THALES

Thales Luna USB HSM 7

PRODUCT OVERVIEW

Document Information

Last Updated	2025-08-27 11:24:28 GMT-05:00

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

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

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

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

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

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

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

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

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 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.

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

This document provides an overview of the 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 specific releases. Read the CRN to fully understand the capabilities, limitations, and known issues for each release. You can view the latest version of the CRN at www.thalesdocs.com.

Audience

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

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

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

Document Conventions

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

Notes

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

> **NOTE** Take note. Contains important or helpful information.

Cautions

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

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

Warnings

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

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

Command syntax and typeface conventions

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

Format	Convention
<variable>	In command descriptions, angle brackets represent variables. You must substitute a value for command line arguments that are enclosed in angle brackets.
[**optional**] [<optional>]	Represent optional **keywords** or <variables> in a command line description. Optionally enter the keyword or <variable> that is enclosed in square brackets, if it is necessary or desirable to complete the task.
{**a**|**b**|**c**} {<a>|<b>|<c>}	Represent required alternate **keywords** or <variables> in a command line description. You must choose one command line argument enclosed within the braces. Choices are separated by vertical (OR) bars.
[**a**|**b**|**c**] [<a>|<b>|<c>]	Represent optional alternate keywords or variables in a command line description. Choose one command line argument enclosed within the braces, if desired. Choices are separated by vertical (OR) bars.

Support Contacts

If you encounter a problem while installing, registering, or operating this product, please 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 is governed by the support plan negotiated between Thales and your organization. Please consult this plan for details regarding 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 and create and manage support cases. It offers 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.

> **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: 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 "Luna Network HSM 7" below.
- Hardware cards that plug into existing network-attached systems, as described in "Luna PCIe HSM 7" on the next page.
- Portable USB-connected HSMs that connect to a client system, as described in "Luna USB HSM 7" on page 12.
- USB-connected backup HSMs, as described in "Luna Backup HSM" on page 13.

For a comparison of the Luna HSM variants, and descriptions of the available models:

- "Comparing the Luna HSM Variants" on page 13
- "Luna HSM Models" on page 14

For a high-level overview of the distinctive features of the Luna HSM, see "Luna HSM Features" on page 15.

Luna Network HSM 7

Luna Network HSM 7 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, Luna Network HSM 7 works seamlessly across your on-premises, private, public, hybrid, and multi-cloud environments. Luna Network HSM 7 is the most trusted general purpose HSM on the market, and with market leading performance, true hardware-based security, and the broadest ecosystem available, Luna Network HSM 7 is at the forefront of HSM innovation.

Ethernet-attached

An Ethernet-attached HSM, Luna Network HSM 7 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 Luna Network HSM 7 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 Luna Network HSM 7 offers powerful key management and high-performance cryptographic processing to clients on the network. To achieve this, the Luna Network HSM 7 includes an integrated FIPS 140-3[*-validated HSM and the Luna K7 Cryptographic Engine. Additionally, the Luna Network HSM 7 adds a secure service layer that allows the Cryptographic Engine to be shared between network clients.

[*Firmware version 7.8.4 of Luna PCIe HSM 7 and Luna Network HSM 7 HSMs was the first to be validated at FIPS 140-3, while earlier firmware versions were validated against FIPS 140-2.]

Partitions

The Luna Network HSM 7 allows its single physical HSM to be divided into logical HSM partitions, each with independent data, access controls, and administrative policies. HSM partitions can be thought of as ‘safe 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 safe deposit boxes protect their specific contents from people who have access to the vault by having separate access-control keys. 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 model, a Luna Network HSM 7 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 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 Luna Network HSM 7. Each Client is assigned to one or more specific HSM partitions. Clients authenticate to the Luna Network HSM 7 with a digital certificate and unique HSM partition challenge.

Employ the HSM as a Service

Luna Network HSM 7 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 Luna Network HSM 7 is able to provide trusted key ownership and control, with full multi-tenancy across on-premises, private, public, hybrid, and multi-cloud environments.

Luna PCIe HSM 7

Luna PCIe HSM 7 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 Luna PCIe HSM 7 cryptographic processes are offloaded to a high-performance cryptographic processor. Luna PCIe HSM 7 easily embeds in

servers and security appliances for an easy-to-integrate and cost-efficient solution for FIPS 140-3** validated key security. Luna PCIe HSM 7 benefits from a diverse feature set that enables greater centralized control through secure remote management, transport, and backup.

[**Firmware version 7.8.4 of Luna PCIe HSM 7 and Luna Network HSM 7 HSMs was the first to be validated at FIPS 140-3, while earlier firmware versions were validated against FIPS 140-2.]

Single-partition

The Luna PCIe HSM 7 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 Luna PCIe HSM 7 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 the other Luna HSMs, the Luna PCIe HSM 7 securely stores cryptographic keys in its hardware; sensitive information never leaves the HSM protection. The Luna PCIe HSM 7 provides PKCS#11-compliant cryptographic services for applications running on the server in a secure and tamper-proof hardware package. Leveraging a Luna PCIe HSM 7 in your appliance or service represents a cost effective way to bring FIPS 140-2 or -3, Common Criteria, and eIDAS-validated solutions to market.

Luna PCIe HSM 7 empowers organizations to take a best practices approach to cryptographic key security by offloading cryptographic processes to a dedicated small form factor cryptographic processor. Luna PCIe HSM 7 is the highest performing embedded HSM on the market.

Luna USB HSM 7

Luna USB HSM 7 stores, protects, and manages sensitive cryptographic keys in a small form factor handheld device, providing a root of trust for sensitive cryptographic data transactions. Luna USB HSM 7 connects directly to a client workstation to provide PKCS#11-compliant cryptographic services, and can be secured safely as an offline root of trust. Luna USB HSM 7 provides easy multifactor quorum authentication, using USB iKey connected directly to the HSM and its built-in touchscreen to authenticate critical roles.

Portable

The Luna USB HSM 7's hand-held form factor and USB connectivity make it the most portable model of Luna HSM. This allows you to easily store your important keys and connect the device to any client to perform cryptographic operations.

Easy to Store and Use

The Luna USB HSM 7 can be stored indefinitely, making it ideal to safely store an offline root of trust, and retrieve from storage only when that root of trust is required. Using the Luna USB HSM 7 is as simple as connecting it to a client with the correct Luna HSM Client components installed.

Self-Contained

The Luna USB HSM 7 can be operated entirely from the Luna HSM Client computer. Its built-in touchscreen allows you to perform all multifactor quorum authentication and iKey management operations locally, with no need to connect a Luna PED.

Single-partition

The Luna USB HSM 7 is a single-partition HSM. Access to the partition is managed by a special access control role. The Luna USB HSM 7 offers hardware accelerated RSA 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.

Cost Effective

Like the other Luna HSMs, the Luna USB HSM 7 securely stores cryptographic keys in its hardware; sensitive information never leaves the HSM protection. The Luna USB HSM 7 provides PKCS#11-compliant cryptographic services for applications running on the client in a secure and tamper-proof hardware package. Leveraging a Luna USB HSM 7 in your appliance or service represents a cost effective way to bring FIPS-validated solutions to market.

Luna Backup HSM

The Luna Backup HSM allows you to back up the objects in your Network, PCIe, or USB application partitions and store the object archive in a secure HSM. Luna 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 35 for more information.

Two versions are available, as detailed in "Backup HSM Models" on page 15.

Comparing the Luna HSM Variants

Luna Network HSM 7 Appliance	Luna PCIe HSM 7	Luna USB HSM 7
> Field-upgradable to 100 partitions > Includes hardened OS > High security, stable networking, and environmental protection via built-in chassis > Routine firmware and software updates > Automatic system logging	> Limited to 1 partition > Compatible with external OS: Windows, Linux > Allows custom and flexible chassis intrusion security > Routine firmware updates > Light and low-cost	> Limited to 1 partition > Compatible with external OS: Windows, Linux > Portable, hand-held device with touchscreen PIN entry > Routine firmware updates

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 Luna Network HSM 7 bypasses this limitation by

implementing multiple virtual HSMs, or HSM Partitions on a single HSM server. A Luna PCIe HSM 7 is useful for cases that need limited, but highly secure, data protection. A Luna Network HSM 7 and its appliance are useful for cases that require a more complex security infrastructure, like cloud computing.

Luna HSM Models

Both the Luna Network HSM 7 and the Luna PCIe HSM 7 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	Luna Network HSM 7	Luna PCIe HSM 7
Luna A700	> Standard performance > 2 MB memory (4 MB from firmware version 7.7.0 onward) > Password-based authentication > 5 partitions	> Standard performance > 2 MB memory (4 MB from firmware version 7.7.0 onward) > Password-based authentication
Luna A750	> Enterprise-level performance > 16 MB memory (32 MB from firmware version 7.7.0 onward) > Password-based authentication > 5 partitions, upgradable to 20	> Enterprise-level performance > 16 MB memory (32 MB from firmware version 7.7.0 onward) > Password-based authentication
Luna A790	> Maximum performance > 32 MB memory (64 MB from firmware version 7.7.0 onward) > Password-based authentication > 10 partitions, upgradable to 100	> Maximum performance > 32 MB memory (64 MB from firmware version 7.7.0 onward) > Password-based authentication

Luna S (multifactor quorum-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 quorum (PED) authentication. Depending on your needs, Luna S models are available at several performance levels, as follows:

Model	Luna Network HSM 7	Luna PCIe HSM 7
Luna S700	> Standard performance > 2MB memory (4MB from firmware version 7.7.0 onward) > Multifactor Quorum authentication > 5 partitions	> Standard performance > 2MB memory (4MB from firmware version 7.7.0 onward) > Multifactor Quorum authentication
Luna S750	> Enterprise-level performance > 16MB memory (32MB from firmware version 7.7.0 onward) > Multifactor Quorum authentication > 5 partitions, upgradable to 20	> Enterprise-level performance > 16MB memory (32MB from firmware version 7.7.0 onward) > Multifactor Quorum authentication
Luna S790	> Maximum performance > 32MB memory (64MB from firmware version 7.7.0 onward) > Multifactor Quorum authentication > 10 partitions, upgradable to 100	> Maximum performance > 32MB memory (64MB from firmware version 7.7.0 onward) > Multifactor Quorum authentication

Backup HSM Models

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

> multifactor quorum-authenticated backup HSMs can back up multifactor quorum-authenticated partitions.

> password-authenticated backup HSMs can back up password-authenticated partitions.

Two versions are available:

> the Luna Backup HSM G5 desktop model

> the Luna Backup HSM 7 is available in the following models. Each model allows you to back up up to 100 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
B790	256 MB storage, up to 100 partitions of the same authentication type

Luna HSM Features

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

Security	Luna HSMs are designed and manufactured to high security standards, to comply with FIPS Level 3 and Common Criteria certifications, and updated validations are sought whenever major changes/improvements are introduced. Luna HSMs protect your data from unwanted tampering with secure anti-intrusion and vulnerability detection mechanisms. See "Security" on page 17 for details.
Redundancy	Luna HSMs are equipped with physical features and configurations that enable auto-recovery of your HSMs. See "Redundancy and Reliability" on page 24 for details.
Access control	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. See "User Access Control" on page 31 for details.
Authentication	Luna Network HSM 7s and Luna PCIe HSM 7s are factory-configured to be either: > password-authenticated (single-factor authentication) > multifactor quorum-authenticated (physical iKey authentication with option for quorum authentication) The Luna USB HSM 7 can be initialized using either method, to be compatible with your existing Luna HSM deployment. See "Authentication" on page 27 for details.
Capabilities and policies	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. See "Capabilities and Policies" on page 33 for details.
Backups	Luna HSMs contain sensitive material that, if lost, could be detrimental. The Luna Backup HSM and Remote Backup Service securely back up and store such information that can be restored in case of failures in primary HSM functioning. See "Flexible Backups" on page 35 for details.
Logging and reporting	Luna HSMs are equipped with performance monitoring and audit logging features to monitor security and provide audits of HSM activity. See "Logging and Reporting" on page 37 for details.

CHAPTER 2: Security

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

Layered Encryption

Luna HSMs do not keep any objects unencrypted. 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 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 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.

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 securely 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.
> Other than direct use of the partition clone command, 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.

Scalable Key Storage

Luna HSM Firmware 7.7.0 and newer supports Scalable Key Storage (SKS), the ability to securely store off-board many more keys than can fit within the bounds of the HSM card hardware. Partitions at Luna HSM Firmware 7.7.0 and newer can be configured in one of the following ways by the HSM SO:

- version zero (V0) partitions, the default, continue to use the cloning model described above (also referred to as "Keys in Hardware")
- version one (V1) partitions use cloning only for the SKS Master Key (SMK), while all other backup/restore and HA operations involve keys and objects being exported and imported as encrypted binary large objects (blobs), while otherwise remaining securely encrypted in external storage (either in Luna Network HSM 7 appliance storage or on a host computer for a Luna PCIe HSM 7 or Luna USB HSM 7)

The SMK secures all stored keys and objects within the security perimeter of the HSM, even when they reside in offboard storage because:

- the keys and objects are securely encrypted with the SMK when not in use inside the cryptographic module.
- the SMK is secured by the traditional "keys in hardware" cloning/security domain, and can be copied only to another HSM or partition that shares the specific cloning/security domain. The cloning (or security) domain is set by the Partition SO and changes only through intentional action of the Partition SO, for the life of the partition.

On V1 partitions, HA replication and synchronization that traditionally used cloning transparently use a combination of SMK cloning and SKS extract/insert operations. An operation like a cloning command or backup/restore command invokes cloning of all indicated objects when used against a V0 partition or a pre-firmware-7.7.0 partition.

The same command, when used against a V1 partition, invokes cloning for the SMK, and then silently invokes SKS to complete the copying of indicated keys and objects, once the SMK is in place on the destination partition.

Either way, your keys and objects remain protected by the HSM's security perimeter. Externally stored keys (in the form of encrypted blobs) cannot be decrypted or used until they are brought back inside the cryptographic module.

Tamper Protection

Physical Security

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.

Luna Network HSM 7

The Luna Network HSM 7 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 card 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.

Luna PCIe HSM 7

The Luna PCIe HSM 7, or cryptographic module, is a multi-chip standalone module as defined by FIPS PUB 140–2 section 4.5. This means that:

- The module is enclosed in a strong enclosure that provides tamper-evidence. Any tampering that might compromise the module's security is detectable by visual inspection of the physical integrity of the module. In addition, any attempts to physically tamper with the token would likely result in the destruction of its circuitry and components, thus ensuring that your keys and sensitive objects are safe from an attacker.
- The module's physical design also resists visual inspection of the device design, physical probing of the device and attempts to access sensitive data on individual components of the device.

If an attacker with unlimited resources were to simply steal the module, 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 iKeys (multifactor quorum-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.

Luna USB HSM 7

The Luna USB HSM 7 is a multi-chip standalone module as defined by FIPS PUB 140-2 section 4.5, like the Luna PCIe HSM 7 described above, and provides the same physical tamper resistance measures. The Luna USB HSM 7 contains HSM hardware in a sealed, tamper-resistant enclosure, and all keys are stored encrypted within the hardware, inaccessible without the proper credentials (password or iKey).

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 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 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

All of the above security features are built into the HSM product, and they do present strong barriers to attackers. It is important that your own organization's security mandates, processes, and procedures avoid compromising that protection. It is all very well to have protection against external and opportunist attackers. But it is also necessary to ensure consistent proper handling by your own staff, over the long term.

Procedural checks and balances, with oversight, are important.

It is your responsibility to protect passwords and/or iKeys 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.

As a best practice, engage in role/responsibility separation as much as possible (the HSM interfaces encourage this), but if your model puts all administrative functions in the hands of one person, at least be aware of how much power that gives them over the content and the use and the availability of your important keys and objects, and have contingencies in place to address the possibility of that person ever becoming compromised in any way.

For example, when the HSM SO creates an application partition, the eventual owner of that partition should change passwords (including hardware authentication tokens, like iKeys for multifactor quorum) for themselves [partition SO] and others [User or Crypto Officer, Limited Crypto officer, Crypto User] as applicable. The HSM SO can still delete the partition, but has no visibility or entry into it.

Password authentication for roles and cloning/security domains are only as secure as any text string can be made secure.

Multifactor Quorum authentication for roles and cloning/security domains are generally much more secure (and used to protect the highest value keys and objects), because you can exert procedural control over the physical portion of the authentication secrets, such as lockups, sign-outs/sign-ins, audits, etc.

Certification

The Thales website provides more information about the certifications, compliance, and validation progress for each of the Luna HSM variants:

https://cpl.thalesgroup.com/encryption/hardware-security-modules/general-purpose-hsms

FIPS

At any given time, a FIPS-validated version of the HSM firmware 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.

Common Criteria

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

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

Handling and best practices

All of the above security features are built into the HSM product, and they do present strong barriers to attackers.

It is up to you to avoid practices that devalue or circumvent the security features.

Common Criteria/eIDAS Compliance

Luna HSMs regularly qualify against relevant standards that are important in the information security, data protection, and transaction protection spaces, and for which a business case supports the resource expenditure. Validation is repeated/updated when product changes warrant doing so, according to the respective standards and the requirements of the qualified testing laboratories.. HSM validations are reacquired when major new versions of applicable standards are released, and are also kept up with minor submissions and adjustments when a standard is tweaked or when interpretations shift on the part of testing/validation laboratories.

Under Common Criteria, Thales has qualified our Luna HSM products against eIDAS standards relevant to general purpose hardware security modules (also known as the cryptographic module).

Luna HSMs are eIDAS certified as Qualified Signature Creation Devices and Qualified Seal Creation Devices (QSCD), and are used by Qualified Trust Service Providers (QTSP) in the role of their root of trust.

See https://cpl.thalesgroup.com/compliance/eidas and https://cpl.thalesgroup.com/compliance/americas/fips-140-2

CC takes the view that a solution is validated for a purpose, which generally means that a number of moving parts are considered in concert. Thus an HSM is evaluated as an element of an overall solution that also includes software products, procedures, and systems all interacting. The following documents provide expanded detail on the relevant topics.

DOW0006186 (KB0023049) is "Thales Luna K7(+) Cryptographic Module COMMON CRITERIA USER GUIDANCE - PART 1: PREPARATIVE PROCEDURES"

DOW0006187 (KB0023050) is "Thales Luna K7(+) Cryptographic Module COMMON CRITERIA USER GUIDANCE - PART 2: OPERATIONAL GUIDANCE"

DOW0006188 (KB0023051) is "Thales Luna K7(+) Cryptographic Module COMMON CRITERIA USER GUIDANCE - PART 3: EIDAS GUIDANCE"

DOW0006189 (KB0023052) is "Thales Luna K7(+) Cryptographic Module COMMON CRITERIA USER GUIDANCE - PART 4 TOE INTEGRATION FOR USE IN COMPOSITE EVALUATION"

The K7 module referred to, in those document titles,

- is the heart of the Luna Network HSM 7 (Luna Network HSM appliance) and
- is also available in a separate PCIe card format for insertion in a host system (Luna PCIe HSM).

Roles	Principal Duties
HSM Security Officer (HSM SO) [Admin Partition Role]	The HSM SO is responsible for managing the HSM (cryptographic module). As such, they are authorized to install and configure the HSM, set and maintain global HSM security policies. They are also able to request the load of new HSM firmware update files (FUF), new Configuration Update Files (CUF) and new Functional Modules (FM). The HSM SO is able to create and delete partitions, but is not authorized to generate, load or use keys stored on the user partitions that have been created. The HSM SO is able to create, manage and use keys created in the Admin Partition along with being responsible for initializing the 'Administrator role'. The HSM SO can reset the Administrator password (configuration dependent). The HSM can have only one HSM SO.
[Admin Partition Role]	The Administrator is authorized to create, use, transfer and destroy key objects contained in the Admin partition. This role has privileges that are a subset of the HSM SO role. The Admin partition is for internal use; it is not intended, nor supported, for use as an application partition.
Partition Security Officer (Partition SO) [User Partition Role]	The Partition SO creates the partition level Partition CO role, activates partition, sets and changes partition-level policies, with an option to reset the Partition CO password (configuration dependent).
Partition Crypto Officer (Partition CO) [User Partition Role]	The Partition CO role is authorized to create, use, destroy and transfer key objects for a given partition. The Partition CO can optionally create the Partition LCO and Partition CU, and perform initial assignment of key authorization data.
Partition Limited Crypto Officer (Partition LCO) [User Partition Role]	The Partition LCO is an optional partition role authorized to create and use key objects, and perform initial assignment of key authorization data. The role is only permitted to delete key objects where per-key authorization is used and the correct authorization data for a given key object can be presented to the cryptographic module.
Partition Crypto User (Partition CU) [User Partition Role]	The Partition CU is the partition role authorized to use the key objects within the partition (e.g. sign, encrypt/decrypt).
Audit User [Admin Partition Role]	The Audit User initializes the secret key used to generate Message Authentication Code (MAC) for secure audit messages alongside configuring logging levels for the HSM.

Roles	Principal Duties
Key Owner [Admin or User Partition Role]	Implicit role used to authenticate the owner of a key through verification of the related key authorization data.
STC User [Admin or User Partition Role]	The STC user is optional role used with a remote Thales Luna client to initiate a secure tunnel with a target partition. Once successfully authenticated based on pre-registered authentication credentials, the STC user is able to submit commands to the target partition over a trusted channel.

CC-EIDAS site certification

Visit this link:

Site certification

After the table loads, use the search box to search for "Thales".

CHAPTER 3: Redundancy and Reliability

Luna HSM partitions can be configured in high-availability groups for redundancy and reliability.

High-Availability Groups

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

Objects (session or token) are replicated immediately to all members in an HA group when they are generated in the virtual HA slot. Similarly, deletion of objects (session or token) from the virtual HA slot is immediately replicated across all group members. Therefore, 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.

NOTE If you are using Luna HSM Client 10.4.0 or newer and are setting up an HA group with a mix of FIPS and non-FIPS partitions as members, objects will not replicate across all HSMs in the group in the following cases:

> If you have set a non-FIPS primary, a FIPS secondary, and created a non-FIPS approved key on the group, the key will not replicate to the FIPS secondary. No error is returned when this occurs.

> If you synchronize group members with the **hagroup synchronize** LunaCM command, any non-FIPS keys will fail to replicate to the FIPS member(s). An error is returned when this occurs, but lunaCM synchronizes everything else.

NOTE If your application bypasses the virtual slot and creates or deletes directly in a physical member slot, the action occurs only in that single physical slot, and can be overturned by the next synchronization operation. For this reason we generally advise to enable HA-only, unless you have specific reason to access individual physical slots, and are prepared (in your application) to perform the necessary housekeeping.

Key replication, for pre-firmware-7.7.0 HSM partitions and for V0 partitions, uses the Luna cloning protocol, which provides mutual authentication, confidentiality, and integrity for each object that is copied from one partition to another. Therefore, *prior to Luna HSM Firmware 7.8.0*, all HA group member partitions must be initialized with the same cloning domain.

Key replication, for Luna HSM Firmware 7.8.0 (and newer) HSM partitions and for V0 partitions, and Luna HSM Client 10.5.0 (and newer), becomes more versatile with Extended Domain Management, as each member partition can have as many as three cloning/security domains. It becomes possible to easily mix password-authenticated and multi-factor (PED) authenticated partitions in HA groups. Any member must have at least one of its domains in common with the current primary member. [For reasons of redundancy and overlap, we recommend that you *not* create (say) a 4-member group where the primary has domains A, B, C, and the three secondary members include one member with domain A, one member with domain B, and one member with domain C, where no other domains belong to the group -- such a group could function only until the primary failed/went-offline, at which point the next primary would have no domain peers with which to synchronize. Therefore, consider redundancy overlap when using Extended Domain Management with HA group members.

Key replication for V1 partitions uses the Luna cloning protocol to ensure that all HA group members have the same SMK, and uses SKS to export a key originating at one member and to import and decrypt that key (using the common SMK) on each other member in the group. Again, all HA group member partitions must be initialized with the same cloning domain in order that the common SMK can be available on every member.

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.

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.

CHAPTER 4: Authentication

Each Luna HSM comes in one of two authentication types – password or multifactor quorum (also called PED-authenticated). PED stands for PIN Entry Device. The authentication type for Luna Network HSM 7 and Luna PCIe HSM 7 is configured at the factory and cannot be modified in the field. Luna USB HSM 7 can be initialized to use one or the other.

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

Table 1: Authentication Types

Password Authentication	Multifactor Quorum Authentication (iKeys/Luna PED)
Two-factor authentication is not available; relies on "something you know".	Two-factor authentication consisting of a physical iKey and optional PIN; 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.
Access to cryptographic keys is restricted to knowledge of partition CO (read/write) or CU (read-only) password.	Access to cryptographic keys is restricted to CO (read/write) and CU (read only); possession of appropriate iKey(s) and PIN 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 iKeys, 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 depend on password knowledge only.	Key-custodian responsibility and role separation depend on iKey(s) ownership; physical possession and PIN knowledge.

Password Authentication

For Luna HSMs using password authentication, the various, layered roles are protected by passwords. Refer to "User Access Control" on page 31 for descriptions of specific HSM roles and their responsibilities.

Authentication

Objects on the HSM are encrypted by the owner of each application partition, and can be decrypted and accessed only by means of the specific secret (password) associated with the Crypto Officer or Crypto User.

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 role.

Advantages

Using password 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 multifactor quorum authentication, and thus have the following disadvantages:

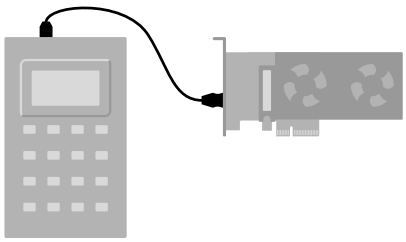
- Vulnerability to observation: passwords being typed can be easily observed in person, through a camera, or with malware like keystroke loggers
- Record-keeping: secure passwords are obscure and must be written, with its record securely stored
- Accountability: it is difficult to know who might have seen or been told a password

Multifactor Quorum Authentication

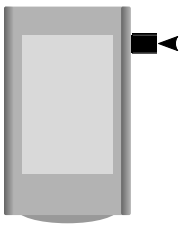
For Luna HSMs configured for multifactor quorum authentication, the various, layered HSM roles are protected by cryptographic secrets stored on physical USB iKeys, each of which may be assigned a memorized PIN, presented to the HSM using the Luna PED (PIN Entry Device). The connection between the Luna PED and the Luna HSM is a secure, trusted path. Refer to "User Access Control" on page 31 for descriptions of specific roles and their responsibilities.

- For the Luna Network HSM 7, the PED connection is on the appliance rear panel.

- For the Luna PCIe HSM 7, 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 the Luna USB HSM 7, the Luna PED is not required. iKeys are presented directly to the HSM via the USB-C connector and an adapter, and PINs are entered using the built-in touchscreen. You can also authenticate roles on the Luna USB HSM 7 using a Remote Luna PED connection.



For Local PED, the connection is a secure physical link, directly to the HSM, bypassing the computer memory and bus. At no time does an authentication secret exist in the clear, anywhere in computer memory or on any computer bus.

Remote Luna PED

By default, Luna PED is connected directly to the HSM via a USB cable. When it is not convenient to be physically near the host or client computer, Remote Luna PED allows you to operate the HSM remotely and securely.

The multifactor quorum-authenticated Luna HSM generates a unique Remote PED Vector and saves it on one or more orange iKeys. You can generate or regenerate this secret at any stage of your HSM deployment. If the HSM is not yet initialized, you can generate the RPV remotely using a one-time password. If the HSM is already initialized, the HSM SO must log in and generate the RPV using a locally-connected Luna PED. The RPV is used to authenticate the Remote PED server (a client computer with a Luna PED connected) for all future HSM role authentication processes, and the HSM itself can be located at a secure facility for its entire deployment.

Partition Activation and Challenge Secrets

Once initialized, a multifactor quorum-authenticated application partition can be configured to accept a password string, known as a challenge secret, as a secondary form of authentication. This is referred to as partition activation. For some use cases, such as key vaulting, the requirement to present a physical key to access objects on the partition may be desired. For most application use cases, however, requiring a physical key each time the application accesses the partition is impractical.

Activation allows the Crypto Officer or Crypto User iKey secrets to be cached, and for those users to authenticate their roles from then on using the secondary challenge secret. Activation is allowed or disallowed by the setting of partition policies by the Partition Security Officer (PO). The PO role cannot be activated; the PO must always log in using a physical iKey.

Advantages

Using multifactor quorum 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 (iKeys) can be tracked and controlled
- Duplication restrictions: duplication and promulgation can be prevented by physical security measures
- Physical device: using the Luna PED or Luna USB HSM 7 touchscreen to input passwords and PINs prevents key-logging exploits that typed passwords are vulnerable to

Disadvantages

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

CHAPTER 5: 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 client system, 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 Luna USB HSM 7 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:

HSM/Crypto-Module-Level Roles

HSM roles are responsible for administration, configuration, and auditing of the cryptographic module . HSM-level roles cannot perform cryptographic operations on the application partition.

Table 1: HSM Roles

HSM Security Officer (SO) **PED Key: Blue**	- Initializes the HSM, creating the SO credential - Creates/deletes the application partition - Configures global HSM policies - Performs updates of the HSM firmware
Auditor (AU) **PED Key: White**	- Manages HSM audit logging

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.

Table 2: Partition Roles

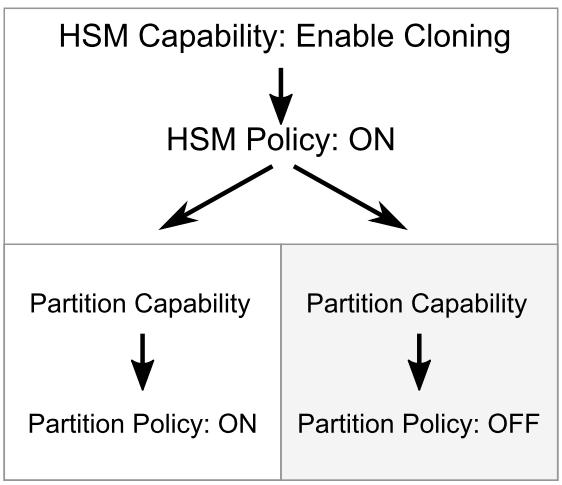
Partition Security Officer (PO) **PED Key: Blue**	- Initializes the partition, creating the PO credential and setting the cloning domain - Initializes the Crypto Officer role and can reset the CO credential (if permitted by HSM policy) - Configures partition policies

Crypto Officer (CO) **PED Key: Black**	> Creates and modifies cryptographic objects on the partition > Manages backup and restore operations for the partition > Performs cryptographic functions via user applications > Initializes the Crypto User role and can reset the CU credential
Crypto User (CU) **PED Key: Gray**	> Performs cryptographic functions via user applications (optional read-only role) > Can create public objects only > Can perform backup/restore of public objects on the partition

CHAPTER 6: 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 Luna HSM.

Figure 1: 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 Security Officer 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 changehsmpolicy 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.

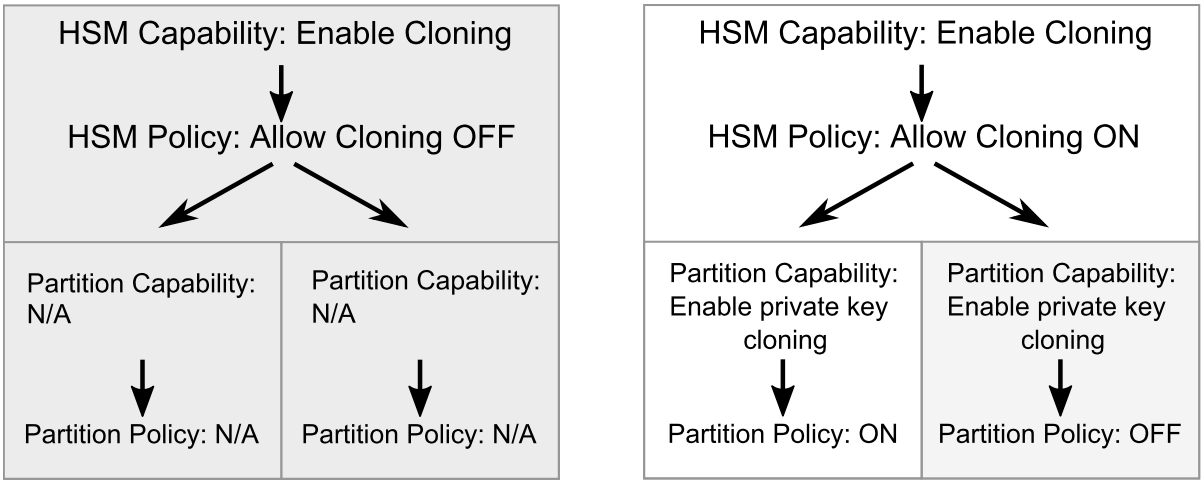
Example: Cloning

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 2: 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 be set to enable it or not.

CHAPTER 7: Flexible Backups

While some applications might deal in ephemeral objects that are erased after their use, in many 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.

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 Luna Backup HSM 7 or Luna Backup HSM G5 can be connected to the Luna HSM Client 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 multifactor quorum-authenticated Backup HSM when backing up a multifactor quorum-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 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" below

> "Remote Backup" on the next page

> "Comparing Local Versus Remote Backup" on the next page

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.

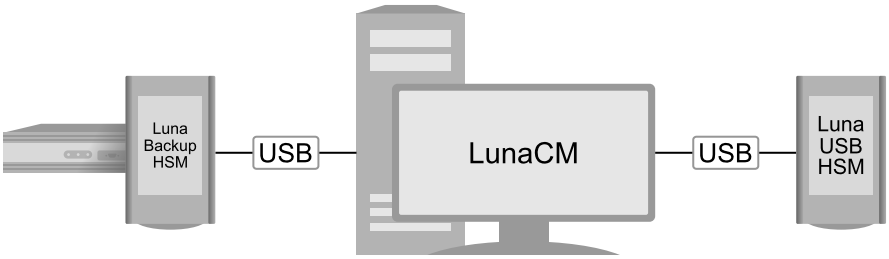
Local Backup

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.

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 3: Client-side Local Backup

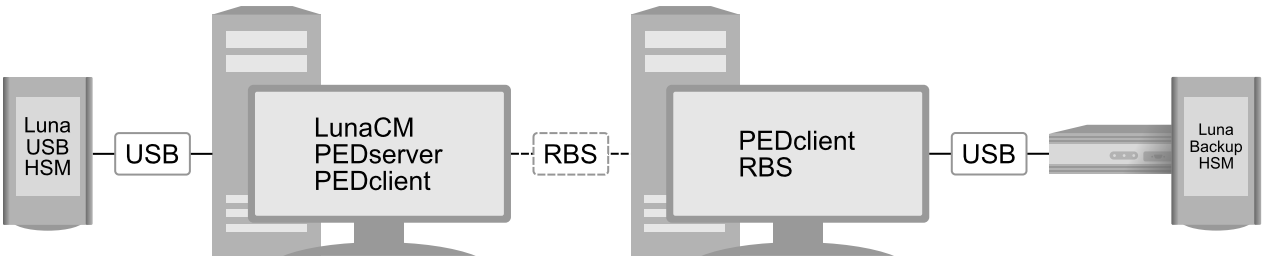


The backup operation in this case is still local, and thus requires a direct wired connection between your Backup HSM and client workstation. This method is highly secure, and allows for some flexibility in case the HSM you wish to back up is not easily available for direct connection. A PC running Luna 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" below outlines the basic setup required for remote backup.

Figure 4: Remote Backup



Remote Backup Service (RBS) runs on a system hosting a 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 Partition Backup and Restore.

CHAPTER 8: Logging and Reporting

Luna USB HSM 7 allows you to track and report all activity on your HSM to encourage responsibility, ensure accountability, and maintain tight security.

Logging can be done at two levels

> the cryptographic module

> the host system that contains the crypto module.

Luna HSMs come equipped with HSM-level (that is, cryptographic module level) audit logging via the **Audit** HSM role. See "HSM-Level Audit Logging" below.

For Luna USB HSM 7 it is your responsibility to manage audit log intensity, disk-space consumption,

HSM-Level Audit Logging

Monitoring HSM activity is essential to maintaining a high level of security for the highly sensitive material on your HSM. 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, when configured, sends HSM log event records to a remote logging server, with cryptographic safeguards ensuring verifiability, continuity, and reliability of HSM event log files. Log records can also be accumulated to tar files for alternative handling, and to ensure that limited storage inside the cryptographic module is not filled.

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 iKey for multifactor quorum-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.

Best Practices HSMs, Partitions, Clients

HSMs are really good for securing and using cryptographic material and sensitive data, and they provide the means to securely access their contents and operations (key generation, key storage, cryptographic processing), and they provide the means to implement secure practices. But to be useful, an HSM must be accessed and used; therefore, the material you are protecting can only be as secure as allowed by your practices surrounding the HSM. Here are some overall best practices for securely using Luna HSMs.

Hardware Inventory

Perhaps too obviously, it is expected that you would maintain an inventory of your cryptographic modules (HSMs), as you would for any other important equipment and assets, including

- model and type
  - standalone or appliance
  - embedded,
  - in-service live or backup, etc., and
  - serial number
- the hostname and HSM label, or other names you assigned to each HSM
- membership, if applicable, in an HA group or groups
- physical location (geographical, rack and shelf within your data center, etc.)
- asset-tracking badge or similar identifier.

Credential Inventory

Specific to the nature and purpose of HSMs, the owner and location of each credential related to the HSM must be recorded in a document that the relevant people can find, when needed:

- for ongoing operation and personnel changes,
- for mandated credential updating/cycling (example, 'password' expiry and rollover),
- for disaster recovery.

The actual credentials are to be stored securely and separately. Physical keys should never be kept where a potential attacker could retrieve them, and text/character passwords should be kept on paper in a controlled-access safe or encrypted in a secure password manager.

A user who rarely accesses a credential, or a backup person, might need to retrieve a password or physical key, so they need to retrieve from the physical safe or from the password manager, and the location of that 'vault' or repository must be knowable as part of their duties. The list should say where the credential storage resides, and who has access to the credential storage safe(s) and must be present to open such a secure-storage lockup.

For personnel who have access to a safe storage containing

- the written passwords for Password-authenticated HSMs

  or

> the iKeys (iKey for multifactor quorum-authenticated HSMs, as well as secondary typed character authentications, including passwords, PED Pins, etc.

...you want to minimize the exposure of such access. But for highest security it should require two or more persons present, which implies a form of split-knowledge secret for credentials (like the MofN option for physical iKeys (PED Keys), or for text-string passwords, some scheme where each of two or more persons knows only a portion of a complete password.

This, in turn, implies that there would be *spare* empowered persons in case of absences for illness, business travel, vacation, extreme weather, etc., such that you can always achieve quorum when needed.

Here (table below) is an example summary, as a starting point; it would be readily accessible by persons who might need it in the performance of their duties.

*The secrets themselves are **never stored** in such a document*, only the *who* and the *where* for retrieving them, in case of need.

Function, role, or credential	**Name (the title or label assigned to a protected container or to a scope of responsibility)**	**Owner [person(s) and/or their title] currently controlling the text string or iKey (s) protecting the role**	**Safekeeping location of access credentials (physically, or on your network, where to go in case of loss or destruction of primary credentials)**
HSM Security Officer			
Partition 1 Security Officer			
Partition 1 primary Cloning Domain			
Partition 1 Crypto Officer			
Partition 1 Crypto User			
Audit User (HSM/crypto module role)			
Audit Domain			
Backup HSM Security Officer			
Backup Partition Crypto Officer			
Backup Partition Domain			

Roles, credentials, and areas of responsibility

HSM Security Officer

The HSM SO handles all the administrative and configuration tasks at the HSM level, including :

- Initializing the HSM and setting the SO credential.
- Setting and Changing global HSM policies.
- Creating/deleting the application partition(s).
- Updating the HSM firmware.

The HSM SO credential is a password string in A-Series HSMs (Password authenticated), or a Blue iKey (PED Key) in S-Series HSMs (Multifactor-Quorum authenticated). As this is the admin of the cryptographic module (HSM), this credential has considerable power(*) among all of the roles. If attempted access fails for three (3) consecutive HSM SO login attempts,

- application partitions are destroyed,
- the entire cryptographic module (HSM) is zeroized and
- all of its contents are rendered unrecoverable.

The number is not adjustable. As soon as the HSM SO role is successfully authenticated (logged in), the bad login counter is reset to zero. Other roles have their own rules, as follows.

(* The HSM SO has the maximum *administrative* power over the cryptographic module, but has *no access to the contents* of application partitions within the crypto module (HSM). This separation of roles is inherent in the security regime underlying the Luna HSM; however, if you do not require such separation in your operations, simply set up your operational procedures to allow one person to control the access credentials for all roles on an HSM. The behavior of the cryptographic module/HSM is governed by HSM configuration settings: some of those are fixed for the module version you have purchased, while some have merely default values that you can modify with policy settings. See HSM Capabilities and Policies.)

Partition Security Officer

The Partition SO handles all administrative and configuration tasks in the application partition, a functional logical subdivision of the overall cryptographic module, including:

- Initializing the partition, setting the PO credential, and setting a cloning domain secret for the partition.
- Configuring partition policies**.
- Initializing the Crypto Officer role.
- Activating the partition (only for Multifactor Quorum authenticated)

This credential is similar to the HSM SO but it applies only to an individual application partition, and not to other aspects of the cryptographic module (HSM). The Partition SO credential is a password string in A Series HSMs (Password authenticated), or a Blue iKey (PED Key) in S Series HSMs (Multifactor-Quorum authenticated). If attempted access fails for ten (10) consecutive Partition SO login attempts, the partition is zeroized and all cryptographic objects are destroyed. The Partition SO must re-initialize the partition and a Crypto Officer role, who can restore key material from a backup device.

The Partition SO has administrative oversight for the partition, but cannot see or access partition contents. It is up to the partition's Crypto Officer to create, use, move/clone, and delete partition objects. See below.

(** Partition-level capabilities and policies are mostly inherited from related crypto-module/HSM-level capabilities and policies, and as with the HSM-level, some settings at the partition level are fixed and some merely have a default value that can be modified by policy setting configuration. See Partition Capabilities and Policies.)

Partition Crypto Officer

The Crypto Officer is the primary *user* of the application partition and the cryptographic objects stored on it. The Crypto Officer has the following responsibilities:

- Creating, deleting, and modifying cryptographic objects via user applications.
- Performing cryptographic operations via user applications.
- Managing backup and restore operations for partition objects.
- Creating and configuring HA groups.
- Initializing the Crypto User role.
- The CO can modify keys - in PKA schemes, must provide per-key authorisation (PKA) data for unassigned keys.
- The CO can unblock blocked (due to per-key authentication failures) PKA keys.
- The CO can increment usage counters and set or change the limit.
- The CO can perform rollover of the **S**calable Key Storage **M**asking **K**ey (the SMK).
- If attempted access fails for ten consecutive Crypto Officer login attempts, the CO and CU roles are locked out. The default lockout threshold of 10 is governed by Max failed user logins allowed, and the Partition SO can set this threshold lower if desired (see **Partition** Capabilities and Policies). Recovery depends on the setting of **HSM** policy SO can reset partition PIN, as follows:
  - If HSM policy 15 is set to 1 (enabled), the CO and CU roles are contingently locked out by too many consecutive failed login attempts. The lockout does not have a timed expiry, but it can be ended by the Partition SO who must unlock the CO role and reset the credential (Resetting the Crypto Officer, Limited Crypto Officer, or Crypto User Credential).
  - If HSM policy 15 is set to 0 (disabled), the CO and CU roles are permanently locked out and the partition contents are no longer accessible. The Partition SO must re-initialize the partition and the Crypto Officer role, who can then restore key material from a backup. This is the default setting.

Crypto User

The Crypto User is an optional role that can perform cryptographic operations using partition objects in a read-only capacity, but can create only public objects. This role is useful in providing limited access; the Crypto Officer is the only role that can make significant changes to the contents of the partition, while the Crypto User has the following capabilities:

- Performing operations like encrypt/decrypt and sign/verify using objects already on the partition
- Creating and backing up public objects (see Partition Backup and Restore)
- The CU can increment usage counters but, unlike CO, cannot change/set the limit
- If attempted access fails for ten consecutive Crypto User login attempts, the CU role is locked out. The default lockout threshold of 10 is governed by Max failed user logins allowed, and the Partition SO can set this threshold lower if desired (see **Partition** Capabilities and Policies). The CO must unlock the CU role and reset the credential (see Resetting the Crypto Officer, Limited Crypto Officer, or Crypto User Credential).

Partition Cloning Domain

A security domain or cloning domain secret is a layer of encryption that is created, during initialization, on a cryptographic module (HSM) or HSM partition that you control. The domain determines whether a cryptographic object can leave the HSM, and where it can go if it is allowed to leave.

Cloning is a secure-copy operation by which sensitive HSM objects are copied, while strongly encrypted, from oneThalesHSM. to another ThalesHSM. The security domain, or cloning domain, is a special-purpose secret that is attached to a partition on an HSM. It determines to which, and from which, other partitions (on the same HSM or on other HSMs) the current partition can clone objects. Partitions that send or receive partition objects by means of the cloning protocol must share identical cloning domain secrets.

Cloning domain is set generally when the partition is initialized and often forgotten about for years until there is a need to clone the data (restoring, migrating to a newer-generation HSM, etc.). It is very strongly recommended to make sure that the domain is stored securely and well documented so that it can be used in the future without any issues. The domain is a typed text/character secret in A series HSMs and a Red iKey (PED Key) in S series HSMs. There is no way to verify a domain other than by trying a cloning or backup procedure. Note that Luna Client-mediated High Availability (HA) uses key/object cloning as the core of the feature. See High-Availability Groups.

Domains, plural

Prior to Luna HSM version 7.8.0, only one domain could exist and be used on a partition, and objects were not allowed to move from one domain to another.

From firmware version 7.8.0 onward the historic capability is expanded (see Allow Extended Domain Management), while retaining integration with existing applications, by optionally allowing the existence of up to 2 additional domains in a partition. This permits

- migrating keys between Password based and Multifactor Quorum (PED) authenticated HSMs (this includes Luna Cloud HSM)
- changing or rolling-over of partition domains
  - in case of compromise,

    or
  - when mandated by an organization's security rules.

Recommendation for Multifactor Quorum (PED) authenticated HSM

It is generally recommended to use MofN for credentials. For example 2 out of 3: Where at least any two people out of three are required at the same time to login to the HSM.

It is also recommended to create duplicate PED keys for every role, in case of loss or damage, so this includes full duplicate sets where MofN has been invoked.

You can keep a duplicate set of iKey (PED Key) credentials in secure lockup, on premises for local recovery needs, but it is also strongly recommended to have copies of those credentials protected in secure off-site storage for purposes of disaster recovery.

> **NOTE** Although the iKey secrets can be split as many as 16 ways, it is recommended to make only as many splits (n) and require only as many 'members' for quorum (m) as necessary - with sufficient spares for absent key holders - because more splits means more operations with the PED, when there might be time limitations, and larger quorum requirements impose increasing demands on personnel and planning, to ensure that enough secret-split (iKey) holders can be available whenever needed.

HA Recommendations

Luna HSMs provide scalability and redundancy for critical cryptographic applications. For applications that require continuous, uninterruptible uptime, the Luna HSM Client allows you to combine application partitions on multiple HSMs into a single logical High-Availability (HA) group, where members can optionally be geographically distanced to ensure disaster resistance. See High-Availability Groups.

Following are points to take into account while setting up HA:

- All HSMs in an HA group must have the same firmware versions. [see NOTE below]
- Member partitions must have a common cloning domain and same Crypto Officer password, in order to function in a client-mediated HA group.
- It is recommended that all the HSMs in an HA group have same policy settings.[see NOTE below]
- HA should be setup for auto-recovery. Using the value as '-1' sets the auto-recovery retries to infinite. The interval between each try can be configured between 60 and 1200 seconds.
- The recovery mode defaults to activeBasic but should be changed to ActiveEnhanced. ActiveEnhanced mode sets an auto reconnect logic in the HA that helps to recover the session on its own in case of a network failure.
- If physical slots are not required to be used directly by any application, it is always recommended to setup HAOnly as that defaults the HA virtual slot to 0 and hides the physical slots. If it is not set, then
  - the list of all slots is visible, and changes made directly to a physical slot, rather than via the virtual slot cause the HA group to be out-of sync, defeating the advantages of HA and potentially causing trouble with applications
  - in case of a failure of one of the members, then without HAOnly, the slot number of the HA virtual slot can change. This can cause applications to direct operations to a wrong slot. When HAOnly is enabled, the slot numbers do not change as a member is dropped or added.
- In case of a member getting dropped for more than a day, it is recommended to manually sync the HA once the member is back into the group to ensure inclusion of all the objects added to the group while the member was not present.

> **NOTE** Allowing member HSMs to have different policies or different firmware could result in some member partitions rejecting some keys (or key sizes, or curve variants, etc.), or some operations, as unsupported or forbidden, while other members would attempt to accept and perform such operations, but HA function of the group would be compromised.
>
> The only situation where HA group members might be expected to have different firmware or settings is during a brief upgrade or migration interval, where all group members are expected to settle into the new conformation in short order.

Recommended configuration for HA

HA auto-recovery in activeEnhanced mode is strongly recommended

When auto-recovery is enabled, Luna HSM Client performs periodic recovery attempts when it detects a member failure. To enable auto-recovery on an HA group, see hagroup retry. For most implementations of Luna HA, we recommend HA auto-recovery with mode set to active-enhanced see hagroup recoverymode. In other words, in the absence of a good reason to avoid those configuration settings, use them.

HAOnly is strongly recommended

Object management of an HA group is performed by the client that builds/owns the group, only with operations that are sent *via the HA virtual slot number* owned by that specific client. In other words, **do** use just the virtual slot for all operations and **do** use the hagroup haonly setting to make the individual member slots invisible, thus removing any temptation for anyone to make direct changes to individual members, bypassing the scope and control of the virtual slot, and potentially crippling HA synchronization and auto-recovery.

If your use-case demands that you directly address individual members of an HA group, be aware that objects created or deleted in that fashion are not 'known' to the HA virtual slot, and therefore are not replicated to other slots during HA synchronization; you would have to perform any replication between members manually (or via your own application) for any objects not created or deleted via the HA virtual slot. In such a use case, you might consider creating your own HA functionality, in which case see High Availability Indirect Login.

Representative Scenario

Consider an installation where you might have, say, HSMs and clients in one datacenter (A) and HSMs and clients in another datacenter (B), with connections and HA grouping both within and between the two datacenters, as you might do to spread out and minimize disaster risk. So one client has connections to members of its own HA group that reside in the local datacenter with the client, and to other members of its own HA group that reside in the other datacenter. And the reverse for a client in the other datacenter, having members in both places.

So if an object is deleted or created or modified by an application configured to use the HA virtual slot with client "A", and that client loses connectivity to all but at least one HA group member, that operation will get replicated to the other HA members in the other datacenter as those members are re-introduced into the group by client "A". And vice versa for HA clients in the second datacenter with members in the first datacenter.

When connectivity between datacenters is re-established, the client(s) from each datacenter synchronizes only the operations sent by each respective client to the other members of its own HA group.

Synchronization in a group propagates only changes made by the group's own client; the sync operation does not compare the entire contents of each HA member partition when that member is reintroduced. To put that another way, HA is not expecting changes that were made by other means than the HA virtual slot.

So if the HA virtual slot on client A deletes some objects, creates some objects, modifies some objects, only those operations get replicated to the 'physical' member partitions located on the HSMs in the other datacenter. For HA auto-recovery, the Client A does not directly compare the *entire* contents of an HSM partition HA member in one datacenter with the contents of its respective HA group members in the other datacenter. It replicates only operations that were sent to its own 'client A' HA slot. If a 'physical' partition was also modified as a member of another HA group, or if a partition was addressed directly and modified by an application, without using the HA virtual slot to do it, then those changes are not noticed by the current Client overseeing its own HA group.

In the case of directly addressing individual member slots (again, *not* recommended unless you absolutely must), you must be diligent about cleaning up after all such operations, else the affected partitions can become cluttered, potentially slowing or disrupting HA operation.

If working outside the recommendations...

If auto-recovery was not enabled and set to active enhanced, or if connectivity was re-established outside any HA recovery attempts that may have been configured on the client, then the HA synch command must be manually executed.

Manually executing an HA synchronization from a client, then compares the contents of each partition that is a member of the HA group based on handle IDs of objects.

- Manual sync adds objects to a partition only if it determines those objects are missing.
- Manual sync does not delete objects, nor does it synch changes to objects (such as changes made to any attributes of an object).
- Therefore, manually delete objects from a partition that you don't want replicated to other HA group members, and do that *before* manually synchronizing.

Summing up

The best-practice recommendation when configuring and managing HA groups is to enable HA auto-recovery in activeEnhanced mode for almost any active production scenario.

By contrast, a *manual synchronization* is ***not recommended*** in an active production scenario, as that could potentially cause a race condition.

HSM & Partition Policies

HSM Capabilities are features of HSM functionality, set at time of manufacture, based on the HSM model you selected at time of purchase. You can add new capabilities to the HSM by purchasing and applying capability licenses from Thales. Some capabilities (whether original or added via license update) have corresponding modifiable HSM policies.

HSM Policies are configurable settings that allow the HSM Security Officer to modify the function of their corresponding capabilities. Some policies affect HSM-wide functionality, and others allow further customization of individual partitions by the Partition Security Officer.

Some policies affect the security of the HSM. As a security measure, changing those security-affecting policies results in application partitions, or the entire HSM, being zeroized. Such policies are called Destructive policies.

> **CAUTION!** If your HSM, or a partition of it, contains important keys or data, you should always have a backup of your sensitive or important material before making policy changes.

Here are recommendations for setting up the policies that are most commonly used:

1. Set the destructive policies at the time of initialization in order to avoid the process of rebuilding or restoring the key material if you make the change later.
2. The policy associated with the HSM-level capability **15 : Enable SO reset of partition PIN** is set to OFF by default. Change the "SO can reset partition PIN" policy to ON at the time of initialization so that the SO can recover the Crypto Officer password in case of a lockout. If the policy is set to OFF, the entire partition has to be rebuilt in case of a lockout.

3. The policy associated with the HSM-level capability **12 : Enable non-FIPS algorithms** is set to ON by default. Turn the "Allow non-FIPS algorithms" policy OFF for the HSM to operate in FIPS 140 approved configuration. The policy is destructive, hence the HSM must be reinitialized after setting this policy.
4. The policy associated with the HSM-level capability **21: Enable forcing user PIN change**" is set to ON by default.
   - For credentials created by partition SO, when the policy is ON, the Crypto Officer password must be changed by the CO before being able to use it - this forces initial separation between the .administrative and operational roles.
   - Turning the Force user PIN change after set/reset policy **OFF** allows the CO (Crypto Officer) to use the credential assigned by the Partition SO, on the assumption that your security regime doesn't demand that you maintain separation between the administrative and operational functions for your application.
5. The policy associated with the partition-level capability **22: Enable activation** is not valid for password-authenticated partitions, and affects Multifactor Quorum partitions.
   - When the policy set to 0 (zero, meaning OFF), it requires that black and/or gray PED Keys must be presented at each login via LunaCM or by a client application.
   - Set Allow activation to 1 (one, meaning ON) so that the iKey/PED Key secrets are encrypted and cached, and only a keyboard-entered challenge secret is required for login while the HSM remains powered.
6. The policy associated with the partition-level capability **23: Enable auto-activation** also affects Multifactor Quorum partitions.
   - Set the policy to 0 (zero, meaning OFF), to cause the partition to deactivate in the event of a power loss, such that the return to operation after power is restored requires presenting the black and/or gray iKeys (PED Keys).
   - Set Allow auto-activation to 1 (one, meaning ON) so that the ability to automatically resume partition activation (without presenting iKeys) is maintained through a power loss up to 2 hours in duration. Beyond two hours, the iKey data is uncached and the primary authentication must be presented again, to resume operation with your application.

Policies 22 and 23 are applicable only to Multifactor Quorum (PED) authenticated HSMs; activation is not applicable to password authentication.

HSM Backup

Following these recommendations when taking backups of HSMs:

1. In addition to having an online backup in other HSMs in HA, it is strongly recommended to have an offline backup in a Backup HSM, which helps in recovery from unexpected human errors or application errors.
2. The backup HSM should be stored in a secure safe.
3. Backup frequency should be in line with the frequency of keys being created by the application.
4. The name of the partition on the backup HSM should resemble the partition on the source and it is a good idea to add a date of the backup within the label itself.

Disaster Recovery

In case of an event that results in zeroization, follow these steps to restore the HSM to a working state:

1. Clear the tamper events, if any.

2. Locate the credentials and their owners for a successful restore, referring to your checklist similar to the table that was suggested earlier in this document.
3. Initialize the HSM using the HSM SO credentials. If necessary, use credentials retrieved from off-site storage.
4. Set the required HSM policies.
5. Create the partitions and initialize them using Partition SO credentials with the same cloning domain that was used while creating the original partitions.
6. Set the appropriate partition policies (Optional).
7. Restore the objects from either another member from the same HA group or from an offline backup.
8. Connect the application to the partition and restart the application.

Logging

Audit logs record important actions and events in the cryptographic module (HSM). You can decide the level of detail that needs to be logged.

Syslog on your host system records selected events occurring in the host computer, but does not capture events within the cryptographic module.

Compare and contrast the respective logging services at Comparing Syslog vs Audit log.

- Always configure the Audit role and audit logging. In a rigorous auditing regime, you would want to configure Audit before initializing the HSM SO, as this order ensures that the audit logs capture timestamped events from the beginning of HSM usage with no gaps in the record.
- As a best practice, keep your important logs safely on remote servers. Configure syslog remotehost add and audit remotehost add, ensuring that the receiving host and port configuration are not the same for both remote syslog and remote audit log.
- Use TLS encryption when sending logs to a remote repository, and ensure that the remote syslog host(s) is/are secure from physical or network intrusion.
- Host logs on your HSM host are stored as plain text (syslog). The physical security that you erect around the HSM's host should also protect the host logs from tampering.
- Establish log rotation schedules, balancing quantity/intensity of logging with frequency of rotation - the more detailed the logs you configure, the faster the storage space is used, therefore the more frequently you should rotate the logs out and ship them off to your remote repository.
- Log only as detailed as makes sense for your industry and the demands of your auditing agencies - very intensive audit logging can consume significant HSM resources and might slow cryptographic operations for your client applications.
- When you set up HSM audit logging, be sure to verify your procedures end-to-end such that you can access (decrypt) and verify the logs you are capturing - don't wait until the auditors arrive.