SafeNet HSM 6.2.4

CUSTOMER RELEASE NOTES

Issue Date: 05 May 2017

Document Part Number: 007-012225-010 Rev. A

The most up-to-date version of this document is at:

http://www.securedbysafenet.com/releasenotes/luna/crn_luna_hsm_6-2-4.pdf

Product Description

The SafeNet HSM (hardware security module) family provides FIPS-certified, PKCS#11-compliant cryptographic services in a high-performance, ultra-secure, and tamper-proof hardware package. By securing your cryptographic keys in hardware, SafeNet HSMs provide robust protection for your secure transactions, identities, and applications. They also offer high-performance encryption, decryption, authentication, and digital signing services.

SafeNet Network HSM

SafeNet Network HSM is a network-based, Ethernet-attached HSM appliance that offers high-availability configuration options, remote management PED and backup, and dual hot-swappable power supplies. SafeNet Network HSM provides cryptographic services for network clients that are authenticated and registered against HSM partitions. Two performance variants are available, the SafeNet Network HSM-1700 and SafeNet Network HSM-7000, which are capable of 1700 and 7000 (RSA 1024-bit) signings per second respectively.

Release Description

SafeNet HSM Release 6.2.4 is a mandatory patch update for release 6.2.3, that fixes some important issues. Release 6.2.4 must be installed immediately on any 6.2.3 SKS Network HSM and SKS Backup HSM, before you begin using the HSM.

- Firmware 6.25.1 must be manually installed on the SKS Backup HSM.
- Firmware 6.25.1 is installed automatically on the Network HSM when you install the HSM software.

SafeNet HSM Release 6.2.4 :

- is a field update of the 6.2.3 factory released SafeNet SKS Network HSM appliance and SKS Backup HSM, only
- does NOT include the SafeNet USB HSM or the SafeNet PCI-E HSM
- is a new Client software, Network HSM appliance software, and Appliance/Backup HSM firmware implementing the Scalable Key Storage feature
- Client software upgrade consists of a fresh installation following uninstall of the previous version.
- supports all features of release 6.2.2, except
  - Per-partition Security Officer (PPSO)
  - Host Trust Link (HTL -- deprecated feature)
  - NTLS Keys in Hardware
  - Small Form-Factor Backup (SFF)
  - Crypto Command Center (CCC)
- supports only PED-authenticated HSMs
- supports a maximum of one partition on the HSM

A Scalable Key Storage HSM can be identified by two entries in the lunashell **hsm displaylicenses** command output:

- Scalable key storage
- Enable network replication

An SKS HSM must be ordered from the factory. Non-SKS HSMs in the field cannot be upgraded to SKS functionality.

A Scalable Key Storage Remote Backup HSM can be identified by

- the firmware version 6.25.x. (lunacm **hsm showinfo** command).

If you have a cloning (non-SKS) Remote Backup HSM with any firmware other than 6.25.x, it cannot be upgraded to become an SKS Remote Backup HSM in the field. An SKS Remote Backup HSM must be ordered from the factory. An SKS Network HSM can be backed up only to an SKS Remote Backup HSM.

Note: Apply a physical label to differentiate your SKS Backup HSM, if you possess any non-SKS Backup HSMs.

Note: Migration of SMK from Luna SA 4.x SIM version to SafeNet SKS Network HSM (6.2.4) is currently not supported.

Critical Information

Patch 6.2.4 **must** be applied and firmware version updated to 6.25.1 **before** using the HSM.

Any SKS-encrypted blobs created prior to the 6.2.4 field update will not be usable after the update is applied. Due to this issue, the stability of High Availability synchronization, autorecovery, and manual recovery features is adversely affected.

Therefore, all customers must apply the 6.2.4 field update including the 6.25.1 firmware before using the SKS HSM (and SKS Backup HSM).

New Features and Enhancements

The following is a summary of the single feature new to SafeNet Network HSM 6.2.4 (formerly 6.2.3).

Scalable Key Storage (SKS)

Scalable Key Storage, or SKS, adds the ability to extract keys from the HSM as encrypted SKS objects and then insert the key SKS objects back into the HSM at a later time, when the key is needed, in a secure manner. This feature addresses use-cases where the number of keys needed for your application exceeds the capacity of the HSM. This allows for highly scalable solutions.

Scalable Key Storage is one of three main configurations of SafeNet HSM, available from the factory: Cloning, Key Export, and SKS.

CAUTION: You must apply field update 6.2.4 to your 6.2.3 HSM appliance before using the HSM. This updates appliance software to version 6.2.4, and both appliance HSM and Backup HSM firmware to version 6.25.1.

The following are summaries of features new to SafeNet HSM in release 6.2.2 and applicable to 6.2.3, 6.2.4, and newer, as well.

HA Auto-Reconnect

The HA feature now includes the ability of the Client to reconnect and resume application operation, without intervention, after completely losing contact with the HA group of HSMs. Context is retained, and token object states are preserved. Login is hands-free.

HA Failover withstands member deactivation and reconnects on activation of member partition

The following scenarios are addressed in 6.2.2 Client (and newer):

- When an application starts up the HA system ensures that the partition is activated.
- If a member has failed, during recovery the system checks that the partition is activated and confirms activation before the member is added back to the group.
- When a new member is being added to an HA group, the system checks whether or not the new member partition is activated and subsequently ensures activation before the member is successfully added to the HA group.

Network HSM gets OpenSSL upgrade

The SafeNet Network HSM receives enhanced OpenSSL to address the vulnerability described in CVE-2016-6304.

Advisory Notes

This section highlights important issues you should be aware of before deploying this release.

SKS Notes

The SKS feature is a factory-only release of the Network Appliance HSM and the SKS Backup HSM, both at firmware 6.25.1 (which must be immediately updated to version 6.25.1 with this update).

- There is ***no*** ability to modify existing units in the field to install SKS functionality.
- SKS HSM supports a single application partition, with the SKS Master Key (or SMK) created when the partition is created.
- An SKS partition can be created only on an SKS HSM.
- SKS backup and restore operations archive only the SMK (not crypto objects); ordinary backup and restore operations archive only crypto objects and not the SMK - the SKS Backup HSM can archive both in separate partitions.
- The SKS Backup HSM can backup multiple SMKs, but requires a unique partition for each one.
- SKS Multisign is not supported for this release.
- The SKS-encrypted object (blob) preserves all attributes, including fingerprints.
- The SKS-encrypted object and header, together, have SHA512 integrity. Objects are encrypted using AES-GCM with random IV per object. Contained objects, not including header, are also protected by SHA256.
- Key creation, blob export, blob import, and encryption/decryption of data records make use of session objects exclusively - only the SMK resides in flash memory, so there are no ongoing flash rewrite operations when using the SKS feature.
- Some legacy folder structures have not been updated. You might see references to SIM, which is an earlier version of what is now SKS.

Note: Do ***not*** perform firmware roll-back, unless directed to do so by Technical Support personnel. Firmware 6.25.1 contains several mandatory fixes that are not in 6.25.0.

Partition smkclone command does not confirm before overwrite

The **partition smkclone** command securely copies the SMK from a source SKS HSM to the SKS partition of a target HSM. Only one SMK can exist in an SKS partition. Therefore, the smkclone operation overwrites any SMK in the target HSM's SKS partition. However, the command proceeds directly to completion without pausing to request confirmation - caution is advised.

Notes from recent releases

Terminology Change

The feature formerly called SIM is now called Scalable Key Storage. The Capability Update now appears under that name when capabilities are listed. The terminology has also been updated throughout the documentation where appropriate.

Create a new SSL/NTLS Certificate on first use

All SafeNet Network HSMs come from the factory with the same SSL (NTLS) key. For proper security, run the **sysconf regencert** command before configuring your system for first use.

After SRK is enabled lunacm reports transport mode disabled

If Lunacm **srk show** command does not show the expected state for SRK after you run this command, the cache might not have been updated, following the most recent change. Exit and re-launch lunacm to see the current state of SRK.

Minimum Recommended Firmware for SafeNet Remote Backup HSM

For SKS-capable HSMs (release 6.2.4), the Backup HSM should be at firmware version 6.25.1.

SQL 2016 Support

Firmware 6.25.1 supports SQL 2016 only in non-FIPS mode.

HTL is deprecated

The HTL feature is now deprecated, and will be discontinued in a future release. If you have been using HTL, please plan for configuration and work-flow that does not make use of it.

Compatibility and Upgrade Information

The SafeNet Network HSM appliance version 6.2.3 is configured and shipped from the factory. There is no provision to field-upgrade to version 6.2.3 from other versions.

	Appliance Software		HSM Firmware		Client Software	
	Original	**After Update**	**Original**	**After Update**	**Original**	**After Re-installing**
SKS HSM Network Appliance	6.2.3	6.2.4	6.25.0	6.25.1	6.2.3	6.2.4
SKS Backup HSM	n/a	n/a	6.25.0	6.25.1	6.2.3	6.2.4

Orderable configurations and bundles

Part numbers for orderable items/bundles include:

908-000353-001 LUNA SA 7000 PED-AUTHENTICATED,1 HSMP,SKS,SW 6.2.3,FW 6.25.0

908-000354-001 LUNA SA 1700,PED-AUTHENTICATED,1 HSMP,SKS,SW 6.2.3,FW 6.25.0

908-000355-001 LUNA REMOTE BACKUP HSM FOR SKS,FW 6.25.0

908-000356-001 LUNA SA 7000 REMOTE PED BUNDLE (1 HSMP,SKS,SW 6.2.3,FW 6.25.0,REMOTE PED,20 PED KEYS,BACKUP HSM)

908-000358-001 LUNA SA 1700 REMOTE PED BUNDLE (1 HSMP,SKS,SW 6.2.3,FW 6.25.0,REMOTE PED,20 PED KEYS,BACKUP HSM)

Note: If you intend to backup the SMK (which should be mandatory in any production environment), you will need at least one SKS Backup HSM. Regular Backup HSMs for archiving crypto objects are not supported for SKS.
However, you can use your SKS HSM to archive crypto objects

Certifications and Compliance

About FIPS Validation

Note: HSMs with firmware 6.25.1 (for SKS) are not FIPS validated at this time, and have not been submitted for evaluation.

About Common Criteria

Note: HSMs with firmware 6.25.1 (for SKS) are not Common Criteria validated at this time, and have not been submitted for evaluation.

Supported Operating Systems

This section lists the supported operating systems for the SafeNet HSM client and Remote PED server.

SafeNet HSM Client

Operating system	Version	64-bit client installer on 64-bit OS	32-bit applications on 64-bit OS	32-bit client installer on 64-bit OS	32-bit client installer on 32-bit OS
Windows **Note:** The 64-bit Windows installer also installs the 32-bit libraries for compatibility with 32-bit client applications. No standalone 32-bit SafeNet HSM client is available.	2008 R2	Yes	Yes	No	No
	2012 R2	Yes	Yes	No	No
	2016	Yes	Yes	No	No
	10	Yes	Yes	No	No
Redhat-based Linux (including variants like CentOS and Oracle Enterprise Linux)	5	Yes	Yes	Yes	Yes
	6	Yes	Yes	Yes	Yes
	7	Yes	Yes	Yes	Yes

Remote PED Server

The remote PED server must be installed on any workstation used to host a remote PED. The remote PED server software is supported on the following Windows operating systems only:

- Windows 2016
- Windows 2012 and 2012 R2
- Windows 2008 R2
- Windows 10
- Windows 7 (64-bit)

Supported APIs

The following APIs are supported :

- PKCS#11 2.20
- Java 7
- Java 8
- OpenSSL
- Microsoft CNG

RADIUS Compatibility

For this release, we support the use of one RADIUS server, only.

Update Instructions

Reasons for Upgrade

If you have any SafeNet HSM at release 6.2.3, it must be updated to version 6.2.4 to fix service-affecting issues.

> **Note:** All components must be updated, client, appliance software, and HSM firmware.

Upgrade Paths

This update can be applied to release 6.2.3 SKS HSMs only.

Component Firmware Versions

The following table lists the supported firmware versions for the various components supported in SafeNet HSM 6.2.4.

Component	Version
SafeNet SKS Network HSM firmware	6.25.1
SafeNet SKS Remote Backup HSM firmware	6.25.1
SafeNet PED 2	2.4.0-3 through 2.6.0
SafeNet PED 2 Remote (Remote PED - requires PED workstation s/w on PC) [optional]	2.4.0-3 through 2.6.0

Preparing for the Upgrade

Before attempting to upgrade to SafeNet HSM 6.2.4, ensure that you have satisfied the following prerequisites:

- you have the upgrade software (downloaded from the Gemalto Service Portal).
- you have the authentication credentials required to perform the upgrade.
- you have prepared your HSMs for the upgrade.

Each of these prerequisites is discussed in detail in the following sections.

Obtaining the Upgrade Software

All of the software and firmware required to upgrade to SafeNet HSM 6.2.4 is available via download from the Gemalto Service Portal (formerly Customer Connection Center or C3).

> **Note:** Authorization codes are required to install firmware. To obtain the authorization codes for your firmware, contact Gemalto/SafeNet Technical Support.

The following packages are included in the upgrade software:

- SafeNet HSM 6.2.4 client software

- SafeNet Network HSM 6.2.4 appliance software
- SafeNet HSM 6.25.1 firmware (suitable for SafeNet SKS Remote Backup HSM, and SafeNet SKS Network HSM)
- PED firmware (Refer to the readme.txt file included in the SafeNet HSM 6.2.4 client software for more information)

Required Authentication Credentials

You must be able to log in to the HSM as the security officer (SO) to perform the upgrade. On PED-authenticated HSMs, you need the blue PED key. On password-authenticated HSMs, you need the SO password. On SafeNet Network HSM, you also need to be able to log in to the appliance using an admin-level account before you can log in to the HSM as the SO.

To install the SafeNet HSM Client software on a computer, you must run the installer with root/super-user privileges (Linux/UNIX) or Administrator privileges (Windows), or be able to launch the installer from an “Administrator: Command Prompt” (Windows).

Preparing your HSMs for the Upgrade

Perform the following tasks to prepare your HSM for the upgrade:

Note: Generally, the following actions can be performed remotely for PED-Authenticated HSMs, as long as you have already imprinted an orange Remote PED Key for that HSM, and have that orange key available to use at a Remote PED workstation (see the main SafeNet HSM customer documentation for instructions to configure and use the Remote PED feature).

1. Ensure that your appliance software (for SafeNet Network HSM only), and firmware are at a starting version listed in the "Upgrade Paths" section above. (The installed Client software version does not matter, because the Client software installs in place of any previous version, with no dependencies on any previous version.)
2. Connect your HSM appliance or host computer to an uninterruptible power supply (UPS), if available. Although this is not a requirement, use of a UPS is strongly recommended to ensure successful completion of all upgrade activities.
3. Ensure that your USB devices (SafeNet USB HSM, SafeNet Remote Backup HSM) are connected using a USB cable, to the computer on which you are installing the Luna software. If the USB devices are not connected to the host computer, the USB drivers do not install successfully. This issue applies to Windows 2008 only.
4. If the Secure Recovery Key (SRK) on the HSM is enabled, it must be disabled before you can upgrade the HSM firmware. The SRK carries an external split of the HSM's Master Tamper Key (MTK) that is imprinted on the purple PED key. When you disable the SRK, the SRV (Secure Recovery Vector) portion of the MTK is returned to the HSM, so that the SRV is no longer external to the HSM. It is only in this state that you can upgrade the HSM firmware. After you upgrade the firmware, you can re-enable SRK, if desired, to re-imprint a purple PED key with the SRV.
5. Backup the content of your HSM or HSM partitions to SafeNet Backup HSMs, or to Small Form-Factor Backup devices (if you have the SFF Backup option).
6. Copy the SafeNet HSM 6.2.4 upgrade software package (the downloaded tar file) to the client computer and use your favorite archiving program to untar the archive.
7. Stop all applications and services that are using the HSM.

Performing the Upgrade

Upgrade the client software, appliance software, and the HSM firmware, as specified in the following table:

Product	Client software upgrade	Appliance software upgrade	HSM firmware upgrade
SafeNet SKS Network HSM	X	X	X
SafeNet SKS Backup HSM	X		X

Upgrade the software/firmware in the following order:

1. Client software
2. Appliance software (SafeNet Network HSM only)
3. HSM firmware

Upgrading the Client Software

> **Note:** Upgrade the client software before upgrading the appliance software or HSM firmware.

Overview - upgrading your client software consists of the following main steps:

1. Ensure that all applications using the SafeNet HSM software libraries are stopped.
2. Uninstall your old client software. When you uninstall your old SafeNet HSM client software, backups of your existing configuration file (all SafeNet HSM types), and certificates (SafeNet Network HSM or Remote PED), are retained so that they may be restored. Any other custom files/directories found in the client installation directory/folder that are not part of the standard client installation are also retained.
3. Install the SafeNet HSM 6.2.4 client software. On Linux/Unix, your backup configuration file and certificates are automatically restored. On Windows, your configuration file and certificates are retained.

To upgrade the client software to SafeNet HSM 6.2.4

1. Uninstall the currently installed SafeNet HSM client software. The method you use is platform specific, as follows:
   - **Windows** Use the Windows uninstaller (Start > Control Panel > Programs and Features) to uninstall SafeNet HSM Client, which removes all of the SafeNet HSM Client software components.
   - **AIX/Linux** Run the /usr/safenet/lunaclient/bin/uninstall.sh script.
   - **HP-UX/Solaris** Run the /opt/safenet/lunaclient/bin/uninstall.sh script.
2. Install the SafeNet HSM 6.2.4 software. The method you use is platform specific, as follows:
   - **Windows** Run the LunaClient.msi installation program and respond to the prompts as they appear.
   - **Linux/Unix** Run the install.sh installation script and respond to the prompts as they appear.

Upgrading the SafeNet Network HSM Appliance Software

Firmware

Upgrading the SafeNet SKS Network HSM appliance software **automatically** upgrades the SafeNet SKS Network HSM firmware. This contrasts with non-SKS appliance updates, that normally allow you to choose when firmware is upgraded. The 6.25.1 firmware update is mandatory.

Applicability

The SKS appliance software update can be applied only to the SafeNet SKS Network HSM appliance. You cannot turn a non-SKS appliance into an SKS appliance.

No Appliance Rollback

Appliance software upgrade is a one-way operation. There is currently no way to downgrade the appliance software once a new version is applied. This contrasts with

- SafeNet HSM Client software, which can be replaced by any version, simply by uninstalling the current version and installing a desired version, and
- SafeNet HSM firmware, which can be rolled back to the version that was installed before the currently-installed version. This applies only to versions since firmware rollback was enabled. Rollback to 6.25.0 is **not** recommended. Firmware 6.25.1 is mandatory.

To upgrade the SafeNet Network HSM Appliance software to Luna HSM 6.2.4

1. Copy the SafeNet HSM 6.2.4 appliance package file (.spkg) to the SafeNet Network HSM appliance you want to upgrade:
   - Windows pscp <path>\<partnum>.spkg admin@<LunaSA_hostname>:
   - Unix/Linux scp <path>/<partnum>.spkg admin@<LunaSA_hostname>:
2. Stop all client applications that are connected to the SafeNet Network HSM.
3. At the console, log in to the SafeNet Network HSM appliance using an admin-level account. The default account is admin.
4. Log in to the SafeNet Network HSM as the HSM Security Officer:

   lunash :> hsm login
   - For SafeNet Network HSM with PED authentication, the blue PED Key is required.
   - For SafeNet Network HSM with Password Authentication, you are prompted for the HSM Admin (SO) password.
5. (Optional) Verify that the upgrade package file that you copied is present:

   lunash :> package listfile
6. (Optional) Verify the upgrade package:

   lunash :> package verify <partnum>.spkg -authcode <authorization_code>

   Verification requires approximately 90 seconds.
7. Install the upgrade package:

   lunash :> package update <partnum>.spkg -authcode <authorization_code>

   The installation/upgrade process takes approximately 90 seconds. During that time, a series of messages are displayed that detail the progress of the upgrade. At the end of this process, the message “Software upgrade completed!” is displayed.

Upgrading the HSM Firmware

SKS Backup HSM Firmware Target

Backup firmware 6.25.1 that is delivered in the Client software archive can be applied only to an SKS Backup HSM that has firmware 6.25.0.

No FIPS

Firmware 6.25.1 is not FIPS validated, and has not been submitted for evaluation at this time.

Upgrading SafeNet Network HSM firmware

For 6.2.4 release, when you install the SKS Network appliance software, the HSM firmware updates automatically.

Upgrading the SafeNet SKS Backup HSM firmware

To upgrade the firmware on a SafeNet SKSBackup HSM, launch the LunaCM utility on a SafeNet HSM client computer

- that contains a copy of the firmware upgrade (.fuf) file with its associated firmware authentication code (.txt) file, and
- is connected to the SafeNet SKS Backup HSM that you want to upgrade.

1. Copy the firmware file (<fw_filename>.fuf) from the firmware folder on the software CD to the SafeNet HSM client root directory:
   - Windows: C:\Program Files\SafeNet\LunaClient
   - Linux/AIX: /usr/safenet/lunaclient/bin
   - Solaris/HP-UX: /opt/safenet/lunaclient/bin
2. Obtain the firmware authorization code:
   a. Contact SafeNet Customer Support (support@safenet-inc.com). The firmware authorization code is provided as a .txt file.
   b. Copy the <fw_auth_code>.txt file to the SafeNet HSM client root directory:
   - Windows: C:\Program Files\SafeNet\LunaClient
   - Linux/AIX: /usr/safenet/lunaclient/bin
   - Solaris/HP-UX: /opt/safenet/lunaclient/bin
3. Launch the LunaCM utility:

   Windows

   a. Open a Command Prompt window

      (Start > Programs > Accessories > Command Prompt).

   b. Change to the SafeNet HSM client root directory:

      cd C:\Program Files\SafeNet\LunaClient

   c. Enter the following command

      Lunacm

   Linux

   a. Open a terminal window and change to the SafeNet HSM client root directory:

      /usr/safenet/lunaclient/bin

   b. Enter the following command:

      ./lunacm
4. Enter the following command to log in to the HSM. Note that the password is not required on PED-based systems:

   hsm login [-password <password>]
5. Enter the following command to upgrade the firmware on an attached SafeNet USB HSM:

   hsm –updateFirmware –fuf <fw_filename>.fuf –authcode <fw_authcode_filename>.txt

Additional Tasks for Java Users

You must copy the Java library (LunaAPI.dll) and jar file (LunaProvider.jar) from the client installation folder to the jre/lib/ext folder.

Returning the HSM to Operation

After performing the upgrade, you must reactivate the HSM partition (if applicable) and re-register the SafeNet HSM client to return the HSM to operation.

HSM Summary Information

The following is the output of "hsm show" command for a SafeNet Network HSM release 6.2.4.

```
Luna SA 6.2.4-8 Command Line Shell - Copyright (coffee) 2001-2017 SafeNet, Inc. All rights
reserved.

[auto224] lunash:>hsm show


   Appliance Details:
   ==================
   Software Version: 6.2.4-8

   HSM Details:
   ============
   HSM Label: mysa
   Serial #: 156674
   Firmware: 6.25.1
   HSM Model: K6 Base
   Authentication Method: PED keys
   HSM Admin login status: Not Logged In
   HSM Admin login attempts left: 3 before HSM zeroization!
   RPV Initialized: Yes
   Audit Role Initialized: No
   Remote Login Initialized: No
   Manually Zeroized: No

   Partitions created on HSM:
   ==========================
   There are no partitions.

   Number of partitions allowed: 1
   Number of partitions created: 0

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

   HSM Storage Information:
   ========================
   Maximum HSM Storage Space (Bytes): 2097152
   Space In Use (Bytes): 0
   Free Space Left (Bytes): 2097152

Command Result : 0 (Success)
```

The following is the output of "hsm showinfo" command for a SafeNet Backup HSM release 6.2.4.

```
lunacm:> hsm si

        Partition Label -> SKSBkHSM
        Partition Manufacturer -> Safenet, Inc.
        Partition Model -> G5Backup
        Partition Serial Number -> 475289
        Partition Status -> OK
        Token Flags ->
                CKF_RNG
                CKF_USER_PIN_INITIALIZED
                CKF_RESTORE_KEY_NOT_NEEDED
                CKF_PROTECTED_AUTHENTICATION_PATH
                CKF_TOKEN_INITIALIZED
        RPV Initialized -> No
        Slot Id -> 28
        Session State -> CKS_RW_PUBLIC_SESSION
        Role Status ->   none logged in
        Token Flags ->
                TOKEN_KCV_CREATED
        Partition OUID: 000000000000000099400700

        Partition Storage:
                Total Storage Space:  262144
                Used Storage Space:   52604
                Free Storage Space:   209540
                Object Count:         4
                Overhead:             9424

        *** The HSM is NOT in FIPS 140-2 approved operation mode. ***

        Firmware Version -> 6.25.1
        Rollback Firmware Version -> 6.25.0
        HSM Storage:
                Total Storage Space:  16252928
                Used Storage Space:   21748
                Free Storage Space:   16231180
                Allowed Partitions:   20
                Number of Partitions: 2

        License Count -> 5
                1. 621010355-000 Luna remote backup HSM base configuration
                1. 621000006-001 Enabled for 15.5 megabytes of object storage
                1. 621000007-001 Enable the master tamper key to be stored externally
                1. 621000008-001 Enable remote PED capability
                1. 621000005-001 Maximum 20 partitions

Command Result : No Error
```

The following is the output of "slot list" command for a SafeNet Backup HSM release 6.2.4 (firmware 6.25.1).

```
Slot Id -> 3
HSM Label -> no label
HSM Serial Number -> 7002733
HSM Model -> G5Backup
HSM Firmware Version -> 6.25.1
HSM Configuration -> Luna G5 (PED) Undefined Mode / Uninitialized
HSM Status ->  Zeroized
Current Slot Id: 1
```


Known Issues

This section lists the issues known to exist in the product at the time of release. Workarounds are provided where available.

Issue Priority Definitions

The following table defines the priority of the issues listed in this section.

Priority	Classification	Definition
C	Critical	No reasonable workaround exists.
H	High	Reasonable workaround exists.
M	Medium	Medium level priority problems.
L	Low	Lowest level priority problems.

Known Issues

Release 6.2.3/6.2.4 is a feature release, only. The Known Issues list from release 6.2.2 remains valid.

Issues from release 6.2.3

Issue	Priority	Synopsis
LHSM-42681	M	**Problem:** When this feature is enabled, the shim slot cannot backup or restore the smk to the G5 backup device. It throws CKR_DATA_LEN_RANGE error. **Workaround:** 1. Turn off the feature. 2. Use another regular LunaClient 6.2.4 without this feature and perform the backup/restore operation. .
LHSM-42487	M	**Problem:** Inserting an existing SKS object should return a more meaningful message If the SKS object already exists on the HSM, CA_SIMInsert returns CKR_ CANCEL, which is ambiguous. It should return "Object already exists."
LHSM-42389	M	**Problem:** sysconf config factoryReset issue When performing "sysconfig config factoryReset", previously configured network setting maybe lost. When the Network HSM appliance is rebooted, it can come back with a new DHCP configured IP address. If the appliance is configured for radius server, ssh login after the reboot might result in some delay as radius server does not recognise the new IP as a registered client. **Workaround:**When the Network HSM appliance is rebooted after performing "sysconfig config factoryReset", ensure that network configuration is updated such that the HSM appliance is assigned an IP address that is registered with the radius server.

Resolved Issues

The Known Issues list from release 6.2.2 remains valid.

Issues from release 6.2.3 fixed in release 6.2.4

Issue	Priority	Synopsis
LHSM-42420	C	**Problem:** OUIDs in HA members are NOT the same When a key was generated from HA slot, in each of HA members it should have the key with the same uid, but in 6.2.3, they are different. **Fixed:** in release 6.2.4
LHSM-42408 / LHSM-42436	M	**Problem:** HA slot "partition contents" throws CKR_OBJECT_HANDLE_ INVALID error **Fixed:** in release 6.2.4
LHSM-42323	H	**Problem:** Snmp Trap Missing trap messages are generated locally at the Network HSM appliance /var/log however they are not being sent out to rsyslog. **Fixed:** in release 6.2.4
LHSM-42322	M	**Problem:** Mismatched configuration in LunaCM for SIM partitions **Fixed:** in release 6.2.4
LHSM-42320	M	**Problem:** SSH to SA Audit Role Failed at public-key Authentication with error "Unsupported option 'gssapiauthentication' " **Fixed:** in release 6.2.4

Support Contacts

If you encounter a problem while installing, registering, or operating this product, ensure that you have read the documentation. If you cannot resolve the issue, contact your supplier or Gemalto Customer Support. Your level of access to this service is governed by the support plan arrangements made between Gemalto and your organization. Consult that support plan for further information about your entitlements, including the hours when telephone support is available to you.

Contact method	Contact
Customer Support Portal	https://supportportal.gemalto.com Existing customers with a Technical Support Customer Portal account can log in to manage incidents, get the latest software upgrades, and access the Gemalto Knowledge Base.