Enable Decommission on Tamper

A new capability, **Enable Decommission on Tamper**, allows you to set **HSM policy 40** to decommission the HSM in the event of a tamper.

See HSM Capabilities and Policies.

## Controlled Tamper Recovery

If **Policy 48: Do Controlled Tamper Recovery** is enabled (the default), the HSM SO must clear the tamper condition before the HSM is reset, to return the HSM to normal operation.

See Tamper Events.

# Version Dependencies by Feature

Some of the SafeNet Luna Network HSM functionality described in the documentation has been introduced in updates since the initial product release. For your own reasons, you may wish to apply some aspects of a product update and not others. For example:

> you may choose to update appliance or client software while keeping an earlier, FIPS-certified firmware version

> if you are maintaining a large number of client workstations, it may be cumbersome to apply software updates to all of them

The following table outlines the SafeNet Luna Network HSM functions that depend on a certain software/firmware version, or have other requirements you must consider.

| Function | Minimum Version Requirements | Notes |
|---|---|---|
| **Support for 3GPP, SM2/SM4, and SHA-3 Cryptographic Algorithms**<br>> 3GPP Mechanisms for 5G Mobile Networks<br>> SM2/SM4 Mechanisms<br>> SHA-3 Mechanisms | **Firmware:** 7.4.2<br>**Client:** 10.2 (or patched 7.4) | Refer also to Firmware 7.4.2 Mechanisms for descriptions of the applicable mechanisms. Refer to the *SafeNet Luna HSM Firmware 7.4.2 Technical Note* for installation instructions. |
| **DPoD HSM on Demand Support**<br>> Adding a DPoD HSM on Demand Service | **Client:** 10.1 | Refer to Cloning Keys Between Luna 6, Luna 7, and HSM on Demand for more information on using an HSMoD service with Luna HSMs. |

| Function | Minimum Version Requirements | Notes |
|---|---|---|
| **Remote PED Server Support on Linux Clients**<br>> Remote PED Setup | **Client:** 10.1 | |
| **Client NTLS Certificates can be Signed by a Trusted Certificate Authority**<br>> Creating an NTLS Connection Using a Client Certificate Signed by a Trusted Certificate Authority | **Client:** 10.1 | |
| **SafeNet Luna Backup HSM (G7 model) Support**<br>> Backing Up Partition Objects to a G7-based Backup HSM | **Client:** 10.1 | |
| **Functionality Modules**<br>> Functionality Modules<br>> About the FM SDK Guide | **Hardware:** FM-Ready<br>**Firmware:** 7.4.0<br>**Appliance:** 7.4<br>**Client:** 7.4 | Refer to Preparing the SafeNet Luna Network HSM to Use FMs for an overview of hardware/software/firmware requirements. |
| **Manage Allowed Origin Domains for REST API**<br>> webserver origin | **Appliance:** 7.4 | |
| **Support for BIP32 Cryptographic Algorithms**<br>> BIP32 Mechanism Support and Implementation | **Firmware:** 7.3.0<br>**Client:** 7.3.0 | Refer also to Firmware 7.3.0 Mechanism Summary for descriptions of the applicable mechanisms. |
| **Appliance Re-image**<br>> Re-Imaging the Appliance to Factory Baseline | **Firmware:** 7.3.0<br>**Appliance:** 7.3 | The Appliance Re-image feature is not supported on HSMs that use Functionality Modules. If you have ever enabled **HSM policy 50: Allow Functionality Modules**, even if the policy is currently disabled, you cannot re-image the HSM appliance. See "Planning Your FM Deployment" on page 1 for details. |

| Function | Minimum Version Requirements | Notes |
|---|---|---|
| **Partition Utilization Metrics**<br>> Partition Utilization Metrics | **Firmware:** 7.3.0<br>**Appliance:** 7.3<br>**Client:** 7.3 | |
| **Improved Luna HSM Client**<br>> Version-Compatible Luna HSM Client (Luna HSMs version 6.2.1 and higher)<br>> Cloning Keys Between Luna 6, Luna 7, and HSM on Demand<br>> Modifying the Installed Windows Luna HSM Client Software<br>> User-Defined Luna HSM Client install paths<br>> Luna Minimal Client (for Linux) | **Client:** 7.2 | > Luna HSM Client 10.1 or higher is required to use Luna partitions with DPoD's HSM on Demand services<br>> The **PE1756Enabled** setting on Luna 6.x HSMs is not supported for use with the Version-Compatible Luna HSM Client<br>> Minimum OS requirements for Luna HSM Client 7.2 must be met (Refer to the CRN for details)<br>> Minimal Client does not include tools, and is intended for customer application containers connecting to the Network HSM. A separate full Luna HSM Client installation and configuration must be performed on the container host (and the resulting config file and certificate folders saved on the host), to establish NTLS or STC connections for use by the containers. |
| **Initialize the orange RPV key remotely**<br>> "Remote RPV Initialization" on page 1 | **Appliance:** 7.2<br>**Client:** 7.2 | |
| **Configure Cipher Suites**<br>> Set TLS Ciphers | **Appliance:** 7.2<br>**Client:** 7.2 | The Luna 7.2 appliance update includes the **sysconf tls ciphers** LunaSH commands, but you must update Luna HSM Client to use any of the newly-included ciphers. For older clients, the ciphers available for negotiation are those that are common to your client version and to the updated Network HSM. |
| **Customize system logging by severity level**<br>> Customizing Severity Levels<br>> Customizing Remote Logging Severity Levels | **Appliance:** 7.2 | If you were using remote logging before you upgraded the appliance software to 7.2, you must delete any existing remote hosts (see syslog remotehost delete) and re-add them before you can customize severity levels. |

| Function | Minimum Version Requirements | Notes |
|---|---|---|
| **Re-name/Re-label partitions**<br>> **partition rename**<br>> **partition changelabel** | **Firmware:** 7.2.0<br>**Appliance:** 7.2<br>**Client:** 7.2 | |
| **Crypto User can clone public objects** | **Firmware:** 7.2.0 | The Crypto User (CU) role has always been able to create public objects, but not clone them. In HA mode, this would cause the replication and subsequent object creation operations to fail. Firmware 7.2.0 allows the CU to clone public objects, and therefore to perform operations on HA groups without Crypto Officer authentication. |
| **Configure partition policies for export of private keys**<br>> Configuring the Partition for Cloning or Export of Private Keys | **Firmware:** 7.1.0 | You can configure partition policies for Cloning or Key Export Mode manually, as long as you have updated the HSM firmware. To set these modes using Policy Templates, you must meet the Policy Template requirements. |
| **Policy Templates**<br>> Setting HSM Policies Using a Template<br>> Setting Partition Policies Using a Template | **Firmware:** 7.1.0<br>**Appliance:** 7.1<br>**Client:** 7.1 | |

# CHAPTER 3:   Security

SafeNet Luna HSMs ensure the highest quality of protection of your cryptographic material with the following security measures:

> "Layered Encryption" below
> "Tamper Protection" on page 35
> "Certification" on page 36

## Layered Encryption

SafeNet Luna HSMs do not keep any objects in the clear. All objects are encrypted by multiple layers, and are fully decrypted in temporary (volatile) memory only when needed.

### Hierarchy of Protection

One general storage key (GSK), for the HSM, protects general storage objects that might be needed by various roles. A separate user storage key (USK) for each role, protects the contents of the partition accessed by that role. The hierarchy of protection, depicted in "HSM Layered Encryption" on the next page, applies to each individual role. The USK for each role on the HSM encrypts objects that are owned by that role, ensuring that each person sees and touches only what belongs to them. Every SafeNet Luna HSM has a master tamper key (MTK) that strongly encrypts each object generated and stored within the HSM.

The key encryption key (KEK) further encrypts every key being used to ensure that your keys are never shown in plaintext.

### Three-Layer Authentication Model

The SafeNet Luna Network HSM, and access to data stored on the Cryptographic Engine contained within it, is protected by a number of different means to provide in-depth security. The SafeNet Luna Network HSM's three-layer authentication model includes separate HSM partition authentication, 2-way network authentication, and process level application authentication to respectively control administrative, client, and application access. This three-layer model, coupled with multi-level user authentication policies, integrated FIPS 140-2 Level 3-validated Cryptographic Engine, and secure software and hardware design, allows the SafeNet Luna Network HSM to offer the same high degree of security and performance as traditional HSMs without sacrificing the flexibility of a network-attached device.

**Figure 2: HSM Layered Encryption**
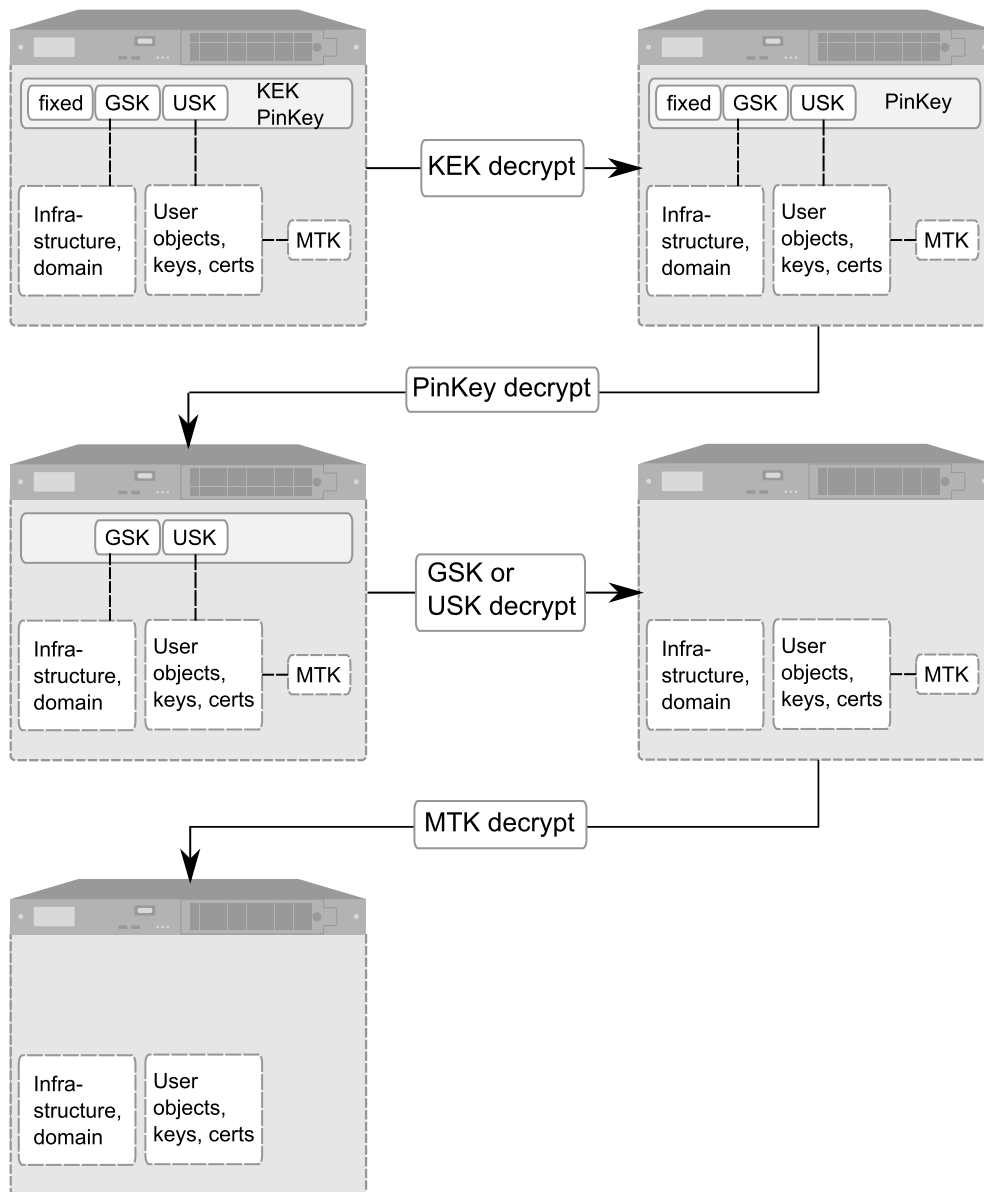


When the HSM is powered on, all stored objects are still tightly encrypted. When an object is decrypted for use, the decrypted version exists in volatile memory, only while being used, and only while the HSM has power.

**1.** KEK is unique to each HSM, and encrypts everything that is encrypted by the PinKey.

**2.** During login, KEK and PinKey decryptions are performed.

- For password-authenticated HSMs, the PinKey is the HSM SO password (or Partition SO, or CO or CU or Auditor, depending on who is logging in).

- For PED-authenticated HSMs, the PinKey is the secret retrieved from the correct blue SO PED key (or black or gray or white, depending on who is logging in).

At this point, objects are partially decrypted, but still under further levels of encryption (see next steps).

**3.** GSK encrypts all general-storage objects, while USK encrypts all security and user objects for the role logged into the HSM. Objects are decrypted (into volatile memory) individually when needed.

4. At the lowest level, MTK encrypts all objects.

5. Some objects are fully decrypted in volatile memory only when in use. Others, including ECDSA with NIST Prime curves, AES, DES3, and RSA keys remain MTK-encrypted. Once decrypted and accessible, objects inside the HSM can be used. If power is lost or a tamper occurs, all temporarily decrypted objects instantly evaporate, and stored objects remain tightly encrypted as always.

The in-depth application of multiple layers of security at all levels of the interface to SafeNet Luna HSMs and their internal HSMs provides a high degree of confidence that cryptographic material within the HSM will not be compromised. Customers with extremely demanding security requirements can enhance the already strong security of SafeNet Luna HSMs by choosing appropriate installation, HSM configuration, and policy options.

## Cloning Domain or Security Domain

Every HSM or partition is part of a security domain, set at initialization time. This is also called a cloning domain, because objects under such a domain can be securly copied (cloned) only to other HSMs or partitions that share that exact domain.

Multiple HSMs or partitions can be set to be part of the same cloning domain or different ones. Key material cannot leave its cloning domain, so if an attacker were to try to copy your cryptographic material to a device that does not share a cloning domain with your HSM or partition, they would be unsuccessful. Using cloning domains ensures that key material can travel only between trusted and authorized devices. This adds a strong layer of defense against attackers.

> **NOTE**  The security or cloning domain is not the lowest encryption level, so a cloning operation does not provide access to Crypto material.
> Operations that use cloning are limited to backup, restore and synchronizing the HSMs in HA groups ( among HSMs that share the same domain). Only the backup operation imposes a source-partition domain on the target partition within the Backup HSM; the restore operation and the HA synchronization both require that the source and target HSMs or partitions must already have matching domains.

# Tamper Protection

## Physical Security

SafeNet Luna HSMs are equipped with intrusion-resistant, tamper-evident hardware, and use the strongest cryptographic algorithms to ensure that your data is secure. If a security breach is detected, a tamper event occurs and the HSM becomes locked until the tamper is cleared by the appropriate authority or the HSM is reset.

**SafeNet Luna Network HSM**

The SafeNet Luna Network HSM appliance is a commercial-grade secure appliance. This means that:

> It is provided with anti-tamper external features that make physical intrusion into the unit difficult. These measures deter casual intrusion and leave visible evidence of attempts (successful or otherwise) to open the unit.

> Vents and other paths into the unit are baffled to prevent probing from the outside.

> It includes a hardened OS that constantly monitors for security vulnerabilities.

> The HSM Keycard inside the appliance houses the actual HSM components. It is encased in an aluminum shell, filled with hardened epoxy. Attempts to gain access to the circuit board itself would result in physical evidence of the attempted access and likely physical destruction of the circuitry and components, thus ensuring that your keys and sensitive objects are safe from an attacker.

If an attacker with unlimited resources were to simply steal the appliance, and apply the resources of a well-equipped engineering lab, it might be possible to breach the physical security. However, without the password (password-authenticated HSMs) or the PED keys (PED-authenticated HSMs), such an attacker would be unable to decipher any signal or data that they manage to extract.

With that said, it is your responsibility to ensure the physical security of the unit to prevent such theft, and it is your responsibility to enforce procedural security to prevent an attacker ever having possession of (or unsupervised access to) both the HSM and its authentication secrets.

## Surrounding Environment

The data sheets provided for individual products show the environmental limits that the device is designed to withstand. It is your responsibility to ensure that the unit is protected throughout its working lifetime from extremes of temperature, humidity, dust, vibration/shock that exceed the stated limits.

We do not normally specify operational tolerances for vibration and shock, as the SafeNet Luna HSM is intended for installation and use in an office or data center environment. We perform qualification testing on all our products to ensure that they will survive extremes encountered in shipping, which we assume to be more demanding than the intended operational environment.

It is also your responsibility to ensure that the HSM appliance is installed in a secure location, safe from vandalism, theft, and other attacks. In summary, this usually means a clean, temperature-, humidity-, and access-controlled facility. We also strongly recommend power conditioning and surge suppression to prevent electrical damage, much as you would do for any important electronic equipment.

## Authentication Data Security

It is your responsibility to protect passwords and/or PED keys from disclosure or theft and to ensure that personnel who might need to input passwords do not allow themselves to be watched while doing so, and that they do not use a computer or terminal with keystroke logging software installed.

# Certification

## FIPS

At any given time, a FIPS-validated version of the HSM is available, and a newer not-yet-validated version might also be available for newly introduced products that have not had time to go through the long evaluation and validation process. The usual practice is to ship units pre-loaded with the firmware and software at the FIPS-validated level by default, while providing the option to update the Client software, Appliance software, and HSM firmware to the newer version. This allows customers who need FIPS validation to have that configuration from the factory, and customers who need newer features (and do not need FIPS validation) to upgrade by simply installing the newer software and following the upgrade procedure. To check the progress of HSM versions that are submitted for FIPS 140-2 validation visit the NIST site at
http://csrc.nist.gov/groups/STM/cmvp/validation.html.

## Common Criteria

Some versions of the product are submitted for Common Criteria EAL evaluation.

You can check with Thales Group Customer Support to inquire about the certification status of SafeNet Luna HSM products. If FIPS validation or CC EAL certification are not requirements for you, then the newest version is normally the preferred option.

# CHAPTER 4:   Redundancy and Reliability

SafeNet Luna HSMs are reliable in the case of unexpected events like power failures in the following ways:

> They have hot-swappable power supplies that can be replaced without turning off your system.

> They have dual fans to ensure that your HSM remains at a constant temperature and does not overheat and fail should one fan fail. This allows you to continue using your HSM while you replace the defective fan.

SafeNet Luna HSMs can also be grouped in a High Availability (HA) configuration for auto-recovery of your data in case an HSM fails. See "High-Availability Groups" below for an overview of this scheme.

## High-Availability Groups

SafeNet Luna HSMs can provide scalability and redundancy for cryptographic applications that are critical to your organization. For applications that require continuous, uninterruptible uptime, the Luna HSM Client allows you to combine application partitions on multiple HSMs into a single logical group, known as a High-Availability (HA) group.

An HA group allows your client application to access cryptographic services as long as one member HSM is functional and network-connected. This allows you to perform maintenance on any individual member without ever pausing your application, and provides redundancy in the case of individual failures. Cryptographic requests are distributed across all active group members, enabling a performance gain for each member added. Cryptographic objects are replicated across the entire group, so HA can also be used to keep a current, automatic, remote backup of the group contents.

HA functionality is handled by the Luna HSM Client software. The individual partitions have no way to know they are configured in an HA group, so you can configure HA on a per-application basis. The way you group your HSMs depends on your circumstances and desired performance.

### Performance

For repetitive operations (for example, many signings using the same key), an HA group provides linear performance gains as group members are added. The best approach is to maintain an HA group at a size that best balances application server capability and the expected loads, with an additional unit providing capacity for bursts of traffic.

### Load Balancing

Cryptographic requests sent to the HA group's virtual slot are load-balanced across all active members of the HA group. The load-balancing algorithm sends requests for cryptographic operations to the least busy partition in the HA group. This scheme accounts for operations of variable length, ensuring that queues are balanced even when some partitions are assigned very long operations. When an application requests a repeated set of operations, this method works. When the pattern is interrupted, however, the request type becomes relevant, as follows:

> Single-part (stateless) cryptographic operations are load-balanced.

> Multi-part (stateful) cryptographic operations are load-balanced.

> Multi-part (stateful) information retrieval requests are not load-balanced. In this case, the cost of distributing the requests to different HA group members is generally greater than the benefit. For this reason, multi-part information retrieval requests are all targeted at one member.

> Key management requests are not load-balanced. Operations affecting the state of stored keys (creation, deletion) are performed on a single HA member, and the result is then replicated to the rest of the HA group.

## Key Replication

When an application creates a key on the virtual HA slot, the HA library automatically replicates the key across all group members before reporting back to the application. Keys are created on one member partition and replicated to the other members. If a member fails during this process, the HA group reattempts key replication to that member until it recovers, or failover attempts time out. Once the key exists on all active members of the HA group, a success code is returned to the application.

All key replication uses the Luna cloning protocol, which provides mutual authentication, confidentiality, and integrity for each object that is copied from one partition to another. Therefore, all HA group member partitions must be initialized with the same cloning domain.

## Failover

When any active HA group member fails, a failover event occurs – the affected partition is dropped from the list of available HA group members, and all operations that were pending on the failed partition are transparently rescheduled on the remaining member partitions. The Luna HSM Client continuously monitors the health of member partitions at two levels:

> network connectivity – disruption of the network connection causes a failover event after a 20-second timeout.

> command completion – any command that is not executed within 20 seconds causes a failover event.

As long as one HA group member remains functional, cryptographic service is maintained to an application no matter how many other group members fail.

## Recovery

Recovery of a failed HA group member is designed to be automatic in as many cases as possible. You can configure your auto-recovery settings to require as much manual intervention as is convenient for you and your organization. In either an automated or manual recovery process, there is no need to restart your application. As part of the recovery process:

> Any cryptographic objects created while the member was offline are automatically replicated to the recovered partition.

> The recovered partition becomes available for its share of load-balanced cryptographic operations.

**Automatic Recovery**

With automatic recovery, the client library automatically performs periodic recovery attempts while a member is failed. The frequency of these checks is adjustable. Most customers enable auto-recovery in all configurations.

**Manual Recovery**

Simply run the client recovery command and the recovery logic inside the client makes a recovery attempt the next time the application uses the HSM. As part of recovery, any key material created while the member was offline is automatically replicated to the recovered unit.

Even if a manual recovery process is selected, the application does not need to be restarted.

**Permanent Failure**

Sometimes a failure of a device is permanent (for example, if the HSM is re-initialized). In this event, you only need to remove the failed unit and deploy a new member to the group. The running clients automatically resynchronize keys to the new member and start scheduling operations to it.

## Standby Members

After you add member partitions to an HA group, you can designate some as standby members. Cryptographic objects are replicated on all members of the HA group, including standby members, but standby members do not perform any cryptographic operations unless all the active members go offline. In this event, all standby members are immediately promoted to active service, and operations are load-balanced across them. This provides an extra layer of assurance against a service blackout for your application.

## Mixed-Version HA Groups

Generally, Thales Group recommends using HSMs with the same software/firmware in HA groups; different versions have different capabilities, and a mixed HA group is limited to those functions that are common to the versions involved. A mixed-version HA group may have access to fewer cryptographic mechanisms, or have different restrictions in FIPS mode. However, HA groups containing both Luna 6 and 7 partitions and HSM on Demand services from SafeNet Data Protection on Demand are supported. This mixed-version configuration is useful for migrating keys to a new Luna 7 HSM or the cloud, or to gradually upgrade your production environment from Luna 6 to Luna 7.

# CHAPTER 5:  Networking

SafeNet Luna HSMs support multiple different network configurations via:

> "Network Interfaces" below

> "NTLS and STC" on the next page

## Network Interfaces

The SafeNet Luna Network HSM appliance enables flexible network configurations by way of multiple network interfaces that can be configured in various ways.

### Ethernet Ports

The SafeNet Luna Network HSM appliance has four 1Gb/a Ethernet LAN ports and one RJ-45 serial port, used 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 in "HSM Appliance Ports" below:

**Figure 3: HSM Appliance Ports**
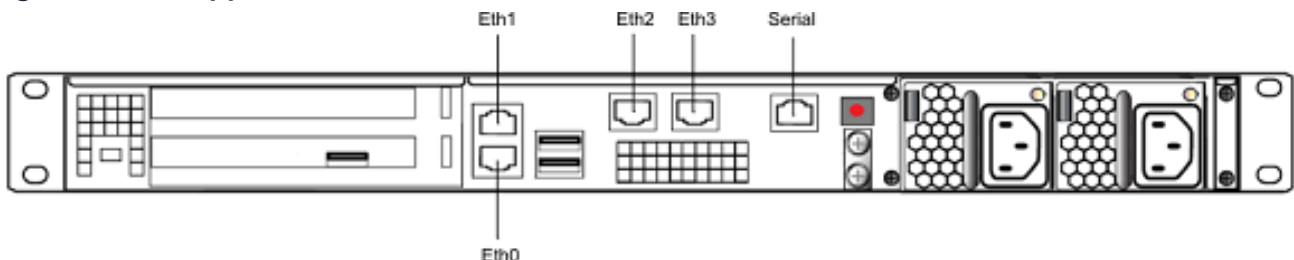


Each Ethernet (Eth) port can be used to configure an individual network device, or the interfaces can be combined to enable a redundant network configuration. (See "Network Interface Bonding" below.)

You 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.

### Network Interface Bonding

SafeNet Luna Network HSM has four physical network interface devices: eth0, eth1, eth2, and eth3. You can bond eth0 and eth1 into a single virtual interface, bond0, or eth2 and eth3 into bond1, to provide a redundant active/standby interface.

"Network Interface Bonding" on the next page shows how individual devices (marked by eth) can be combined to create a bonded device.

**Figure 4: Network Interface Bonding**
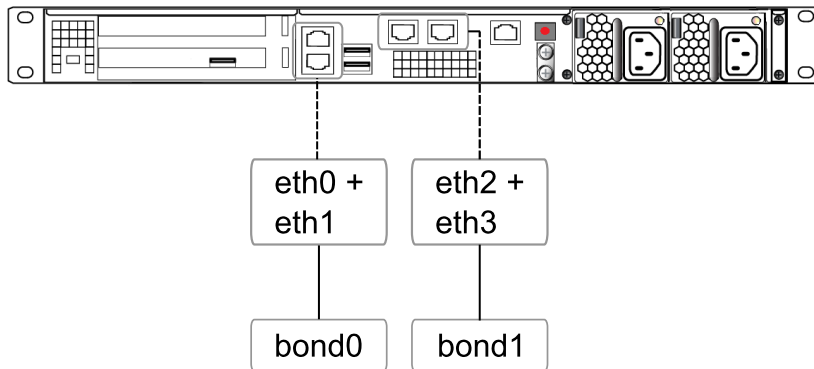


Network traffic can be bound to a single device, or a bonded device. The primary purpose of the bonding service is a hot standby mode for network interface failure, ensuring a constant stable connection to your appliance.

Once bonding is configured, client connections as well as SSH connections continue uninterrupted if either or the bonded interfaces fails.

# NTLS and STC

SafeNet Luna Network HSM supports network connections over two different types of channels:

> NTL (Network Trust Link)

> STC (Secure Trusted Channel)

## NTLS

Network Trust Links (NTLs) are secure, authenticated network connections between the SafeNet Luna Network HSM appliance and clients. NTLs use two-way digital certificate authentication and TLS data encryption to protect your sensitive data during all communications between HSM partitions on the appliance and its clients. NTLs are made up of:

> NTLS: Network Trust Link Server, on the appliance

> NTLA: Network Trust Link Agent, on the client

> NTL itself: a secure connection between NTLS and an authenticated NTLA

"NTLS Connection" on the next page shows how an NTL connection is made between the client and the appliance.

**Figure 5: NTLS Connection**
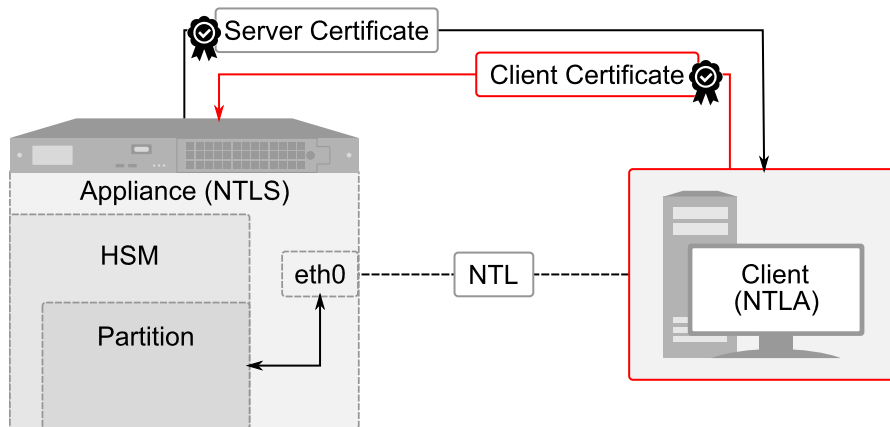


Certificates are created on both the appliance and the client. These certificates are exchanged to register the appliance and client with each other. Once registered, the appliance will recognize the client and allow it access to the HSM and partitions it wants. NTLS encrypts data between the network interfaces of the appliance (shown as eth0 in the diagram) and client, but not between the network interface and the HSM within the appliance.

The SafeNet Luna Network HSM appliance can support up to 800 simultaneous NTL connections.

# STC

STC (Secure Trusted Channel) uses secure key exchange and data encryption to protect your sensitive data during communications between HSM partitions and clients. The type of data encryption you use is up to you; STC is flexible and customizable.

STC supports a wide range of end-points, but its primary end-points are client applications connecting to the HSM to access its cryptographic services and/or to perform module management functions. STC provides three basic services:

> Privacy of all communicated data through the use of symmetric encryption so only the end-points can read any sensitive data.

> Integrity of the communicated data through the use of message authentication codes so that not eavesdropper could add, delete, modify or replay any command or response.

> Mutual authentication of the HSM and the end-point so that only authorized entities can establish a STC connection and there can be no man-in-the-middle attack.

"STC Connection" on the next page shows how an STC connection is made between the client and the appliance.

**Figure 6: STC Connection**
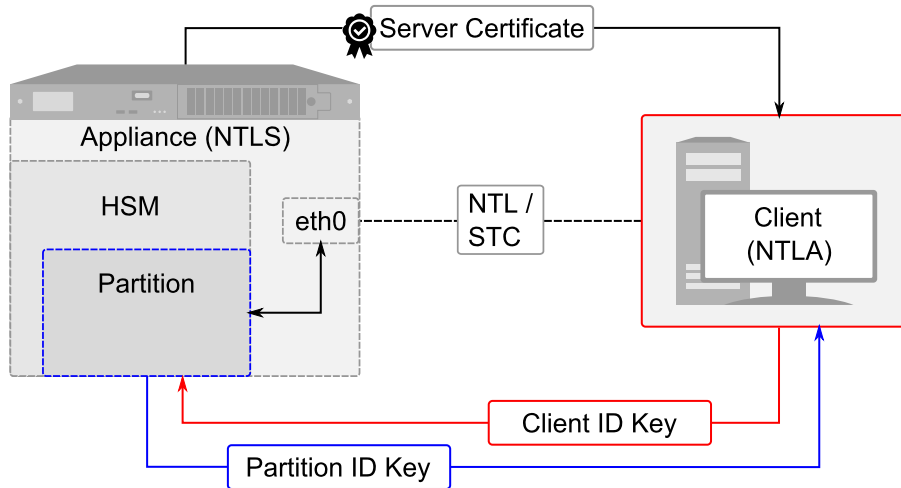


STC connects a client directly to a specific partition on the HSM in the appliance.

The STC connection consists of two phases: tunnel establishment and message handling. During tunnel establishment the end-parties perform bi-directional authentication and then establish unique session keys for each connection. After a connection is established between the network interfaces of the appliance (shown as eth0 in the diagram) and client, the message handling phase securely transmits commands to the HSM and receives HSM responses. Any attempt to alter, insert or drop messages is detected by both end-points and results in immediate termination of the connection.

NTLS must be set up before you use STC.

## Comparing NTLS and STC

| NTLS | STC |
|---|---|
| > Consistent high performance<br>> Does not encrypt data between network interface and HSM<br>> Not recommended for use with public networks | > Exceptionally secure and safe to use with public networks<br>> Encrypts data between network interface and HSM<br>> Customizable parameters<br>> Performance depends on parameters set |

For detailed instructions on setting up NTLS or STC, see Client-Partition Connections.

# CHAPTER 6:   User Access Control

The security of an HSM and its cryptographic contents depends on well-controlled access to that HSM. A controlled access policy is defined by:

> the set of users with valid login credentials for the appliance, the HSM and the application partition

> the actions each user is allowed to perform when logged in (the user's role)

For example, an access policy that adheres to the PKCS#11 standard requires two roles: the security officer (SO), who administers the user account(s), and the standard user, who performs cryptographic operations. When a user logs in to the HSM, they can perform only those functions that are permitted for their role.

Access to SafeNet Luna Network HSM is controlled through an enhanced version of the PKCS#11 hierarchy of roles, assigned to different users in your organization. Each role allows its user to execute a different set of commands to perform specialized tasks at one of the following levels:

## Appliance-Level Users and Roles

SafeNet Luna Network HSM consists of an HSM inside a secure appliance with a hardened operating system (accessed via the LunaSH command-line interface). Administration of the appliance (including network setup, file management, and system logging) is considered separate from administration of the HSM and its cryptographic functions. This separation of duties is essential to a secure environment and it allows you to easily delegate responsibilities to personnel.

Although appliance-level roles are not security roles as defined in the PKCS#11 standard, they do provide an additional level of security by requiring that the user be logged in to the appliance before they can log in to the HSM.

When one of the default appliance roles is logged in to LunaSH on the appliance, only the commands available to that role are visible. A user with **admin**-level access can create custom user roles to limit access to specified commands and operations.

**Table 1: Default Appliance Roles**

| Role | Function |
|------|----------|
| **admin** | > Can perform all administrative and configuration tasks on the appliance<br>> With the HSM Security Officer credential, can perform all HSM administrative tasks<br>> Activates other optional appliance roles and sets/resets their passwords<br>> Creates custom users and roles with access to a specified subset of commands<br>> Creates NTLS connections between the SafeNet Luna Network HSM appliance and Luna HSM Clients |
| **operator** | > Can perform administrative tasks on the appliance, except for some configuration tasks<br>> With the HSM Security Officer credential, can perform some basic HSM administration tasks<br>> Cannot execute any commands that affect other roles on the appliance |

| Role | Function |
|------|----------|
| **monitor** | > Executes commands that present information about the appliance and HSM<br>> Cannot affect the state or contents of the appliance or HSM |
| **audit** | > Initializes the Auditor role on the HSM<br>> With the Auditor credential, manages HSM audit logging |

## HSM-Level Roles

HSM roles are responsible for administration, configuration, and auditing of the HSM within the SafeNet Luna Network HSM appliance. After logging in to LunaSH with the appropriate appliance-level role, you can access commands available to the HSM roles.  HSM-level roles cannot perform cryptographic operations on the application partition.

**Table 2: HSM Roles**

| | |
|---|---|
| **HSM Security Officer (SO)**<br>**PED Key: Blue** | > Initializes the HSM, creating the SO credential<br>> Creates/deletes the application partition<br>> Configures global HSM policies<br>> Performs updates of the HSM firmware and appliance software<br>> Must have **admin**-level access to the appliance to perform all HSM tasks |
| **Auditor (AU)**<br>**PED Key: White** | > Manages HSM audit logging<br>> Must have **audit**-level access to the appliance to perform auditing tasks |

## Partition-Level Roles

Partition-level roles are responsible for administration and configuration of the application partition, and using the partition to perform cryptographic functions. Partition roles log in using LunaCM, or supply their credentials via crypto applications. An application partition acts as its own virtual HSM, and has its own set of roles.

**Table 3: Partition Roles**

| | |
|---|---|
| **Partition Security Officer (PO)**<br>**PED Key: Blue** | > Initializes the partition, creating the PO credential and setting the cloning domain<br>> Initializes the Crypto Officer role and can reset the CO credential (if permitted by HSM policy)<br>> Configures partition policies |
| **Crypto Officer (CO)**<br>**PED Key: Black** | > Creates and modifies cryptographic objects on the partition<br>> Manages backup and restore operations for the partition<br>> Performs cryptographic functions via user applications<br>> Creates and configures HA groups<br>> Initializes the Crypto User role and can reset the CU credential |

| | |
|---|---|
| **Crypto User (CU)**<br>**PED Key: Gray** | > Performs cryptographic functions via user applications (optional read-only role)<br>> Can create public objects only<br>> Can perform backup/restore of public objects on the partition |

# CHAPTER 7:  Authentication

Each SafeNet Luna HSM comes in one of two authentication types – Password authenticated or Multi-factor-authenticated (also called PED-authenticated). PED stands for PIN Entry Device. The authentication type is configured at the factory and cannot be modified in the field.

For an outline of the key differences between password and PED authentication, see "Authentication Types" below.

**Table 1: Authentication Types**

| Password Authentication (single factor) | PED Authentication (multi-factor) |
|---|---|
| Two-factor authentication is not available; relies on "something you know". | Two-factor authentication is available by way of physical PED Key per role and optional PED PIN per key; that is, can require "something you know" in addition to "something you have" for authentication |
| Authentication can be input locally or from a remote terminal. | Authentication requires physical local connection or pre-configured Remote PED link. |
| Knowledge of partition password is sufficient for accessing cryptographic keys. | Access to cryptographic keys is restricted to CO (read/write) and CU (read only); possession of appropriate PED key(s) and potentially also their PED PINs is required. |
| Dual or multi-person access control is not available. | Dual or multi-person (quorum) access control is available by way of MofN (split-knowledge secret sharing); physical PED Keys, each containing a portion of the role-authentication secret, can be held by separate people who must cooperate to perform authentication. |
| Key-custodian responsibility and role separation are linked to password knowledge only. | Key-custodian responsibility and role separation are linked to partition password knowledge *and* PED key(s) ownership / physical possession. |

For more detailed information on each authentication type, see:

> "Password Authentication" below

> "Multi-factor (PED) Authentication" on page 50

## Password Authentication

In general, there are two paths to access the SafeNet appliance and its HSM:

> The administrative path, via SSH or via local serial link, which uses the LunaSH command-line interface

> The client path, via SSL, by which client applications use the SafeNet Luna Network HSM API to perform cryptographic functions within pre-assigned virtual HSMs (called partitions) on the SafeNet system

For SafeNet Luna HSMs with Password Authentication, the various, layered roles are protected by passwords.

## HSM Admin

To access the HSM to perform HSM-specific administration tasks (set HSM-wide policies, update firmware and capabilities, backup and restore the HSM, create and remove HSM Partitions, etc.), you must be logged in to LunaSH as admin, then you must further be logged in as HSM Admin (of which there can be only one per SafeNet Luna HSM). Good security practices suggest that the HSM Admin password should be different from the appliance admin password. However, your corporate policies may differ. As the HSM Admin, you can connect locally, via a serial terminal, or remotely via SSH  – you must first be logged in as admin to have access to LunaSH commands.

## Partition Owner

To access HSM Partitions, in order to perform partition-specific administration tasks (set partition-specific policies, assign Partition to Clients, revoke Clients, etc.), you must be logged in to LunaSH as admin, then you must further be logged in as Partition Owner (of which there can be several - one for each partition in the HSM) , using the Partition Password. Good security practices suggest that the Partition Password should be different from the appliance admin password, different than the HSM Admin password, and different than other Partition Passwords (for other partitions). However, your corporate policies may differ. As the Partition Owner, you can connect locally, via a serial terminal, or remotely via SSH – you must first be logged in as admin to have access to LunaSH commands.

## Client

To access HSM Partitions with an application to perform cryptographic operations on data, you must connect remotely via SSL (called NTLS in our implementation) as a Client (one that has been registered by certificate exchange and assigned by the Partition Owner to this partition), then pass a User-type (this is done invisibly by your client application), and present the Partition Password (also done automatically by your application). The password used by a Client is the same Partition Password that is used by the Partition Owner for the particular partition. What limits the scope of operations that a registered, authenticated Client can perform on a partition is the fact that partition administrative commands can be issued only via LunaSH. Thus, for security, Clients must not be allowed to learn the appliance admin password that gives access to LunaSH.

## Authentication

Objects on the HSM are encrypted by the owner of the HSM Admin space or of the User space (partition), and can be decrypted and accessed only by means of the specific secret (password) imparted by the HSM Admin or the partition User respectively.

If you cannot present the secret (the password) that encrypted the objects, then the HSM is just a secure storage device to which you have no access, and those objects might as well not exist.

> **NOTE**  The administrative role secret is also the application-authentication secret: one plain-text secret used for two purposes. On a Password-authenticated HSM, once the administrator (Crypto Officer or Crypto User) has distributed the secret to the application(s), the only way to restrict access by applications (or personnel) that have come into possession of that secret is to change the password - which also changes the authentication for the associated administrative role.

## Advantages

Using password authentication, as opposed to PED authentication, has the following advantages:

> Convenience: changing passwords and authentication secrets is easy in the case of personnel changes or suspected compromise

> Direct mapping to organizational policies: password change policies already existing in an organization are easy to map onto a password authenticated framework

## Disadvantages

Passwords are less secure than the two-factor authentication provided by the PED, and thus have the following disadvantages:

> Vulnerability to observation: passwords being typed can be easily observed in person, through a camera, or with mal-ware like keystroke loggers

> Record-keeping: secure passwords are obscure and must be written, with its record securely stored

> Accountability: it is difficult to know who might have seen or been told a password

# Multi-factor (PED) Authentication

The connection between the Luna PED and the SafeNet Luna HSM is a secure trusted path.

> For the SafeNet Luna Network HSM, the PED connection is on the appliance rear panel.
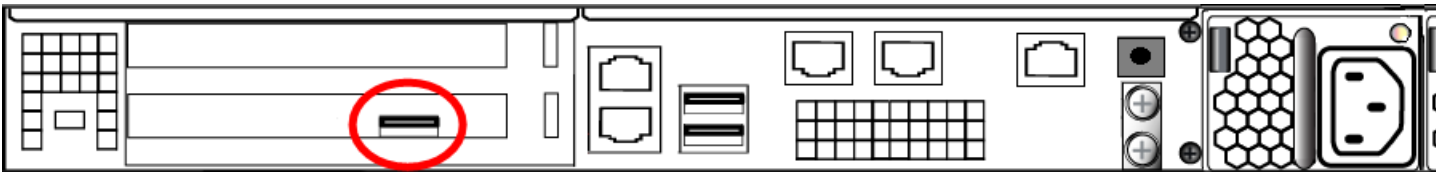


> For the SafeNet Luna PCIe HSM, the PED connection is a slot-edge connector, directly on the HSM card, accessible at the exterior of a tower or server computer (not through the host computer).
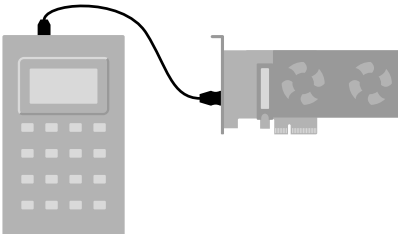


For Local PED, the connection is a secure physical link, directly to the HSM, bypassing the computer memory and bus.

For Remote PED, the PED Key information is made available from the PED location by a PedServer instance, and is received at the HSM location by a PedClient instance there. Two connection options are available:

> standard, or client-initiated Remote PED involves the PedClient reaching out to a PedServer; while the path is clear, the PED Key data is encrypted and secured at both ends by the Remote PED Vector (on an orange PED Key and in the HSM)

> peer-to-peer, or server-initiated Remote PED involves the PedServer instance reaching out to the PedClient instance, in order to satisfy HSM location behind a firewall that forbids outgoing initiation of connections; the PED Key data is secured at both ends by the Remote PED Vector (on an orange PED Key and in the HSM), and the network connection is secured by a TLS link, using previously exchanged certificates.

At no time does an authentication secret exist in-clear, anywhere in computer memory or on any computer bus.

In general, there are three paths to access the SafeNet Luna HSM:

> The administrative path, via SSH or via local serial link, which uses the LunaSH command-line interface

> The Client path, via TLS (our implementation is called NTLS), by which client applications use the SafeNet Luna HSM API to perform cryptographic functions within pre-assigned virtual HSMs (called Partitions) on the HSM

> The Trusted Path, used for authentication data passed from the PED and PED keys - this path ensures that HSM authentication data does not pass unencrypted through a host or terminal computer, where it might be subject to attack. This applies only to PED-authenticated (multi-factor) HSMs.

For SafeNet Luna HSMs with PED Authentication, the various layered roles are protected by a combination of PED keys and passwords.

## HSM Admin (Security Officer)

To access the HSM to perform HSM-specific administration tasks (set HSM-wide policies, update firmware and capabilities, backup and restore the HSM, create and remove HSM Partitions, etc.), you must first be authenticated as SO (Security Officer) or HSM Admin (of which there can be only one per SafeNet Luna HSM). The authentication data for SO/HSM Admin is a secret carried on a blue PED key. For the SO to login and issue HSM commands, someone must be present at the connected local Luna PED, or at the configured Remote Luna PED, to insert the required blue PED key when prompted. Otherwise, HSM commands cannot be used.

## Partition User (Crypto Officer)

To access HSM Partitions to perform partition-specific administration tasks, such as setting partition policies, assigning partitions to clients, or revoking clients, you must be authenticated as Partition User. There can only be one Partition User per HSM on the SafeNet Luna PCIe HSM, or there can be several on the SafeNet Luna Network HSM - one for each partition. The authentication data for the CO (Crypto Officer) or Partition User is both a password and a secret carried on a black PED key. As the Partition User/CO, you can connect locally, via a serial terminal, or remotely via SSH. To perform partition administration on SafeNet Luna Network HSM, you must first be logged in as admin to have access to LunaSH commands.

> For the SafeNet Luna PCIe HSM, you simply need access to the host computer, where you can use LunaCM commands. For the Partition User/CO to login and issue partition administration commands, someone must be present at the connected Luna PED (or the configured and validated Remote PED) to insert the required black PED key when prompted, or the partition must have been left in Activated state.

> For the SafeNet Luna Network HSM, good security practices suggest that the Partition Password be different than the appliance admin password, and different from other Partition Passwords.

If you have invoked the Crypto Officer/Crypto User distinction, there are two Partition Passwords, but only the Crypto Officer password allows you to run LunaSH or LunaCM commands to administer the partition. It is also recommended that the passwords for each of these roles differ.

**Client (Crypto User)**

To access HSM Partitions with an application to perform cryptographic operations on data, you must pass a User-type (this is done invisibly by your client application), and present the Partition Password (also done automatically by your application).

> For a standard "Client", the password is the same Partition Password that is used by the Partition User for the particular partition. What limits the scope of operations that a registered, authenticated Client can perform on a partition on a SafeNet Luna Network HSM is the fact that partition administrative commands can be issued only via LunaSH. Thus, for security, Clients should not be allowed to learn the appliance admin password that gives access to LunaSH command line. For SafeNet Luna PCIe HSM, the password or other authentication that gives access to the client application is often the same authentication that gives access to LunaCM for partition administration, so the ability to keep roles separate is more dependent on control of PED keys.

> For a Crypto User client, the password is different from the Crypto Officer password, offering another layer of protection for the partition and its contents.

**Auditor**

This role combines a special, limited-access appliance account and a special HSM role authenticated by the white PED key, for the purpose of managing HSM audit logs. The auditor is distinct and separate from other role on the appliance and the HSM, conforming to the requirements of auditing standards.

# Remote PED

By default, Luna PED is connected directly to the HSM via a USB cable, and powered by the included power block. However, Luna PED can also be used remotely from the HSM(s) for which it manages access control. When it is not convenient to be physically near the host computer that contains a SafeNet Luna HSM you can operate remotely and securely.

The PED-Authenticated SafeNet Luna HSM, and one or more orange PED keys are imprinted with a Remote PED Vector (RPV). This can occur at any time before the HSM is deployed, and requires a locally connected PED. All future PED and PED key interactions can then be accomplished distantly from the HSM, as follows:

1. One computer, running a supported OS, hosts the HSM. This could be:

   • A server or tower containing a SafeNet Luna PCIe HSM.

   • A SafeNet Luna Network HSM appliance.

   The HSM host computer must be network attached. HSM administration commands can be input locally, or via remote connection, but the network connection is essential for Remote PED operation.

2. A second computer (laptop, workstation, server running a supported OS) has a Luna PED (Remote Capable) attached via USB, and powered via its included power block. The Remote PED host computer must be network attached. The administration of the distant HSM host does not have to come from this Remote PED host computer, but it is usually done that way, since the person handling the PED must coordinate with the person giving commands to the HSM. The Remote PED host computer and PED must have the orange Remote PED Key (RPK) available, along with:

   • Either blue, black and red (optionally, white) PED keys that were imprinted with the HSM previously

   • Or blank blue, black, and red (optionally, white) PED keys that are about to be imprinted along with the HSM

3. The HSM is told to look to a remote PED for its authentication requests.

4. The PED host computer has the LunaPED driver installed, and runs the pedserver utility.

5. The HSM host computer runs the pedclient utility, and the HSM is told to connect to the Remote PED.

6. The Remote PED (via the pedserver) receives the request and prompts for the orange PED Key.

   The Remote PED and the HSM (via the pedclient/pedserver connection) must agree that the provided orange PED key contains the same Remote PED Vector as the one imprinted on the HSM, and only then is the secure Remote PED link is established.

7. The HSM SO runs commands on the HSM (on the host computer) via remote desktop or SSH connection.

All future authentication for the HSM can be performed at the Remote PED, with no need for personnel to visit the HSM host, which could be locked away in a lights-off facility on the other side of the world.

## Authentication

Objects on the HSM are encrypted by the owner of the HSM Admin space (rarely) or of the User space (partition), and can be decrypted and accessed only by means of the specific secret injected from the blue PED key (HSM Admin) or the black PED key (User) respectively.

If you cannot present the secret (the PED key) that encrypted the objects, then the HSM is just a secure storage device to which you have no access, and those objects might as well not exist.

### Challenge Secrets

When the HSM is PED-authenticated:

> The administrative role secret contained on a black or gray PED key is one secret, used only by administrative personnel.

> The challenge-secret or password is a second secret (plain text, initially presented on the PED screen, but you can change it), which is the application-authentication secret, that allows the HSM verify that the presenting application is entitled to perform cryptographic operations on the particular application partition.

The application can submit its own authentication (that second secret) only after the PED key secret has "opened" the HSM partition for operation (by Activating it). That is, there are two levels of protection: one administrative, and the other operational, where the operational level is gated by the administrative level.

### Activation

By default, PED-authenticated partitions require that a PED key and challenge password be provided each time a user or application authenticates to the HSM. For some use cases, such as key vaulting, the need to provide a physical key to access the HSM may be desirable. For most application use cases, however, requiring a physical key each time the application accesses the HSM is impractical.

Activation allows registered users and applications to authenticate to the HSM without a PED key, using only a challenge secret. The PED key secret for the CO or CU role is copied the first time you perform an action that requires authentication, and it is cached on the HSM.

The ability to use activation is determined by its corresponding policy. Enabling this policy will allow you to use activation.

### Auto-Activation

In the event of a restart or short power outage, activated roles are deactivated and must re-authenticate with a PED key and challenge secret.

Auto-activation enables automatic re-activation of an activated role, so that users or applications do not have to provide a PED key again to reactivate their role.

The ability to use auto-activation is determined by its corresponding policy. Enabling this policy will allow you to use auto-activation.

## Advantages

Using PED authentication, as opposed to password authentication, has the following advantages:

> Security: no written record of the secret or password exists, so it cannot be compromised

> Tracking: access and handling of physical devices (PED keys) can be tracked and controlled

> Duplication restrictions: duplication and promulgation can be prevented by physical security measures

> Physical device: using the PED to input passwords and PEN PINs prevents key-logging exploits that typed passwords are vulnerable to

## Disadvantages

PED keys are physical items that can be lost or misplaced, unlike passwords, and thus have the following disadvantages:

> Password change policies: scheduled or mandated password-change cycles in an organization can be logistically intensive when HSMs share PED key secrets

> Inconvenience: handling of secrets requires hands-on, physical action by personnel to perform changes of authentication secrets in case of compromise

# CHAPTER 8:   Appliance Administration

There are several ways to access to your SafeNet Luna Network HSM appliance to perform administrative operations, depending on what works best for you and your organization. They include:

> **Luna Shell (LunaSH)**: a custom command-line interface that can be accessed by using any SSH-capable utility.

> **SafeNet REST API**: a secure web application that can perform many LunaSH functions via scriptable REST APIs.

> **SafeNet Crypto Command Center**: a web-based application that provides separate administrative and application owner interfaces.

The LunaSH command line interface is the standard secure interface with which you can perform operations on your HSM. It creates a secure administration channel for administrative sessions only. The REST API is specifically tailored for the management of your appliance, and does not allow applications to perform cryptographic operations. Crypto Command Center is a highly useable web-based application that facilitates rapid service provisioning and employment. Each of these administrative interfaces allows you to efficiently manage your appliance in different ways.

For detailed instructions on using the LunaSH command line, see About the LunaSH Command Reference. For the REST API and Crypto Command Center applications, refer to their corresponding documentation.

## Appliance Management

The SafeNet Luna Network HSM appliance comes equipped with features that prevent attackers from stealing your proprietary information. Some of these features need to be maintained for maximum protection, and doing so is simple and efficient.

### Physical Maintenance

Physical maintenance, such as replacing power supplies and fans, does not require you to turn off your HSM. This allows you to continue working, and return to the appliance as you left it once you finish maintenance.

### Appliance Roles and Users

Appliance roles, users, and time are configured independently from the HSM(s) inside the appliance. This separation of duties is beneficial to keeping a secure environment and to easily delegate responsibilities to personnel as you wish.

When you login to the SafeNet appliance via LunaSH the accepted IDs are **admin** which requires the admin password, **operator**, which requires the operator password, or **monitor** which requires the monitor password.

As the appliance admin, you can connect and log in locally, via a serial terminal, or remotely via SSH. With no further authentication, admin can perform general, appliance-level administration (not accessing the HSM), and can run view/list/show/display commands on the HSM that do not make changes. Admin sees the full available command set, while operator- and monitor-level users see only subsets that allow them use or read-only access to the appliance respectively. Additional, custom user roles can also be created to restrict user access to specific commands and operations.

**Appliance Authentication**

If any administrative user attempts an HSM command that needs authentication, the interface prompts for that authentication.

On PED-authenticated systems, you are directed to the PED, which prompts for PED keys and keypad actions.

The way you manage and configure your appliance is flexible, adapting to your needs.

# CHAPTER 9:   Capabilities and Policies

HSMs, and partitions within them, are characterized by capabilities that are set at the factory, or added by means of capability updates, and that are adjusted by means of settable policies that correspond to some of the capabilities. HSM capabilities, and the HSM policies that derive from them, apply HSM-wide. Application partition capabilities, and the application partition policies that derive from them, can be inherited from the HSM, or control characteristics that make sense only at the application partition level. "Capability and Policy Inheritance" below illustrates an example of how capabilities and policies can be inherited from the HSM-level to the partition-level on a SafeNet Luna Network HSM.

**Figure 7: Capability and Policy Inheritance**
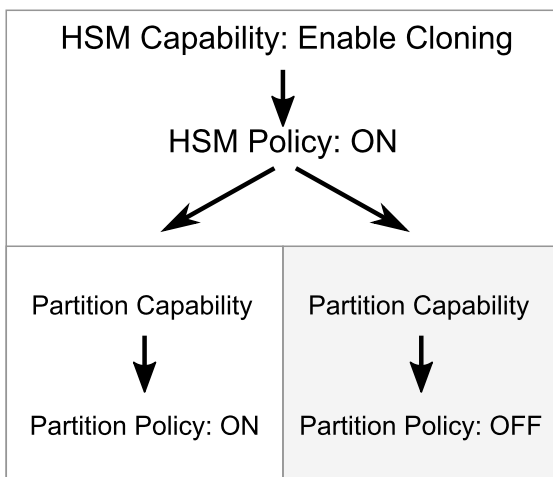


All policies have an equivalent capability, but not all capabilities are matched by a policy that allows adjustment of the capability. The HSM administrator is responsible for setting up the HSM with capabilities, but it is up to the Partition SO to enable their corresponding policies.

Some policy settings are numerical values that can be increased or decreased. Most policy settings are simply OFF/ON switches. Policy setting requires that the SO be logged in. For HSM-wide policies, that is the HSM SO. For partition-level policies, that is the Partition SO.

## Set Policies

Set policies with the **hsm changepolicy** command or the **partition changepolicy** command, as appropriate. The command requires that you identify the policy number that is to change, and the new value it is to hold. For OFF/ON policies, the value is set as zero or one, respectively.

For detailed lists of HSM and Partition capabilities, as well as their corresponding policy settings, see:

> HSM Capabilities and Policies
> Partition Capabilities and Policies

**Example: Cloning**

The cloning operation allows you to duplicate or copy the contents of your HSM or partition to other HSMs or partitions that share a cloning domain. The HSM capability that controls cloning on your HSM is Enable Cloning. The equivalent HSM Policy, Allow Cloning, is the modifiable switch that turns cloning on or off for your specific HSM.

> **NOTE**  Turning cloning ON or OFF is destructive, and resets your HSM. Ensure that you decide early on in your configuration whether or not you will be using this capability.

"Cloning Capability Inheritance" below shows how the cloning capability is inherited by partitions within your HSM, depending on whether you turn it on or off when you set its policy value.

**Figure 8: Cloning Capability Inheritance**
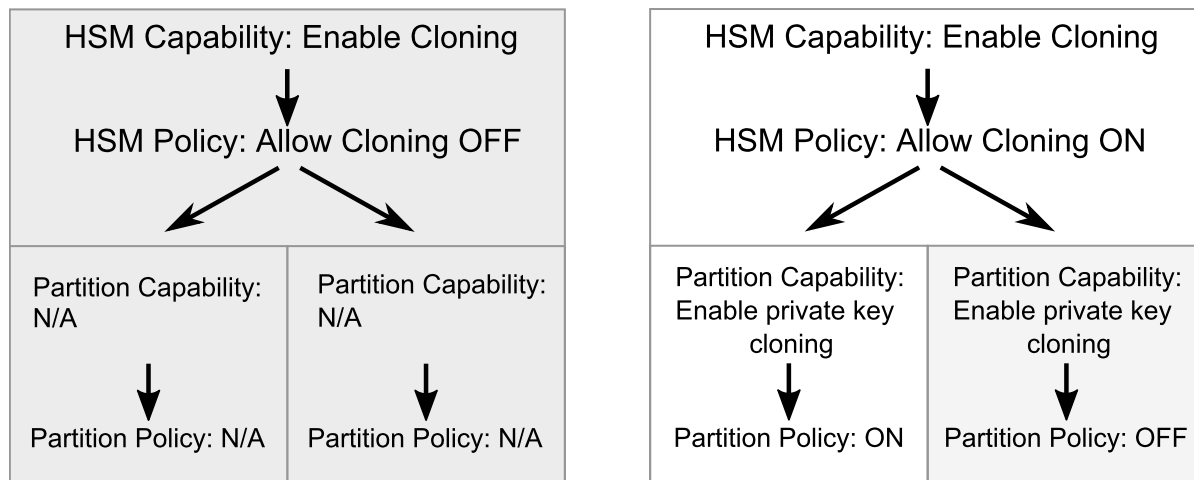


If cloning is not allowed HSM-wide, then no partition on the HSM will be able to use cloning.

If cloning is allowed HSM-wide, then each partition inherits that capability and can independently decide whether it wants to enable it.

# CHAPTER 10:  Flexible Backups

While some applications might deal in ephemeral objects that are erased after their use, in many SafeNet Luna HSM applications the keys and objects within the HSM and partition have value and are meant to persist. For such valuable data, any security regime requires that the data be backed up in secure fashion, and stored securely.

Backup and restore operations require access to the objects in your partition in order to copy them. As such, backup and restore operations are restricted to HSMs that share a cloning domain and partitions whose administrators allow access to.

> **NOTE**  This section describes the backup options G5-based Backup HSM. For a description of the G7-based Backup HSM, see Backup and Restore Using a G7-Based Backup HSM.

## Backup

Backup operations copy the secure material on your HSM and store it on a separate Backup HSM. Backup is not performed continuously. The frequency of backup is dependent on your backup plan or strategy.

The SafeNet Luna Backup HSM can be connected directly to the HSM to perform backup or restore operations on the spot. It is not able to perform cryptographic operations; it functions only in its secure backup/restore role. The Backup HSM takes on the authentication type of the primary HSM with which it is paired for backup - so it becomes a password-authenticated Backup HSM when backing up a password-authenticated primary HSM, and a PED-authenticated Backup HSM when backing up a PED-authenticated primary HSM.

The Backup HSM can also be connected to a host computer, located at a distance from the source HSM, and can perform backup and restore operations over secure network connection. This is normally the case when the source HSM is kept in a secure server room or a lights-out facility.

There are several ways to do backup with SafeNet Luna HSMs. Depending on the type and number of HSMs and partitions you have, and how they are organized, different methods may be more suitable for your situation. The following sections describe these methods in more detail:

> "Local Backup" on the next page

> "Remote Backup" on the next page

> "Comparing Local Versus Remote Backup" on page 61

## Restore

Restore operations are only necessary if there is no hope of recovering your data on your HSM, and using your backup to restore the content is the only solution. The restore operation is identical to the backup operation, only in the opposite direction.

## Local Backup

Local backup requires a direct connection to the HSM to be successful. Backup can be done directly from the secure appliance housing the HSM or from a client workstation connected to the HSM.

### Centralized Local Backup

Centralized backup uses a direct connection between the HSM you wish to back up and the Backup HSM. "Centralized Local Backup" below outlines the basic setup required for simple local backup.

**Figure 9: Centralized Local Backup**
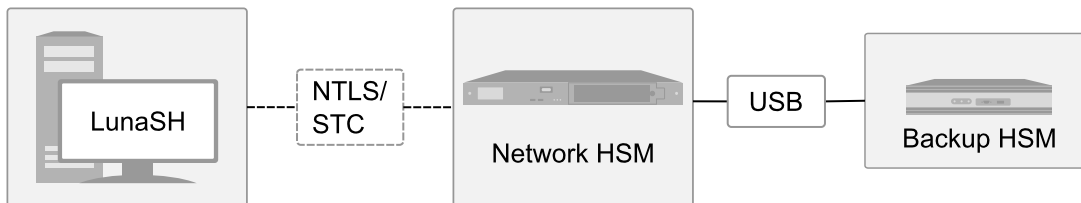


Connecting your Backup HSM directly to the HSM or secure appliance housing the HSM you wish to back up is a highly secure method of copying your keys. It requires you to have physical access to the HSM in addition to the HSM SO and Partition SO credentials for every partition needing backup. The backup operation is initiated from the LunaSH command line.

### Client-side Local Backup

Client-side backup connects to the HSM you wish to back up via your client workstation. The Backup HSM connects directly to the client workstation to perform backup. "Client-side Local Backup" below outlines the basic setup required for local backup via client workstation.

**Figure 10: Client-side Local Backup**
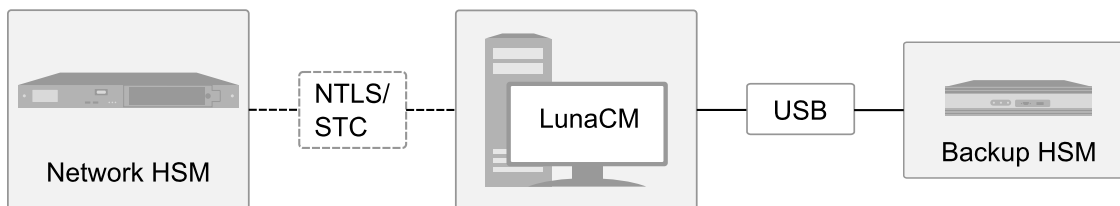


The backup operation in this case is still local, and thus requires a direct wired connection between your Backup HSM and client workstation. This method is highly secure, and allows for some flexibility in case the HSM you wish to back up is not easily available for direct connection. A PC running Luna HSM Client and LunaCM can connect to the HSM and, with the appropriate Partition SO credentials for every partition needing backup, can access and securely copy your cryptographic keys.

## Remote Backup

Remote backup allows you to securely back up your HSM from any location that is convenient. A secure network connection facilitated by RBS enables you to access your HSM or partition without needing to be physically near it. "Remote Backup" on the next page outlines the basic setup required for remote backup.

**Figure 11: Remote Backup**
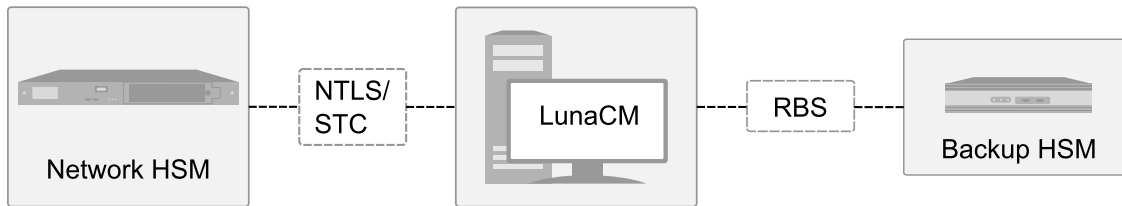


Remote Backup Service (RBS) runs on a system hosting a SafeNet Luna Backup HSM, making the Backup HSM available to distant HSMs. This allows backup and restore operations to run from any location most convenient for the administrator. In this configuration, backup and restore operations are performed over secure network connection.

## Comparing Local Versus Remote Backup

Regardless of whether you use a local connection to backup and restore your HSM, or whether you use a remote one, backup and restore operations always require a Backup HSM. How you decide to connect it and organize your backup/restore infrastructure depends on what your organization needs.

Local backup is easier and faster to configure than remote, but the remote option allows more secure storage of your cryptographic material in case the entire environment in which your HSM resides collapses.

For detailed instructions on carrying out backup and restore operations, see Backup and Restore Using a G5-Based Backup HSM or Backup and Restore Using a G7-Based Backup HSM.

# CHAPTER 11:  Logging and Reporting

SafeNet Luna Network HSM allows you to track and report all activity on your HSM to encourage responsibility, ensure accountability, and upkeep tight security.

Both SafeNet Luna Network and PCIe HSMs come equipped with HSM-level audit logging via Audit role. See "HSM-Level Audit Logging" below.

The SafeNet Luna Network HSM also includes appliance-side audit logging and services that monitor your HSM's performance. See "Appliance-Level Performance Monitoring" below.

## HSM-Level Audit Logging

Monitoring HSM activity is essential to maintaining a high level of security for the highly sensitive material on your HSM. SafeNet Luna HSMs have logging and reporting abilities to support this. These features are implemented in the HSM firmware for maximum security.

**Logging**

Secure logging is done at the whole HSM level. The HSM stores a record of past operations that is suitable for security audit review. Audit logging sends HSM log event records to a secure database on the local file system, with cryptographic safeguards ensuring verifiability, continuity, and reliability of HSM event log files.

Each log entry indicates what event occurred when, and who initiated it. Critical events are logged automatically.

**Audit Management**

For circumstances that require more comprehensive review of events taking place on the HSM, an HSM-level Audit role (White PED key for PED-authenticated HSMs) can be used. Each HSM has a unique Audit role whose purpose is to manage audits and monitor HSM activity.

The Audit role is independent from the other roles on the HSM. Creating the Audit role does not require the presence of the HSM SO and if the Audit role is initialized, the HSM and partition administrators are prevented from working with the log files. Only the Auditor can add failures, successes, key usage, and other events to the HSM logging procedure.

Audit log integrity is ensured against altering log records. Separating logging and its role from other administrative roles protects critical information related to the operations of your HSM.

For detailed instructions on implementing audit logging, see Audit Logging.

## Appliance-Level Performance Monitoring

SafeNet Luna HSMs monitor their own conditions for issues that might require administrative attention. Appliance-side logging of HSM activity moves HSM logging directly into the appliance file system. The purpose is to record HSM operations while bypassing the resource-heavy in-HSM log security features. Like at the

HSM-level, appliance-level logging and auditing are split into separate services and roles. Only the Auditor on the appliance can engage in audit management. The Audit role is separate from Admin, Operator, and Monitor.

Appliance performance monitoring can be done via LunaSH, SafeNet Crypto Command Center, or SafeNet REST-API. LunaSH allows you to specify commands yourself, while the latter two provide a friendly user interface to query the appliance.

## Syslog

Syslog is a standard logging facility that writes messages it gets from the appliance to organized log files.

When a sensor reading on the appliance changes by an amount that crosses a configured threshold, the appliance will generate log messages according to their severity. These logs can be checked and accessed by an audit user.

## SNMP

SafeNet Luna HSMs also support remote monitoring of conditions on a local HSM via SNMP (Simple Network Management Protocol). Should the condition of your HSM change in a way that requires your attention, SNMP will alert you via trap notification. Condition changes can include changes in memory or CPU usage, network connection status, and some environmental variables.

You can configure SNMP according to your organization's preferences; it is a flexible and optional feature. SNMP is secure and efficient, ensuring that faults in your HSM are detected early and that your cryptographic information remains safe.

For detailed instructions on implementing SNMP, see SNMP Monitoring.

# CHAPTER 12: Functionality Modules

Functionality Modules (FMs) consist of your own custom-developed code, loaded into and operating within the logical and physical security of a SafeNet Luna Network HSM as part of the HSM firmware. FMs allow you to customize your SafeNet Luna Network HSM's functionality to suit the needs of your organization. Custom functionality provided by your own FMs can include the following:

> new cryptographic algorithms, including Quantum algorithms

> security-sensitive code, isolated from the rest of the HSM environment

> keys and critical parameters managed by the FM, independent from standard PKCS#11 objects, held in tamper-protected persistent storage

To create FMs, you will need the Functionality Module Software Development Kit (SDK), which is included with the Luna HSM Client software.

See "About the FM SDK Guide" on page 1 and "Functionality Modules" on page 1 for details and procedures.

> **NOTE**
>
> This feature has hardware dependencies described in Preparing the SafeNet Luna Network HSM to Use FMs.