Luna HSM 6.0

CUSTOMER RELEASE NOTES

Issue Date: 19 November 2015

Document Part Number: 007-012225-004 Rev. D

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

http://www.securedbysafenet.com/releasenotes/luna/crn_luna_hsm_6-0.pdf

Contents

Product Description

The SafeNet family of hardware security modules (HSMs) 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 HSMs are available in the following form factors which offer multiple levels of performance and functionality:

Luna SA

Luna SA is a network-based, Ethernet-attached HSM appliance that offers up to 100 HSM partitions, high-availability configuration options, remote management PED and backup, and dual hot-swappable power supplies. Luna SA provides cryptographic services for network clients that are authenticated and registered against HSM partitions. Two models of Luna SA are available – password authenticated and PED authenticated - in two performance variants, the Luna SA-1700 and Luna SA-7000, which are capable of 1700 and 7000 (RSA 1024-bit) signings per second respectively.

Luna PCI-E

Luna PCI-E is a PCI-E form factor HSM that is installed directly into an application server to provide cryptographic services for the applications running on the server. Two models of Luna PCI-E are available – password authenticated and PED authenticated - in two performance variants, the Luna PCI-E-1700 or PCI-E-7000 which are capable of 1700 and 7000 (RSA 1024-bit) signings per second respectively.

Luna G5

Luna G5 is a USB-attached HSM that is attached directly to an application server, to provide cryptographic services for the applications running on the server.

Release Description

Luna HSM 6.0 introduces some major features to improve the scalability and enhance the ability to work in multi-tenant environments.

Luna HSM 6.0 Security Patch

This firmware patch for Luna G5 and Luna PCI-E and Luna SA to firmware version 6.2.5 or 6.10.9 or 6.20.2 or 6.21.2 or 6.22.3, addresses a vulnerability described in security bulletin 150512-1. We recommend that you install this patch immediately on all applicable HSMs.

Find the update instructions in document 007-013037-001 Luna HSM Firmware Vulnerability Update Sheet, accompanying the patch.

See also the FIPS comments below, and the effects of the current patch on firmware update paths.

SIM Migration Patch

If you want to migrate a SIM-based HSM to Luna SA, please contact technical support to obtain a patch to support the migration before you begin. Reference DOW3216 in your query.

About FIPS Validation

Some organizations require that their HSMs be validated by the Cryptographic Module Validation Program (CMVP) to conform to the Federal Information Processing Standards (FIPS) Security Requirements for Cryptographic Modules. If you require FIPS-validated HSMs, refer to the following sections for the FIPS-validation status of the products supported by Luna HSM 6.x at the time of this documents release.

For the most up-to-date information, refer to the following web sites or contact SafeNet Customer Support at support@safenet-inc.com to determine when a particular version of a Luna HSM receives FIPS validation:

- Modules in Process: http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140InProcess.pdf
- Completed Validations - Vendor List: http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/1401vend.htm

Luna SA and Luna PCI-E

The Luna K6 (PCIe) HSM with firmware version 6.2.1 or 6.2.5, used inside the Luna SA and alone as Luna PCI-E, has received the following FIPS 140-2 validations:

- FIPS 140-2 Level 2 validation
  - certificate # 1693 for f/w 6.2.1
  - new certs with new numbers covering f/w 6.2.5 expected shortly (in Coordination)
- FIPS 140-2 Level 3 validation
  - certificate # 1694) for f/w 6.2.1
  - new certs with new numbers covering f/w 6.2.5 expected shortly (in Coordination)
- FIPS 140-2 Level 2 validation (certificate # 2427) for f/w 6.10.9
- FIPS 140-2 Level 3 validation (certificate # 2428) for f/w 6.10.9

Luna G5

Luna G5 with firmware 6.2.3 (see note below about version 6.2.5) has received the following FIPS 140-2 certificates:

- FIPS 140-2 Level 2
  - certificate # 1958 update of existing cert now lists f/w 6.2.5
  - certificate # 2403 for firmware 6.10.9
- FIPS 140-2 Level 3
  - certificate # 1957 update of existing cert now lists f/w 6.2.5)
  - certificate # 2426 for firmware 6.10.9

About Common Criteria

Some organizations specify Common Criteria evaluation for equipment and systems that they deploy. We submit fewer products/versions for CC evaluation than we do for FIPS validation, due to relative demand, cost, and the much longer time-frames involved. Completed CC evaluations: http://www.commoncriteriaportal.org/products/

New Features and Enhancements

The following are summaries of features new to Luna HSM in release 6.0.

50 and 100 Partitions - Scalability

Where formerly you had the option to use the factory-default two application partitions per Luna SA, with option to upgrade to 5, 10, or 20 partitions, you now have the additional option to expand that number to 50 or 100 application partitions per Luna SA. This could prove especially useful in cloud applications and crypto-as-a-service offerings.
[no firmware dependency]

PPSO

Per-Partition Security Officer (PPSO) allows each application partition to have its own Security Officer and to be separately managed. Formerly, every partition was created by the HSM Security Officer, and then remained under the central management of that Security Officer. Now, with the PPSO option, the HSM SO creates an application partition, but can hand it off to a different Security Officer who has administrative ownership of that partition. The HSM SO can still see that the application partition exists, and can destroy it when it is no longer needed, but the content and management of the partition are invisible and inaccessible to the HSM SO. The Partition SO sets policies, creates roles and performs all other management functions independently, and without any outside oversight.
[requires firmware version 6.22.0 or newer]

STC

The Secure Trusted Channel (STC) option takes the Luna SA Network Trust Link (NTL) to a new level, enabling more convenient setup of client-to-application-partition links while offering the possibility to lock the client ability to access a Luna SA partition to specific host computers with the STC soft token. The soft token can also be duplicated, enabling an elastic client model where that is an important consideration.

Alternatively, you have the option to tie that authentication and access control to a portable hardware token, which can be carried to (and used from) any LunaClient computer.
[requires firmware version 6.22.0 or newer]

Port Bonding/Teaming

Luna SA's two physical interfaces, eth0 and eth1, can be configured into a single virtual interface, bond0, for a round-robin load-balancing service.This service provides a hot standby mode in the event of network interface failure.
[no firmware dependency]

SNMP Traps and Alarms

SNMP traps for failures and alarms are extended in the following sub-systems: fans, power supplies, motherboard voltages, system battery, system clock, HSM, NTLS and disk drive.
[no firmware dependency]

Advisory Notes

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

Minimum Recommended Firmware for Luna Remote Backup HSM

With firmware older than version 6.10.x, 'ped connect' fails to work properly. The lunacm command returns "No Error, but the PED ID remains set to 1 and PedServer "Client Information" shows "Not Available". We recommend that you update the Luna Backup HSM firmware to version 6.10.x

RSA Key Sizes and FIPS

The NIST SP800-131A transition required that RSA keygen be restricted to RSA-2048 and RSA-3072 sizes only. Therefore, when FIPS mode is on (HSM policy 12 "Allow non-FIPS algorithms" set to "No"), RSA-1024 and RSA-4096 are unavailable.

Migration Notes

Luna HSM 6.0 introduces significant changes to way in which the product operates. Refer to the Luna HSM 6.0 Update Instructions for descriptions of the tasks you might need to perform to successfully migrate your HSMs to Luna HSM 6.0.

Compatibility and Upgrade Information

This section provides the following information:

"Upgrade Paths" below

"Supported Software and Firmware" below

Upgrade Paths

Component	Directly from version	To version
Luna SA client software	Any	6.0
Luna SA appliance software	5.2.3 , 5.2.4, 5.2.6, 5.3.0, 5.3.1, 5.3.3, 5.3.5, 5.3.6, 5.4.0, 5.4.1, 5.4.2, 5.4.3, 5.4.4, 5.4.6, 5.4.7 [see Note 1]	6.0
HSM firmware	6.2.1, 6.10.1, 6.10.x, 6.20.0, 6.21.0 [see Note 2]	6.22.0

[NOTE 1: If Luna appliance software is older than version 5.2.3-1, you must update to appliance software version 5.2.3-1 before updating to appliance software version 6.0. Refer to the earlier upgrade documentation provided by SafeNet Technical Support.]

[NOTE 2: If HSM firmware is older than version 6.2.1, you must update to firmware version 6.2.1 before updating to firmware 6.22.0. Refer to the earlier upgrade documentation provided by SafeNet Technical Support.

Luna Backup HSMs at their current firmware version, if you wish, and will work to backup and restore newer-firmware HSMs. Backup HSMs do not perform cryptographic operations on the objects that they archive, so there is no urgent requirement to update.]

Supported Software and Firmware

The following table lists the supported firmware/software versions for the various components supported in this release.

Component	Version
Luna HSM client software	6.0
Luna SA appliance software	6.0
Luna SA firmware	6.2.5 through 6.22.2
Luna PCI-E firmware	6.2.5 through 6.22.2
Luna G5 firmware	6.2.5 through 6.22.2
Luna Remote Backup HSM firmware	6.0.8 [see Note 1]
Luna PED 2/ PED 2 Remote firmware versions - minimum required 2.4.0-3 - version shipped 2.5.0-3 - option to upgrade to 2.6.0	2.4.0-3 through 2.6.0 [see Note 2]
[NOTE 1: The Luna Remote Backup HSM performs archiving only, and has no ability to perform cryptographic operations using the keys and objects that it contains. Therefore it can remain at firmware version 6.0.8 (or any higher version); no advantage is gained by updating to newer firmware.]	
[NOTE 2: Version 2.4.0-3 is the PED version required for basic PED and Remote PED function with Luna HSM 5.x or 6.x. For newer options like SFF backup, newer versions of PED firmware are needed. Refer to the table in the *HSM Administration Guide*, on the page "Using the PED", under heading "Versions".]	

Upgrade Paths

This section summarizes upgrade paths for Client software, HSM firmware, and (if applicable) SafeNet appliance software.

Upgrade Paths for Security Patch

The security patch has specific previous firmware versions from which patch updates can be directly installed. Once the patch is installed, you can update only to a firmware version that is also secured by the equivalent patch. See tables below.

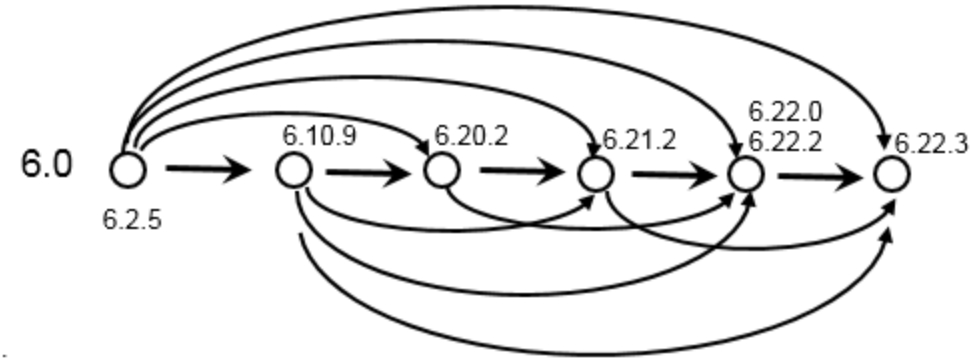
Upgrade Paths for Secure Firmware

The following upgrade paths are available in this patch. If your HSM is at a lower software or firmware version than those indicated in the “current software version” and “current firmware version” columns, upgrade to an indicated current version, and then apply the secure patch.

Software Version / Release FW	Available Firmware Releases	Recommended Firmware	FIPS Target
6.0 / 6.22.0	6.2.1	6.2.5 or 6.10.9	Validated
	6.10.1	6.10.9	Validated
	6.10.2		
	6.10.7		
	6.20.0	6.20.2	Not Planned
	6.21.0	6.21.2	Not Planned
	6.22.0	6.22.3	In Planning
	6.22.2		

Note: If you have a PKI bundle including a Luna SA and an attached Luna G5 running in PKI mode, often the Luna G5 has earlier firmware than the Luna SA. Upgrade the Luna SA first, following the above upgrade paths. Then, when you upgrade the firmware on the associated Luna G5, the Luna G5 upgrades to the same firmware version as is installed on the Luna SA.

Figure 1: Firmware Upgrade Paths Diagram



Supported Operating Systems

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

Luna Client

Note: The Luna SA client works in virtual environments. Luna G5 and PCI-E are not supported in virtual environments.

Operating System	Version	64-bit client	32-bit client on 64-bit OS	32-bit client
Windows	2008 R2	Yes	Yes	No
	2012 and 2012 R2	Yes	Yes	No
Redhat-based Linux (including variants like CentOS and Oracle Enterprise Linux)	5	Yes	Yes	Yes
	6	Yes	Yes	Yes
	7	Yes	Yes	Yes
OpenSuse Linux	11.4	Yes	Yes	Yes
	12	Yes	Yes	Yes
	13	Yes	Yes	Yes
Debian	6	Yes	n/a	Yes
	7	Yes	Yes	Yes
FreeBSD	8.3, 8.4	Yes	Yes	Yes
	9	Yes	Yes	Yes
	10	Yes	Yes	Yes
Solaris SPARC	10	Yes	Yes	No
	11, 11.1, 11.2	Yes	Yes	No
Solaris x86	10	Yes	Yes	Yes
	11, 11.1, 11.2	Yes	Yes	No
AIX (Luna SA only. Luna G5 and Luna PCI-E are not supported on AIX for this release.)	6.1	Yes	Yes	No
	7.1	Yes	Yes	No

NOTE 1: Luna SA and Luna PCI-E supported; Luna G5 is not supported with HP-UX for this release.

NOTE 2: Luna SA supported; Luna G5 and Luna PCI-E not supported with AIX for this release.

NOTE 3: Luna SA supported; Luna G5 and Luna PCI-E not supported with OSX for this release.

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 2012 and 2012 R2;
- Windows 2008 R2
- Windows 7 (64-bit)

Supported APIs

The following APIs are supported :

- PKCS#11 2.20
- Java 5 [See Note below]
- Java 6 [See Note below]
- Java 7
- Java 8
- OpenSSL
- Microsoft CAPI
- Microsoft CNG

> **Note:** Luna HSM 6.0.x is the **last release** to maintain support for Java 5 and Java 6. With future releases, and until further notice, only Java 7 and above will be supported.

Advanced Configuration Upgrades

The following are licenses that can be purchased separately, either factory-installed or customer-installed, with some restrictions.

- Luna SA partition upgrades (5 , 10, 15, 20, 50, or 100)
- Partition SO (PSO)
- Maximum memory
- ECIES acceleration
- Korean algorithms

Server Compatibility

The Luna PCI-E card and Luna G5 USB-connected HSM are tested for compatibility with some commonly used servers. Other servers might work, but are untested.

Specifically, we have noticed compatibility problems with:

Server	slot(s)	Failure
Dell R620	2	Does not fit in slot 2 (but does fit and work in slot 1)
Dell R720	1	HSM card not detected in slot 1

Server	slot(s)	Failure
		(but works in slots 2 and 3)
IBM x3650 M2	4	HSM card not detected in slot 4 (but detected and works in slots 1, 2, and 3)
Dell T610	3 and 4	PCIe training error in slots 3 and 4 (but works in slots 1, 2, and 5)

Luna PCI-E Server Compatibility

The Luna PCI-E card is designed to the PCIe 1.1 standard, for use in servers with PCIe x4 slots. For further information and compatibility options, refer to the Luna HSM 6.0 Overview that is included with your HSM documentation.

Known Issues

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

Issue Severity Definitions

The following table defines the severity 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.

Luna Known Issues

Issue	Severity	Synopsis
LUC-705: Unable to establish an HTL connection (UNIX/Linux)	M	**Problem:** Attempting to establish a host trust link (HTL) connection fails on UNIX and Linux platforms. **Workaround:** After generating the one-time token (OTT), wait for about 30 seconds before transferring it to the client. Note that you must transfer the token before it expires. Use the htl show command to view the OTT expiry time.
LUC-691: Remote PED fails to connect to G5 (Solaris Sparc)	H	**Problem:** Attempting to use a remote PED to connect to a G5 HSM attached to a Solaris client fails intermittently. **Workaround:** The failure is due to a timeout on the PED connection. When using a remote PED to connect to a G5 hosted on a Solaris client, ensure that you use the **ped disconnect** command on both the server and client to disconnect the remote PED when you are finished authenticating.

Issue	Severity	Synopsis
LHSM-18280 LunaCM: *remotebackup start* cmd, crashes lunacm	M	**Problem:** In LunaCM, when run the remotebackup start cmd, crashes lunacm, leaving it in an indeterminate state. **Workaround:** Exit the DOS prompt, and relaunch LunaCM to bring it back.
LHSM-17289 lunacm "ped vector" commands missing for PPSO Ped-Auth admin partition until I select a legacy HSM, then go back to PPSO slot	H	**Problem:** When running lunacm and selecting a Luna PCI-E PED-Auth PPSO admin slot, the ped vector commands are missing, meaning that setting/unsetting a remote PED key is not possible. If lunacm is then pointed at a legacy firmware slot, the ped vector commands are available. Then if lunacm is pointed back at the original PPSO slot, the command is also there! **Workaround:** See description above. If you encounter this problem and do not have a separate HSM with legacy partition, then there is no workaround. For Luna SA users, the "hsm ped vector" commands are done on the appliance via lunash, so the problem never occurs.
LHSM-17287 Lunacm shows SA HSM and partition after tearing down STC connection - and - LHSM-15030 STC Token init causes any hidden STC-enabled partitions to be revealed	H	**Problem:** When using STC with a Luna SA, if the client computer contains a Luna PCI-E and policy 39 is enabled for that local Luna PCI-E, it can happen that after tearing down STC for the Luna SA, the Luna SA partitions might be visible. **Workaround:** Avoid setting STC policy for a locally installed HSM. It is not yet supported. The above is from obscure testing scenarios, and the improperly visible Luna SA partitions cannot be accessed or used until you properly re-establish an STC link with the Luna SA.
LHSM-16838 Luna SA 6.0: STC K6 crashed after 7 days with LUNA_RET_DEVICE_ERROR	H	**Problem:** Uptime of just 7 days and K6 crashed. Nothing heavy running. Just STC enabled. **Workaround:** None. If you are testing STC, SafeNet Technical Support would appreciate a capture of the logs and of dual-port dump, if this occurs.
LHSM-16776 PKI bundles: partition restore failed with CA4 for migration test	H	**Problem:** For Luna SA, in order to migrate a pre-existing Luna CA4 (on Luna DOCK) PKI bundle to Luna G5, the first step is normally to restore the desired object(s) from the Luna CA4 HSM to a partition on the Luna SA, and then clone to the Luna G5. However, on Luna HSM 6.0 the initial "restore" step fails with "RC_DATA_INVALID" (even though "set legacydomain" succeeded). **Workaround:** If possible, migrate before you upgrade to Luna HSM 6.0.
LHSM-15994 Luna SA 6.0: STC client now could not get a session with 2nd partition with CKR_STC_CONTAINER_INVALID	H	**Problem:** STC client now fails on using a 2nd partition. 1.STC enabled. 2.PSO partitions created. 3.More than 1 PSO partition STC key passed to 'tenant'. 4.Tenant registers the more than 1 PSO partitions they were given to their client token. ◦Note that the tenant cannot have admin partition STC also registered to same token 5.Tenant proceeds as follows: ◦Initializes one PSO partition

Issue	Severity	Synopsis
		◦Enables STC policy for that partition (<<< problem triggered now) ◦Without exiting lunacm, they try to switch to and work with other PSO partition The problem is that in step 5, point 2 above, user is warned (in lunaCM) that their active sessions will be closed upon changing STC policy. The firmware does this. But client does not clear it's session table. Therefore Step 5, point 3 tries to use an orphan session. **Workaround:** Exit and relaunch lunacm.
LHSM-15030 STC Token init causes any hidden STC-enabled partitions to be revealed	H	**Problem:** If you enable the HSM policy 39 for STC on the Admin partition of a PCIe K6, any non-configured slots on that HSM should be hidden. However, if we then run 'stc tokenInit', all the slots that should be hidden, reappear. **Workaround:** None.
LHSM-15026 LunaCM role list command is broken in Solaris Sparc	H	**Problem:** LunaCM role list command is broken in Solaris Sparc **Workaround:** Do not use "role list" in lunacm on Solaris for Luna HSM release 6.0.
LHSM-15016 Luna SA 6.0: STC hsm soft init fails with "Error: 'hsm init' failed. (80000000 : LUNA_RET_ERROR)"	H	**Problem:** When issuing an 'HSM initialize' or 'HSM zeroize' command through lunash or lunacm, the command succeeds, but returns: 'LUNA_RET_ERROR' for lunash or 'CKR_GENERAL_ERROR' for lunacm. LunaCM then needs a restart. This is a result of the active STC link through which the command is issued being dropped unilaterally by the HSM as a result of the zeorize / factory reset actions. **Workaround:** Restart lunacm.
LHSM-15004 Luna SA 6.0: STC hsm soft init fails with "Error: 'hsm init' failed. (80000000 : LUNA_RET_ERROR)"	H	**Problem:** When running initialization/zeroize for HSM with STC: 1. For soft Zeorize – i.e. 'HSM init' of already initialized HSM (original defect report) will work properly and return OK. 2. For hard zeorize – 'HSM zeroize' command will succeed but report "CKR_GENERAL_ERROR" 3. For factory reset – 'HSM factoryreset' command will succeed but report "CKR_GENERAL_ERROR" – HSM will not crash **Workaround:** Be aware that init/zeroize of the HSM generates error messages if STC was active, even though the init/zeroize finished smoothly, without error. The errors are from STC, which loses contact when the HSM zeroizes.
LHSM-14992 After successfully enabling SRK lunacm reports transport mode disabled	H	**Problem:** On an HSM with firmware 6.22.0, if you enable SRK and successfully imprint a purple PED Key, lunacm still shows SRK as disabled. This is a display error that has not caught up with the actual state of the HSM, but can be worrisome and might not be acceptable to an auditor.

Issue	Severity	Synopsis
		Workaround: Restart lunacm to update the cache of hsm capabilities and policies. The correct state of SRK is then visible.
LHSM-14577 Cannot Verify Audit logging secret from source SA to Centos Client:(Legacy Fw)	H	**Problem:** Cannot verify an audit "tgz" file. The file must be untarred, first. Also, the system is unable to verify a log that was in progress when it was archived - that is, only logs in the ready_for_archive folder can be verified. The same log entry that was in progress at the end of one log file will be present and verifiable at the beginning of the next log file. **Workaround:** Be aware of the above. The audit-log handling documentation is being improved, to highlight the above information.
LHSM-14210 Performance loss of RSA, ECDSA, Digest, AES/DES3 and DSA	H	**Problem:**Comparing to Luna SA 5.4, we have performance slow-down on test cases with RSA, ECDSA, Digest, AES/DES3 (PE1746 is disabled) and DSA. The range is about 5-10%. Detailes are attached as spreadsheets. AES/DES3 with PE1746 Enabled have over 20% slowing down. . **Workaround:** None. If performance is critical, do not update at this time.
(LHSM-13408) Diminished performance after upgrading to 6.22.0 firmware.	H	**Problem**: After upgrading the firmware a Luna G5 to firmware 6.22.0, HSM performance is reduced. **Workaround**: Run the **ureset** utility (located in the Luna HSM client root directory) to reset the USB driver after performing the firmware upgrade.
LHSM-11637 Luna G5 performance slowing down arround 50% with ECC and ECDH, etc.	H	**Problem:** Comparing to release 5.4, Luna G5 release 6.0 performance numbers are reduced with: • RSA Encrypt/Decrypt • ECDSA • ECDH • ECIES • HMAC • ARIA • KCDSA **Workaround:** None. If performance is critical, do not update at this time.
(LHSM-8424 MKS190409) The PED client service does not start on Solaris 11 Sparc T-5120 server.	H	**Problem:** The PED client service from 32-bit binaries does not start on Solaris 11 Sparc T-5120 server. **Workaround:** None
(lHSM-8406 MKS190450) Client tools fail to detect Luna G5 on 'unplug and re-plug' operations.	H	**Problem:** When Luna G5 is unplugged and then re-plugged, the client tools fail to detect it on Dell R710, Sun Fire v245 and Sparc T-5120 servers. **Workaround:** None

Issue	Severity	Synopsis
(LHSM-5804 MKS180345 and 170626) change of PED related timeout setting requires pedclient restarting, which has impact on audit logging	H	**Problem:** While testing remote backup with a single Remote PED case, it was found that timeout happens during backing up. To complete a backup, pedtimeout3 value must increase in the configuration file. For the change to take effect, pedclient and the client application must be restarted. Because peclient is shared with audit logging, restarting has an impact on audit logging. Pedclient should pick up the change without restarting. **Workaround:** None. For Luna PCI-E, audit logging is affected when the restart is performed. In Luna SA, there is no provision to restart pedclient, and therefore no way to make a timeout change effective.
(LHSM-5797 MKS182827) Luna G5 HA autorecovery does not work	H	**Problem:** If you enable HA autorecovery on Luna G5, members of the HA group that go down might not be autorecovered when they come back online. **Workaround:** Do not use the autorecover feature. If one of your HA members goes down, restart your applications to manually restore the member.
LHSM-18312 Luna SA 6.0: STC with HA haonly and 1746 enabled in the client fails with (CKR_DATA_ LEN_RANGE) on C_EncryptInit	M	**Problem:** If HA-only is set, STC fails if you attempt to enable PE1746 usage. **Workaround:** When using STC, either avoid using HA-only, or avoid specifying PE1746.
LHSM-18310 'ped connect' doesn't work with G5Base FW 6.0.8 and 6.2.3	M	**Problem:** With Luna G5 having firmware 6.0.8 or 6.2.3, 'ped connect' command in lunacm returns No Error but the PED ID is set to 1. On the PedServer side, however, the "Client Information:" shows "Not Available".. **Workaround:** Update firmware to 6.10.x or newer.
LHSM-18302 STC Status command is displaying incorrect current key life value when executed in SO owned partition.	M	**Problem:** The STC key life, as shown by the STC status command is too small by several orders of magnitude. **Workaround:** None.
LHSM-18299 Confusing "hsm stc status" information for admin channel.	M	**Problem:** [sa97] lunash:>hsm changePo -po 39 -v 1 'hsm changePolicy' successful. Policy Allow Secure Trusted Channel is now set to value: 1 Command Result : 0 (Success) [sa97] lunash:>hsm stc status HSM STC: Enabled Enabled: No **Workaround:** Be aware that the first instance does not really deal with enabling, but rather with whether the policy is set or not, so "HSM STC: Enabled" should say "HSM STC: Allowed". The second "Enabled: No" is the STC admin channel turned on or off by command. We will try to make it less confusing in future.

Issue	Severity	Synopsis
LHSM-18289 Luna SA 6.0: STC keeps piling up tcp sessions even when client fails to see the token.	M	**Problem:** As a result of failed auto-recovery LHSM-18288, the appliance keeps piling up tcp sessions with stc. **Workaround:** None.
LHSM-18288 Luna SA 6.0: STC with HA and multiple groups now failed to recover after reboot of primary	M	**Problem:** HA with multiple groups will not work if using STC AND the HA members belong to the same set of appliances - basically, multiple partitions from the same Luna SA. **Workaround:** Wait before upgrading. OR Split your applications onto two client computers (so that only one HA group exists for each computer)
LHSM-18284 PKI bundle: device error when assigning Luna G5 bundle (firmware 6.0.8/6.21.0)	M	**Problem:** Setup is two Luna G5 bundles, one with firmware 6.22.0 and other one starting with firmware 6.0.8. Both are PED based. Predeploy, deploy and then assign to client. vtl listslot shows only one present (fw 6.22.0), and the other one not. Launch lunacm, got CKR_DEVICE_ERROR. Upgrade the non-working Luna G5 from firmware 6.0.8 to firmware 6.21.0, same behavior. Undeploy and redeploy, then assign again, and the older firmware Luna G5 is still not visible. **Workaround:** None.
LHSM-18283 pedclient relies on deprecated net-tools package	M	**Problem:** When installing the 6.0.0 LunaClient on a CentOS 7.1 system with a minimal install, the pedclient fails to start; the ifconfig and various other system commands have been deprecated and are not installed by default. **Workaround:** yum -y install net-tools
LHSM-18281 'token backup init' command failed due to LUNA_ RET_INVALID_ENTRY_TYPE	M	**Problem:** The first 'token backup init' command after 'token backup factoryReset' always fails with LUNA_RET_INVALID_ENTRY_ TYPE. However, the second 'token backup init' command succeeds. **Workaround:** Repeat the command.
LHSM-18280 LunaCM: *remotebackup start* cmd, crashes the lunacm	M	**Problem:** In LunaCM, running the remotebackup start command, crashes lunacm, leaving it in an indeterminate state. **Workaround:** Exit the command-prompt session, start another, and launch lunacm.
LHSM-18236 Luna SA 6.0: ha will not allow create or add of member if a role is already logged into the slot	M	**Problem:** If there is already a logged in session in the slot, HA create or add of member will fail. **Workaround:** Log out of the slot first.

Issue	Severity	Synopsis
LHSM-18231 Updating "Ignore Idle Connection Timeout" by 'pedClient mode config set' command changes "Idle Connection Timeout"	M	**Problem:** Attempting to to enable "Ignore Connection Time out" but the setting of "Idle Connection Timeout (seconds)" is updated instead. **Workaround:** Edit the config file manually (contact Technical Support).
LHSM-18230 CKR_FUNCTION_ FAILED for 'par crp -l user_PCI' command after PED has been switched from remote to local	M	**Problem:** 1. Initialize HSM. 2. Generate RPV. 3. Connect the Remote PED. Verify the connection via PedServer. 4. Initialize HSM and create a user partition. 5. Disconnect the Remote PED. Verify the [dis]connection via PedServer. 6. Initialize HSM and create a user partition. lunacm:>par crp -l user_PCI Please attend to the PED. Error in execution: CKR_FUNCTION_FAILED. Command Result : 0x6 (CKR_FUNCTION_FAILED) **Workaround:** Exit lunacm and relaunch lunacm.
LHSM-18229 Luna SA 6.0: on reboot of Luna SA, the Backup HSM is not detected,	M	**Problem:** ■Backup HSM attached directly into the appliance ■Reboot the Luna SA After reboot, the Backup HSM is not detected. **Workaround:** Restart the Luna Backup HSM, and it then reappears in LunaSH.
LHSM-18096 Remote PED does not work with Luna Backup HSM attached to a Luna SA	M	**Problem:** The PED for the Luna Backup HSM can be successfully disconnected, but when connecting to the Remote PED, gets 0X300207 (Unknown ResultCode value) error. **Workaround:** Update the Luna Backup HSM firmware to version 6.10.4.
LHSM-18063 "par ar contents/showcontents" displays wrong number at sff token and hangs	M	**Problem:** Create a legacy partition and setup ntls with a linux client. Use the same sff token, with command "par archive contents" in lunacm or "par archive showcontents" in lunash. Wrong number of objects is displayed and command hangs. **Workaround:** Unplug the eToken and the PED to terminate.
LHSM-18031 Cannot change legacy CU challenge when partition activation policy set	M	**Problem:**For PED-auth Luna SA, cannot change legacy CU challenge when partition activation policy is set. **Workaround:** Switch the activation policy off before changing the Crypto User challenge secret: lunash:>partition changepolicy -policy 22 -value 0 -partition mypar1 'partition changePolicy' successful. Policy "Allow activation" is now set to: 0

Issue	Severity	Synopsis
		Command Result : 0 (Success) lunash:>partition changepw -partition mypar1 -cu -oldpw /W5W4dLbAWKLGCxW -newpw cuserpin Luna PED operation required to activate partition on HSM - use User or Partition Owner (black) PED key. 'partition changePw' successful. lunash:>partition changepolicy -policy 22 -value 1 -partition mypar1
LHSM-17857 when installing CA Safenet provider options are not available after ksp registrations	M	**Problem:** Upon registration of ksp partitions using kspconfig.exe, a restart is sometimes necessary when installing your CA, as the Luna provider options for the cryptographic algorithms sometimes do not show up in the drop down menu without the restart. **Workaround:** Restart.
LHSM-17804 Luna SA 6.0: HA manual sync fails with 'ha sync -g <group>' if -password parameter is not used	M	**Problem:** HA manual sync fails if password parameter is not provided. **Workaround:** Provide the password at the command line.
LHSM-17800 LunaCM: Luna Backup HSM can be initialized only in the Local Luna HSM client, not the remote Luna HSM client.	M	**Problem:** Luna Backup HSM can be initialized only in its Local Luna HSM client, not a remote Luna HSM client. After the initialization is completed from the local client, the remote luna client still shows the unlabeled Luna Backup HSM. **Workaround:** Initialize the Backup HSM via the client computer to which it is physically connected.
LHSM-17755 and LHSM-14857 Lunacm "partition clone" logs out current user after successful OR unsuccessful operation.	M	**Problem:** After logging in CO and cloning objects, the CO is logged out of the current working slot for no apparent reason. **Workaround:** Log in again.
LHSM-17753 Sporadic failures with partition sff commands.	M	**Problem:** Various partition sff commands fail intermittently. **Workaround:** Retry command.
LHSM-17181 LunaCM: par ar r didn't handle properly with -replace option	M	**Problem:** 1. have couple of objects pre-created in the user partition 2. restore from backup with -replace option turned on 3. expecting the existing objects will be deleted, then replaced with the backup objects. 4. it turns out, the restore process just skips the existing objects without replacing them. **Workaround:** If in doubt, delete objects on the target partition before restoring from archive.
LHSM-16830 Remote backup server cannot connect to Remote PED when in external lunacm session	M	**Problem:** LunaClient connection to Luna SA on one computer and a Luna Remote Backup HSM with RBS session on a second computer. Assign the Backup HSM as a Remote Backup device for the Luna SA. First computer lunacm instance can now see both the

Issue	Severity	Synopsis
		Luna SA partition and the backup HSM. Attempting "ped connect" against the Backup HSM's slot via lunacm on the first computer fails. Running "ped connect" on the second computer FOR the Backup HSM connected to that computer, succeeds. **Workaround:** Use Luna PED locally connected to the Luna Backup HSM, or use a Luna Remote PED instance on the computer with the Backup HSM as the PED instance for both the Backup HSM and the distant Luna SA.
LHSM-16826 SNMP hsmClientPartitionAssignmentTable reports wrong partition serial numbers	M	**Problem:** Partition serial number format changed with Luna HSM 6.0 release, to accommodate PPSO and other changes, but SNMP appears to show older format in some cases. **Workaround:** Be aware that the serial numbers reported by SNMP might differ from the numbers reported by other Luna tools.
LHSM-16825 Lunacm: partition archive backup -slot remote does not work	M	**Problem:** "partition archive backup -slot remote" command returns " (invalid arguments)" error, regardless of options that are provided. **Workaround:** None.
LHSM-16388 Luna SA 6.0: STC lunash does not find partition with spaces in the name on client register	M	**Problem:** STC client register operation does not work when partition name contains spaces. **Workaround:** Avoid partition names that contain spaces.
LHSM-16315 HA: ha sync up with PKI bundle not performed with two members one having 0 objects.	M	**Problem:** 1. Pre-deploy, then deploy Luna G5s, have two Luna G5s from each Luna SA 2. Assign each G5 bundle to the same client 3. From client, create HA group using both partitions from PKI bundles. 4. Create some objects in one HA member and leave the other one with 0 objects in it. 5. Order synchronization of the objects within the HA group, get "No synchronization performed/needed". 6. Remove the 0 object member from HA group and add it back in, then attempt sync again. Same result, "no sync performed". **Workaround:** None. HA is not working for PKI bundle.
LHSM-16311 When enable bonding false negative error message	M	**Problem:** When port bonding is enabled, the dialog returns an error like: Error adding address 172.20.10.179 for bond0. **Workaround:** Ignore. Bonding is successful, despite the spurious error.
LHSM-16289 Luna SA 6.0: STC lunacm seg faults on migrate from	M	**Problem:** Lunacm sometimes segfaults on migrating from ntls to stc when using the stc enable on a 2nd slot. Setup:

Issue	Severity	Synopsis
ntls to stc with 'stc enable'		■ Client has 2 partitions each from a different Luna SA ■ Client is currently NTLS connected to both Luna SAs. ■ Exchanged public keys to switch to STC ■ 'stc enable' on 1st slot seems ok ■ 'stc enable' on 2nd slot exits out of lunacm . **Workaround:** Relaunch lunacm and try again.
LHSM-16238 PKI bundle: token pki resetPin failed with creating challenge	M	**Problem:** For Luna G5s connected to Luna SA: FW 6.22.0 - has the challenge created in the PED screen, but after pressing Enter on the PED, got message "Failed to create new challenge!" in the lunash. FW 6.2.4 - failed the resetPin right away without displaying the new challenge in the PED. . **Workaround:** If necessary to change the challenge secret on a PKI bundle Luna G5, temporarily attach the Luna G5 to a LunaClient host computer, perform the operation in lunacm, and then return the Luna G5 to the Luna SA.
LHSM-16237 partition backup append replace does not work	M	**Problem:** Backing up a partition to Luna G5 and then attempting to back it up again to the same partition with the append and replace options, no items are backed up, they are just skipped. **Workaround:** Avoid using the "append" and "replace" options in the same command.
LHSM-15991 PKI bundle: Failed to deploy token pki on FW 6.10.1	M	**Problem:** 1. Predeployed the Luna G5 with FW 6.10.1 2. Performed the changepin operation 3. Deploy fails with "Can not locate the token". **Workaround:** None.
LHSM-15975 PKI bundle: token active failed in lunash after deactive from luna client	M	**Problem:** On Luna SA 6.0, with attached Luna G5 having f/w 6.22.0: 1. Assigned the PKI token (the Luna G5) to client 2. Deactivated the token 3. When activated from lunash, failed with error code 65535. **Workaround:** None. But the activation from lunash was observed to work for firmware 6.2.4
LHSM-15964 Luna SA 6.0: sysconf config factoryReset complains of 'hsm[4411]: Unable to locate client token library configured in 'ClientTokenLib' if STC enabled	M	**Problem:** With STC enabled, perform a "sysconf config factoryReset -s all -f" lunash does not see the hsm. **Workaround:** Restore previous configuration with lunash:>sysconf config restore -s all -fi <config filename>.tar.gz.
LHSM-15960 "sysc ssh device eth1" hung on bonded NIC (PED-	M	**Problem:** On a PED-authenticated Luna SA with bonded Ethernet ports, run "sysconf ssh device eth1". The command hangs, with no

Issue	Severity	Synopsis
auth Luna SA)		return. **Workaround:** Close the SSH terminal session and start again.
LHSM-15417 PKI bundle: token pki update capability broken	M	**Problem:** The command 'token pki update capability' is broken, returning RC_FILE_ERROR. **Workaround:** Disconnect the Luna G5 from the Luna SA appliance, and connect to a LunaClient computer. Use lunacm to apply the capability update. Return the updated Luna G5 to its place connected to the Luna SA appliance for PKI Bundle operation.
LHSM-15017 'sysconf regenCert' returns 'ERROR. Partition named "Cryptoki User" not found'	M	**Problem:** When running an ordinary 'sysconf RegenCert' the dialog talks about being unable to find Cryptoki User partition, which would be expected if running a 'sysconf hwregencert'. **Workaround:** Ignore.
LHSM-14848 hsm init from lunacm on a PED-auth HSM should warn when password and domain are provided	M	**Problem:** For a PED-authenticated Luna HSM with older firmware, if you offer a password or domain when initializing, you are told that they are being ignored. On a PED-authenticated HSM with firmware 6.22.0, if both pw and domain are provided, the initialization just works, but without notifying about ignored parameters. However, if an unnecessary password is provided, but the unnecessary domain is not provided, the command simply fails. It should not. **Workaround:** When initializing a PED-authenticated Luna HSM with lunacm:> hsm init, DO NOT provide password, domain, or default domain. Simply run the command "hsm init -label <some label>" and respond to the Luna PED prompts.
LHSM-14761 CKR_DEVICE_ ERROR during RC4 key gen	M	**Problem:** Key gen (CKM_RC4_KEY_GEN) fails with a CKR_ DEVICE_ERROR and renders the HSM unresponsive. The same HSM/test combination ran for weeks without issue. **Workaround:** Restart the HSM. This is a very rare occurrence, and a fix is being tested.
LHSM-14333 Luna SA 6.0: HA using java does not recover and does not terminate/clean up session	M	**Problem:**Setup: Two Luna SA appliances 1. Java with HA HAOnly 2. Run jMultitoken 3. Shut down the interface of 1 member 4. After four attempts at recovering, restart the interface (notice the error code of 0xC0000102 5. After reaching max retries, perform manual recover The client sets up a session with the appliance but HA is never recovered. **Workaround:** Reboot.

Issue	Severity	Synopsis
(LHSM-13949) Long pauses (5 minutes) during SFF restore of existing objects	M	**Problem:** When restoring existing objects from an SFF token to an SA partition, existing objects are found and skipped, as expected, every 5-6 seconds or so. However, on occasion, there may be a lengthy pause (5 minutes or so), between objects. **Workaround:** None. If you notice a pause, please be patient.
LHSM-13421 Changing logpath of audit log while services stopped causes Luna G5 to not respond when services restarted	M	**Problem:**Logged in as the Auditor, set log level to log nothing. Stopped the luna client services - HTL, SNMP, PED Server. Renamed the "logtest" directory to something else. Restarted the 3 services stopped earlier. At this point the Luna G5 froze with its green light on. I couldn't get it back to life without a ureset. Definitely an unlikely edge case, but interesting. **Workaround:** Perform ureset to get Luna G5 going again.
LHSM-12575 Running ssh lush commands immediately after port bonding forces bonding in Fault-Tolerance	M	**Problem:**Calling any lunash commands immediately after bonding enable or disable causes bonding to go into Fault-Tolerance mode causing unexpected behavior. **Workaround:** None.
LHSM-11659 First hsm login after tamper is ignored	M	**Problem:**Tamper a Luna SA. Reboot. Perform hsm login - I and get "success" from lunash. Note that the hsm still isn't really logged in, and requires a second login before I can do things that require SO authentication. **Workaround:** After a tamper event, perform 'hsm login' twice.
(LHSM-10615) KSP does not record success messages	M	**Problem:** KSP is only logging failures. It should also record successes, for auditing purposes. **Workaround:** None.
(LHSM-10594) KSP unable to set usage limits	M	**Problem:** kspcmd.exe has an option to specify a usage limit. The command appears to work and generates a registry entry that sets the limit specified for any key created via KSP (i.e. CA, etc.). However, when keys/certs are created via CA, the KSP log records error CKR_ATTRIBUTE_TYPE_INVALID. Reviewing the keys attributes in ckdemo does not show attributes CKA_USAGE_LIMIT or CKA_USAGE_COUNT. Without these set, the keys can be used an infinite number of times. **Workaround:** After creating your CA, or after every renewal, launch ckdemo and manually add the usage limit attribute.
(LHSM-10162) No way to put Luna Backup HSM into FIPS approved operation mode on Luna SA	M	**Problem:** Luna Backup HSM with firmware 6.10.2 is undergoing FIPS evaluation. To conform to FIPS evaluation, it must be used in FIPS approved operation mode. By default this HSM policy is OFF. There is no way

Issue	Severity	Synopsis
		to turn it on via lunash. **Workaround:** Connect the Backup HSM to a standalone host computer and use lunacm to change the policy, then reconnect the Backup HSM to the Luna SA. Or perform remote backup.
(LHSM-10161) token backup show needs to show whether Backup HSM is in FIPS approved mode or not	M	**Problem:** Luna Backup HSM with f/w 6.10.2 is undergoing FIPS evaluation. To conform to FIPS requirements, it must be used in FIPS approved operation mode and there must be a way to visually confirm this configuration. There is no way via Lunash to query whether this HSM policy is on or off for a Luna Backup HSM. **Workaround:** Connect the Backup HSM to a standalone host computer and use lunacm to view the status, then (if acceptable) reconnect the Backup HSM to the Luna SA. Or perform remote backup.
(LHSM-10160) Attempt to backup to non-existent partition on Backup HSM gives warning but no way to back out	M	**Problem:** Attempting to perform a backup with "replace" option to a partition on the Luna Backup HSM that does not exist, Lunash prompts with a warning, but then gives no opportunity to back out of the command: [192.20.9.127] lunash:>partition backup -partition John1 -password userpin -serial 7000627 -replace -tokenpar Warning: 'replace' mode specified, but no partition named FIPSBackup exists on the backup token. A new partition will be created. Warning: You will need to connect Luna PED to the Luna Backup HSM to complete this operation. You may use the same Luna PED that you used for Luna SA. Please type 'proceed' and hit <enter> when you are ready to proceed> quit Please type 'proceed' and hit <enter> **Workaround:** Close the session, open a new SSH session to the Luna appliance, login to the HSM and try the backup again with a correct, existing partition name.
(LHSM-10152) windows Client – lunacm : Cannot load library	M	**Problem:** After installing Luna Client on windows server 2008 RC2, tried to run lunacm. Got "Cannot load library: The specified module could not be found". **Workaround:** Open a new console/command-line window to allow the library path to be found.
(LHSM-9888) User's lushfiles directory is gone after sysconf backup/restore	M	**Problem:** Steps to reproduce: 1) Create a new user (somebody). 2) Run sysconf config backup 3) Run sysconf config factoryReset

Issue	Severity	Synopsis
		4) Run sysconf config restore <backup file in step 2> 5) Login to appliance as "somebody", run "my file list" will get the following error. [local_host] lunash:>my file list /bin/ls: /home/somebody/lush_files: No such file or directory Command Result : 0 (Success) **Workaround:** Recreate the named user. Re-upload any files that were lost.
(LHSM-9846) sysconf secureKeys broken for PWD-AUTH LunaSA	M	**Problem:** The command to move software NTLS keys into hardware is broken on password-authenticatedLuna SA. Works properly for PED-authenticated Luna SA. **Workaround:** If you prefer to use NTLS keys in hardware (inside the HSM, rather than on the Luna SA file system), then for PED-auth use the command options to generate them there, rather than generating in software and importing.
(LHSM-9818) lunacm "partition archive backup -o" does not read object handles correctly	M	**Problem:** "partition archive backup –o" does not read the object handles correctly, when a single invalid handle is passed to "-o"; it just backs up everything found from Luna SA to etoken. If multiple invalid object handles are passed, it works correctly. **Workaround:** Be aware of the discrepancy… and avoid passing invalid object handles.
(LHSM-9750) Small form-factor backup with Remote PED going to wrong PED	M	**Problem:** When a Remote PED has been specified at the Luna SA via lunash commands, and then a different Remote PED is specified (for that Luna SA) via lunacm commands, the setting from lunash prevails. This could result in unexpected results when setting up Remote PED and remote Small Form-factor Backup. 1- Connect Luna SA to a Remote PED by issuing "hsm ped connect" from lunash. 2- From lunacm, run "ped connect" to connect to your Remote PED 3- then run "par login" No prompt is presented at your Remote PED. Following a timeout period one of the following might occur: "Command Result : 0x8000002e (CKR_PED_UNPLUGGED)" lunacm:>par login Option -password was not supplied. It is required. Enter the password: ******* Please attend to the PED. Command Result : 0x8000002e (CKR_PED_UNPLUGGED) --> If the PED device to which the Luna SA goes is not connected. OR Command Result : 0x80000024 (CKR_TIMEOUT) --> If the PED

Issue	Severity	Synopsis
		prompt went to a PED other than yours and nobody inserted the expected black key and pressed <ENTER>. **Workaround:** For Remote PED authentication or remote Small Form-factor Backup of Luna SA, first run "hsm ped disconnect" from lunash, then run "ped connect and perform Small Form-factor Backup (or other PED-using operations) from lunacm.
(LHSM- 9712) PED SCP communication problem	M	**Problem:** Occasional errors or timeout occurred during local-PED data transfers (using SCP connection). This was probably always present, but went unnoticed during authentication operations due to the small data transactions. However, when PED is used in local mode for lengthy transactions, such as occur in SFF backup and restore operations, the instability is revealed. **Workaround:** Use Remote PED SFF backup when backing up and restoring larger amounts of partition data. (Remote PED SFF backup operations have proven reliable over a reliable network.)
(LHSM-8423, MKS190597) System is rebooted on issuing **hsm reset** command when running HA on Solaris Sparc 11 Netra T5440.	M	**Problem:** System gets rebooted when **hsm reset** command is issued on a G5 HA, running Solaris Sparc 11 (64-bit) Netra T5440 server. **Workaround:** It is recommended to stop any running applications before issuing **hsm reset** command in lunacm.
(LHSM-7696 MKS190048) RBS host app crashes on access when Luna Backup HSM removed	M	**Problem:** If a Luna Remote Backup HSM is removed from its host after the RBS daemon is running, the RBS app will crash on attempted access. Scenario 1: - have running RBS daemon with Backup HSM connected, have remote host configured to use RBS - power-off or remove USB cable from Backup HSM - launch lunacm on remote host; RBS daemon will crash Scenario 2: - have running RBS daemon with Backup HSM connected, have remote host configured to use RBS - launch lunacm on remote host - power-off or remove USB cable from Backup HSM - run remote backup; RBS daemon will crash **Workaround:** The Backup HSM must be connected to the host computer to get the RBS daemon running, and RBS must be stopped before you disconnect the USB cable or power-off the Luna Backup HSM.
(LHSM-7052/2863) Auto and manual recovery conflict during recovery	M	**Problem:** When a system is configured for auto-recovery, running the manual vtl haAdmin recovery option causes errors randomly. **Workaround:** Avoid manual recovery when system is configured for HA auto-recovery.

Issue	Severity	Synopsis
LHSM-5812 Crypto-User cannot create objects when using an HA group (MKS #176840)	M	**Problem:** Firmware allows only Crypto-Officer to clone objects. Currently, Crypto-User is not allowed to do cloning The HA logic for object creation is to create on the primary and then propagate (using the cloning operation) to other members. **Workaround:** Use Crypto Officer when using HA.
(LHSM-5768) Windows installer - when modifying existing Luna Client, extra selected components are not installed	M	**Problem:** When trying to modify an already-installed Luna Client on Windows we have the option to select any extra component we want, but the selected additional components are not actually installed. The installer gives no error message. **Workaround:** When modifying an existing installed Luna Client, on Windows, choose to install a Luna Product and ALL its sub-features. THEN deselect any that are not needed, and the remaining desired files are installed correctly.
(LHSM-2864) HA Key gens do not recover properly when recovering the primary.	M	**Problem:** In an HA environment, configure for auto-recovery. Launch multitoken with 10 threads performing key gens Fail the secondary and recover - everything works. Fail the primary - it switches over to do the key gens on the secondary. Recover the primary and wait; the app fails with CKR_CANCEL **Workaround:** None. Can be avoided if you do not have multiple clients connected to the HA slot.
LHSM-18062 lunash "partition sff showcontent" output not giving full command	L	**Problem:** lunash command "partition sff showcontent" output "'partition sff sho' successful.", should readback the full command "partition sff showcontent" rather than the short form. **Workaround:** Cosmetic; ignore.
(LHSM-10633) Luna Client on Debian requires libcryptoki library purge to reset to the default Chrystoki.conf version on uninstall	L	**Problem:** In some instances, it might be desirable to perform a complete re-install of the Luna HSM client, including replacing the current Chrystoki.conf file with the default version. Doing this on a Debian OS requires, after uninstalling the client, that the libcryptoki library be purged before the Chrystoki.conf.debsave backup file is deleted. **Workaround:** Workaround: To re-install the Luna HSM client with the default Chrystoki.conf file on a Debian OS 1Uninstall the Luna HSM client: /usr/safenet/lunaclient/bin/uninstall.sh 2Purge the libcryptoki library: dpkg -P libcryptoki 3Delete the backup Chrystoki.conf file: rm /etc/Chrystoki.conf.debsave

Issue	Severity	Synopsis
		4Re-install the Luna HSM client: <path>/install.sh
(LHSM-10163) SFF remote backup - Unknown Command Displayed on PED	L	**Problem:** During SFF backup over Remote PED, "Unknown Command" is observed on the PED followed by "Get Version". This should be a message like "write to token..." **Workaround:** Ignore.
(LHSM-10154) "cmu selfsign" fails to display key handler for new generated key	L	**Problem:** Running "cmu selfsign" ends with generating a key. If the command runs successfully, cmu is expected to display the new generated key handler, but it does not. **Workaround:** Issue "cmu list" to verify that the new key has been created.
(LHSM-10153) windows Client - cmu importkey gives wrong error message	L	**Problem:** The cmu utility returns "Buffer too small" instead of "wrong password" against "cmu importkey" cmd. **Workaround:** Be aware that the message is wrong, and re-try with the correct password.
(LHSM-9889) User loses pub key authentication after sysconf backup/restore	L	**Problem:** After: 1) Run sysconf config backup 2) Run sysconf config factoryReset any existing named user is no longer able to log in with public key authentication. **Workaround:** Recreate the named user (see issue LHSM-9888). Upload a public key and re-establish public key authentication for each such user.
(LHSM-9816) All other crypto ops to same HSM halt during init phase of SFF backup, recover slightly during object backup phase	L	**Problem:** When performing any kind of multitoken cryptographic operation, and a Small Form Factor Backup operation is started on the same HSM, all other cryptographic operation ceases during the eToken initialization phase of the operation. This can take 2-3 minutes. After the eToken initialization stage, crypto operations recover somewhat, but not to full speed, until backup completes. **Workaround:** Simply be aware that Luna PED operations and prompting have always blocked crypto operations on the attached HSM, and this continues with PED-mediated Small Form Factor Backup.
(LHSM-9681) Incorrect error when attempting to backup symmetric keys with symmetric SFF turned off.	L	**Problem:** Attempted to back up 2 symmetric keys with SFF symmetric policy turned off for the partition. The objects did not backup, but an overall message said success backing up 2 objects. lunacm:> par archive backup -slot eToken -label G5Backup WARNING: continuing the backup operation will wipe out all keys on the backup token! Are you sure you wish to continue? Type 'proceed' to continue, or 'quit' to quit now -> proceed

Issue	Severity	Synopsis
		Operation in progress, please wait. (1/2): Backing up object with handle 22... Failure (2/2): Backing up object with handle 25... Failure WARNING: Errors occurred while backup up one or more keys. Backup Complete. 2 objects have been backed up to partition G5Backup on the backup device Command Result : 0x63 (CKR_KEY_TYPE_INCONSISTENT) lunacm:> If some objects do not backup due to policy settings, a better message should be presented, such as "Some or all objects failed to backup due to policy restrictions on the current partition" or similar. This should replace the current bad grammar warning: "WARNING: Errors occurred while backup up one or more keys." **Workaround:** Ignore messages like "2 objects have been backed up to partition" when other messages indicate individual failures.
(LHSM-6986) Warning from install script on Debian 6/64 client install	L	**Problem:** During the full client install this warning/error appeared: Unpacking lunajmt (from lunajmt_5.3.0-9_amd64.deb) ... Setting up lunajmt (5.3.0-9) ... Adding new version of lunajcprov /usr/safenet/lunaclient/debian_pkgs Use of uninitialized value $postinst in length at /usr/share/perl5/Alien/Package/Deb.pm line 741. **Workaround:** The error appears to be a harmless coding issue in /usr/share/perl5/Alien/Package/Deb.pm which comes with the alien package. Ignore the message.
(LHSM-6945 MKS160706) Handling of PEDId parameter is inconsistent or confusing	L	**Problem:** Currently, whether an application uses the remote or the local PED is determined by the existence of the PEDId=[0|1] parameter in the 'Luna' section of Crystoki.conf. If this parameter does not exist, applications will always try to use the local PED, even if one is not attached. There is currently no way of setting this through any of the applications (lunacm or ckdemo), so the user must manually edit this file - not a preferred method. Lunacm, ckdemo, and multitoken all allow the user to specify the PED id, either on the command line or via a menu selection, but this works only for one specific session in the given application. Also, commands initrpv and deleterpv are executed only on a locally-attached PED. However, the applications which invoke these functions will simply use whatever PED id is currently specified for that session (or the default from Crystoki.conf). So these commands might incorrectly attempt to invoke a remote PED. **Workaround:** Modify the configuration file, or specify at the command line for each instance.

Resolved Issues

This section lists the issues known to exist in the product at the time of release. The following table defines the severity 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.

List of Resolved Issues

Issue	Severity	Synopsis
(LHSM-14232) Corrupt IV for AES-CTR	H	**Problem:** The AES-CTR mechanism incorrectly encrypts multi-part operations on the HSM (single-part operations are fine). The multi-part operation succeeds and data is encrypted. But the wrong IV gets used for second and subsequent updates in the multi-part operation. The encrypted data can later be decrypted by the HSM. However, the encrypted data cannot be decrypted by non-Gemalto HSMs that support the AES-CTR mechanism. This issue applies to Luna SA and Luna PCI-E only. It does not occur on Luna G5. **Resolution:** This issue is fixed in firmware 6.22.0. Decrypt data previously encrypted, upgrade the firmware to 6.22.0 and re-encrypt the data.
(LHSM-11879) CKR_ DEVICE_ERROR with AES GCM	M	**Problem:** If you use an AES key for a GCM operation with an AAD (additional authentication data) length that is a multiple of 4-bytes, and later use the same key for another GCM operation with an AAD length that is not a multiple of 4 bytes, the HSM will halt. This issue applies to Luna SA and Luna PCI-E only. It does not occur on Luna G5. **Resolution:** This issue is fixed in firmware 6.22.0 and Multitoken.
(LHSM-10592) LunaClient Windows services dependency on printer service	H	**Problem:** It was found that several LunaClient services, on Windows platforms, depend on print “Spooler” services. That dependency should be removed. **Resolution:** Printer service "Spooler" dependency is now removed from all LunaClient services on Windows.
(LHSM-10583) MS-CSP to LunaKSP migration incomplete	M	**Problem:** the KSP version of ms2luna migrates keys, but does not change the proper pointers for SafeNet to take over; if applications are stopped they might not restart, complaining that they can no longer find the private key for the certificate. Steps to reproduce: • create a software CA

Issue	Severity	Synopsis
		• Install/configure base Luna HSM client, • register partition via KSP • run ms2luna and provide the thumbprint of the cert that the CA is using • verify that keys have been copied to HSM • in CA Management see what provider is being used – it shows that the Microsoft RSA Provider (or whatever was selected) is still in use • stop/restart the CA – this fails and generates an error. **Resolution:** This issue is fixed in release 6.0.
(LHSM-9418) Luna JavaDocs missing documentation for LunaSlotManager.reinitialize() method	M	**Problem:** Some Javadoc entries that are available in Linux are not found when LunaClient 5.4.1/5.4.2 is installed on Windows. **Resolution:** Fixed in Luna HSM 6.0.
(LHSM-9817) multitoken errors with rsa operations in FIPS mode	M	**Problem:** multitoken generates an error when attempting RSA 2048 or RSA 4096 sigver against an HSM in FIPS approved operation mode. Due to FIPS restrictions on data size, smaller sizes are refused when the HSM is in FIPS mode. However, 2048 is the new minimum size and should have been accepted by multitoken. **Resolution:** This is expected behavior due to the new FIPS-compliance changes that were enacted in Luna HSM release 5.4.
(LHSM-6864) Client: not all tools work when 32bit lib used on windows 64bit OS	M	**Problem:** With this release, we provide only the 32bit library on windows 64bit OS to support customer's 32bit app in windows 64bits OS; we do not support our tools - like lunacm, vtl etc.. **Resolution:** Installation documentation updated.
(LHSM-5827) pedserver cannot be started due to "LOGGER_init failed"	M	**Problem:** Occasionally pedserver can fail stop/start with message. PedServer.exe mode start LOGGER_init failed Failed to initialize the logger. Exiting **Resolution:** Instructions now emphasize that pedserver.exe must run in an Administrator Command Prompt, and will fail if run in a non-Administrator command session.
(LHSM-5811, MKS#176989) lunacm and ckdemo display negative numbers for HA slot	M	**Problem:** With command lunacm:>ha list HA Group Number displays a negative number. However command "slot list" displays a proper number for HSM Serial Number In ckdemo choose option (11) Slot Info, then select an HA Virtual Card Slot, no serial number information displayed for group or member. However option (12) Token Info has more details about the slot. **Resolution:** Fixed.

Issue	Severity	Synopsis
(LHSM-5793) appliance: "err Luna PED Client[2228]: error : 0 : Error scanning log files"	M	**Problem:** Seeing "err Luna PED Client[2228]: error : 0 : Error scanning log files", and all logs remain in HSM and are not transferred to host. **Resolution:** Fixed in Luna HSM 6.0.
(LHSM-14005) Local PED communication protocol not designed for backups larger than 10 kbits.	H	**Problem:** The local PED uses a communication protocol that was not designed to carry the large amounts of data required to perform some SFF backup operations. **Resolution:** SFF Backup documentation amended to recommend using Remote PED.
(LHSM-9737) eToken objects number wrong after power loss at pedserver	M	**Problem:** During Small Form Factor backup, if power outage or machine reboot occurs at pedserver host, backup fails with "device error". If eToken contents are checked, output shows a huge number objects obviously not correct: lunacm:>par ar c -s etoken Listing all objects... Found 412316860869 backup objects: Partition: etoken_bck Object Type: Partition Object UID: 6b00000c48180000ee5a0200 backup failure (14231/14232): Backing up object with handle 14322... Failure (CKR_DEVICE_ERROR) (14232/14232): Backing up object with handle 11817... Failure (CKR_DEVICE_ERROR) ... Backup Complete. 14232 objects have been backed up to partition etoken_bck **Resolution:** Fixed in Luna HSM 6.0.
(LHSM-10540) SNMP: Subagent fails to automatically reconnect when Service's restart subcommand is used	M	**Problem:** When restart is issued, the NET-SNMP subagent loses its connection when the snmp service stops; as it should. -However it does not reconnect once the service is back up. **Resolution:** Fixed in Luna HSM 6.0.
(LHSM-10174) Add ECDSA to "my public-key list"	M	**Problem:** "my public-key list" does not show the ECDSA fingerprint. Steps to reproduce. 1) On a linux client with openssh6.2 that supports ECDSA, generate ECDSA key pair "ssh-keygen -q -t ecdsa -f id_ecdsa -N "" " 2) Copy the ecdsa pub key to SA appliance. 3) Add the key "my public-key add id_ecdsa.pub" 4) Try ssh access the SA using the ecdsa key and it is successful. -sh-3.2# ssh admin@172.20.9.62 -i id_ecdsa Last login: Mon Feb 3 10:06:26 2014 from 172.20.9.61

Issue	Severity	Synopsis
		Luna SA 5.4.1-1 Command Line Shell - Copyright (c) 2001-2014 SafeNet, Inc. All rights reserved. [local_host] lunash:>exit 5) Run "my public-key list", the ecdsa key is not displayed **Resolution:** Fixed in Luna HSM 6.0.
(LHSM-10109) "hsm driver timeout set" doesn't display error when no value passed in	M	**Problem:** In Luna SA, from lunash command line, run "hsm driver timeout set" without including a value; lunash shows 'success' and no error message. Example: [myluna] lunash:>hsm driver timeout set Command Result : 0 (Success). **Resolution:** Fixed in Luna HSM 6.0.
(LHSM-9883) Lunash fails to shut down certmonitord service	L	**Problem:** Command "ntls certificate monitor disable" in lunashshows that cert monitor was disabled, but in fact the command failed to shut down certmonitord service. **Resolution:** Fixed in Luna HSM 6.0.
(LHSM-9820) Package listfile displays all packages	L	**Problem:** The command “package listf” should return only uploaded-but-not-yet-installed packages, but successfully installed packages are shown as well. **Resolution:** Fixed in Luna HSM 6.0.
(LHSM-6856) appliance: status of "HSM Admin login attempts left" in hsm show command shows incorrectly after three consecutive hsm login failures	M	**Problem:** After three consecutive hsm login failures, "HSM Admin login attempts left" in output of hsm show command still shows "1 before HSM zeroization!" while the HSM has been zeroized. It should show "hsm zeroized". **Resolution:** Fixed in Luna HSM 6.0.
(LHSM-5824, MKS161028) unmasking has been set as disallowed after migrating Luna SA from 5.0	M	**Problem:**After migrating a Luna SA from version 5.0, found that unmasking in HSM policy has been set as disallowed which potentially blocks key migration from a SIM configuration. This is a very rare case and requires a destructive capability/policy change; a general solution is not contemplated, due to the small number of customers potentially affected. **Resolution:** Fixed in Luna HSM 6.0.
LUC-630	M	**Problem**: On updating firmware for G5, a Device Error is returned. However, the firmware is found to be updated after reboot. **Resolution:** Fixed in Luna HSM 6.0.

Support Contacts

Contact method	Contact
Address	SafeNet, Inc.

Contact method	Contact	
	4690 Millennium Drive Belcamp, Maryland 21017 USA	
Phone	Global	+1 410-931-7520
	Australia	1800.020.183
	China	(86) 10 8851 9191
	France	0825 341000
	Germany	01803 7246269
	India	000.800.100.4290
	Netherlands	0800.022.2996
	New Zealand	0800.440.359
	Portugal	800.1302.029
	Singapore	800.863.499
	Spain	900.938.717
	Sweden	020.791.028
	Switzerland	0800.564.849
	United Kingdom	0800.056.3158
	United States	(800) 545-6608
Web	www.safenet-inc.com	
Support and Downloads	www.safenet-inc.com/support Provides access to the SafeNet Knowledge Base and quick downloads for various products.	
Technical Support Customer Portal	https://serviceportal.safenet-inc.com Existing customers with a Technical Support Customer Portal account can log in to manage incidents, get the latest software upgrades, and access the SafeNet Knowledge Base.	

