Luna HSM 5.4.7

CUSTOMER RELEASE NOTES

Document part number: 007-012225-003 Rev J
Release notes issued on: 20 November 2015

The most up-to-date version of this document is at:
http://www.securedbysafenet.com/releasenotes/luna/crn_luna_hsm_5-4.pdf

Contents

Product Description

The Luna 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, Luna HSMs provide robust protection for your secure transactions, identities, and applications. They also offer high-performance encryption, decryption, authentication, and digital signing services. Luna HSMs are available in the following form factors which offer multiple levels of performance and functionality:

Luna SA

Luna SA a network-based, Ethernet-attached HSM appliance that offers up to 20 HSM partitions, high-availability configuration options, remote 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, and are otherwise functionally identical.

Luna PCI-E

Luna PCI-E is an internal 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, and are otherwise functionally identical.

Luna G5

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

Release Description

This CRN addresses Luna HSM 5.4.x releases. How you upgrade depends on your operating system. See “Upgrade Paths” on page 7 for more information. Luna HSM 5.4.x is “update only”, meaning that Luna HSM products continue to be shipped from the factory at version 5.2.3, and you have the option to update the software and firmware to version 5.4.x.

Luna HSM 5.4 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, 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.

Luna HSM 5.4.7

Luna HSM 5.4.7 is a Luna SA-only release, 630-010165-024, which includes the previous 5.4.x releases and patches, as well as firmware 6.21.0.

BASH-related vulnerabilities addressed

In light of the recent BASH-related vulnerabilities (known as Shellshock/Aftershock/Bashdoor) covered within CVE-2014-6271, CVE-2014-6277, CVE-2014-6278, CVE-2014-7169, CVE-2014-7186, and CVE-2014-7187, SafeNet has developed and tested Luna SA software updates to address all of the listed vulnerabilities. Other Luna products do not use BASH and are not affected. See HSMAN-125 in the Luna SA Addressed Issues table.

NTLS lockout (intermittent shutdown)

This release also fixes an issue where NTLS would intermittently stop after days of client application traffic. See LHSM-12955 in the Luna SA Addressed Issues table.

Luna HSM 5.4.6

Limited release.

Luna HSM 5.4.5

Limited release.

Luna HSM 5.4.4

Luna HSM 5.4.4 is a Luna SA-only release, 630-010165-021, which includes the previous 5.4.x releases and patches, as well as firmware 6.21.0.

Fixing BASH-related vulnerabilities

In light of the recent BASH-related vulnerabilities (known as Shellshock/Aftershock/Bashdoor) covered within CVE-2014-6271, CVE-2014-6277, CVE-2014-6278, CVE-2014-7169, CVE-2014-7186, and CVE-2014-7187,

SafeNet has developed and tested Luna SA software updates to address all of the listed vulnerabilities. Other Luna products do not use BASH and are not affected. See HSMAN-125 in the Luna SA Addressed Issues table.

Luna HSM 5.4.3

Luna HSM 5.4.3 was a patch for Luna SA only, addressing OpenSSL vulnerability (http://www.openssl.org/news/secadv_20140605.txt). For more info see SafeNet Security Bulletin 140605-1 'SSL/TLS MITM Vulnerability with SafeNet Luna SA'.

Luna HSM 5.4.2

Luna HSM 5.4.2 solves a problem discovered in Luna SA 5.4.1 where C_Login was taking significantly longer than in previous releases, having an impact on the performance of short-lived applications.

Windows/Linux/Solaris

On Windows, Linux, and Solaris, Luna HSM 5.4.2 consists of a client patch (630-010370-001) and an appliance patch (630-010165-015) that are installed on top of Luna HSM 5.4.1.

HP-UX/AIX

On HP-UX and AIX, Luna HSM 5.4.2 is a single consolidated package that includes client software (5.4.2), appliance software (5.4.1), and HSM firmware for all models of the Luna SA, Luna PCI, and Luna G5 HSMs.

> **Note** Luna HSM 5.4.2 does not include the 5.4.2 appliance patch (630-010165-015). You must install the appliance patch separately.
> UPDATE: See Luna SA 5.4.7 which includes all the previous 5.4.x releases and patches.

Luna HSM 5.4.1

Luna HSM 5.4.1 replaces Luna HSM 5.4.0, which is no longer available. It fixes a vulnerability in OpenSSL (CVE-2014-0160 - TLS heartbeat read overrun).

Windows/Linux/Solaris

Luna HSM 5.4.1 is a single consolidated package for Windows, Linux, and Solaris that includes client software, appliance software, and HSM firmware for all models of the Luna SA, Luna PCI, and Luna G5 HSMs. Luna HSM 5.4.1 is "update only", meaning that Luna HSM products continue to be shipped from the factory at version 5.2.3, and you have the option to update the software and firmware to version 5.4.1.

New Features and Enhancements

Luna HSM 5.4.x introduces some new features and improvements, as follows:

Features that do not require HSM firmware 6.21.0

Improved Remote Management

The default IP address and port for Remote PED are configurable through the lunacm utility.

Remote PED function has been adjusted to work reliably over VPN connections.

Configurable SO Authorization Requirement for Luna SA Admin Operations

A "forceSOlogin" option now allows the Luna SA HSM Security Officer to optionally enforce that the SO must be logged in when certain sysconf, ntls, htl, and client commands are run.

Improved Product Documents

Both HTML/Web and PDF versions of Luna documentation are provided, with a combined navigation page to search or browse in either format, and to view or download individual component documents as separate PDF files. Enhanced monitoring and logging information is included.

Configurable Luna SA Banner

The session-start banner text that appears at the beginning of each new Luna SA SSH session is configurable by uploading a text file and using the command “sysconf banner” to apply the file content as extended banner text.

Features that require HSM firmware 6.21.0

FIPS Certification Update

Luna HSMs updated to firmware 6.21.0 implement conformity with the latest NIST interpretations of applicable FIPS standards, including enforcement of legacy-only status for some older mechanisms. With the HSM not in FIPS mode, you can use any algorithm in any manner. With the HSM set to FIPS mode, certain deprecated algorithms are restricted with respect to key-size range, or with respect to permissible operations.

As discussed on the NIST website, some algorithms and key sizes are already precluded in FIPS mode, and additional restrictions will come into force in 2015. We recommend that you begin migrating away from keys that will no longer be supported.

New Algorithms

Luna HSM 5.4.x adds the X9.19 Retail MAC and DUKPT algorithms.

Small Form-Factor USB Backup

For Luna HSMs with PED authentication, HSM partition objects can be securely backed up to SafeNet e7300 tokens via locally connected Luna PED, or via Luna Remote PED for distant backup. To evaluate the Small Form Factor Backup feature (SFF backup), contact your SafeNet Sales Representative to obtain the necessary Capability Update.

Usage Notes

- SFF backup requires firmware 6.21.0 or higher.
- SFF backup requires the Common Criteria certified version of eToken 7300.
- SFF backup over local PED connection is subject to some stability issues (see Known Issues section, below).
- SFF backup requires that PEDTimeout2 is set to a value of 200000 in the crystoki.ini file.
- If you are applying SFF backup to a Password-authenticated Luna HSM, you must apply the SFF backup capability update file before you apply the Remote PED capability update file. Attempting to install the SFF backup update after the Remote PED capability update causes the following error:

  (10A0B : LUNA_RET_OPERATION_RESTRICTED).

  If you install the Remote PED capability before the SFF backup capability, you can correct the problem by rolling back the firmware (which removes the CUF), re-installing f/w 6.21.0, installing the SFF backup capability file, and then installing Remote PED capability file.

  This issue does not occur on PED-authenticated Luna HSMs.

Advisory Notes

This section highlights important issues you should be aware of before deploying this release. The advisory notes in this section apply to all of the products supported by Luna HSM 5.4.x.

Firmware Update May Be Required For Some New Feature Support

Luna appliances are shipped with the most recent FIPS-validated firmware version installed, and with the newest firmware version (if different) ready to install at your option. Several of the features described in the “New Features and Enhancements” section, above, require that you update the firmware to version 6.21.0.

DUAL_EC_DRBRG is Not Used

SafeNet's HSMs do not use DUAL_EC_DRBRG in the HSM in any capacity. Details on the RNG used are listed in the security policy from each HSM's FIPS 140-2 certification which is available online via the NIST website. The HSM's RNG is compliant with the AES_CTR_DRBG as specified in NIST SP 800-90A.

HSM Firmware 6.21.0 and FIPS 140-2

At the time of writing, firmware 6.2.1 for Luna PCI-E and for Luna SA (or firmware 6.2.3 for Luna G5) is the latest FIPS-validated Luna HSM firmware version. If you require FIPS validated firmware, then do not upgrade the firmware. Firmware version 6.10.2 is the candidate currently under FIPS evaluation, expected to achieve validation later in 2014.

Firmware 6.20.0, provided with Luna HSM release 5.3.1 and firmware 6.21.0, provided with Luna HSM release 5.4.x, are not candidates for FIPS evaluation.

When you install LunaClient software for Luna PCI-E or for Luna G5, earlier standby firmware options (like firmware 6.10.2) are replaced on your hard drive by the firmware package that is current for the current release.

When you install Luna SA appliance software, earlier standby firmware options (like firmware 6.10.2) are replaced by the firmware package that is current for the current release.

Contact SafeNet to acquire a stand-alone package for firmware update to version 6.10.2, if you need it.

Change to Default Chrystoki Library Path Might Affect Third-Party Applications

As of release 5.2, the location of the cryptoki library is defined by the ChrystokiConfigurationPath environment variable. If your applications use a configuration file to point to the location of the cryptoki library instead of using the ChrystokiConfigurationPath environment variable, you will need to edit your configuration file to specify the path to the cryptoki library, as follows:

Windows	C:\Program Files\SafeNet\LunaClient\cryptoki.dll
Unix/Linux	/usr/safenet/lunaclient/lib/libCryptoki2.so (32-bit) /usr/safenet/lunaclient/lib/libCryptoki2_64.so (64-bit)
Solaris	/opt/safenet/lunaclient/lib/libCryptoki2.so (32-bit) /opt/safenet/lunaclient/lib/libCryptoki2_64.so (64-bit)
HP-UX	/opt/safenet/lunaclient/lib/libCryptoki2.sl (32-bit) /opt/safenet/lunaclient/lib/libCryptoki2_64.sl (64-bit)
AIX	/usr/safenet/lunaclient/lib/libCryptoki2.so (32-bit) /usr/safenet/lunaclient/lib/libCryptoki2_64.so (64-bit)

Utilities and Sample Code

Utilities and sample code are provided for example purposes only, and are not intended or supported for use in production environments.

Migration of Key Material

If you need to migrate key material from one Luna HSM to another Luna HSM, contact SafeNet Technical Support for the Migration instruction document.

Configuration "PE1746Enabled=" Is Now Disabled by Default

The configuration setting PE1746Enabled is now set to zero (0), or disabled, by default to accommodate small-packet encryption. If your application uses large-packet sizes when encrypting, consider setting this item to one (1) or enabled in the client-side Chrystoki.conf (Linux) or crystoki.ini (Windows) file. Be aware that using PE1746Enabled=1 disables the HA load-balancing function. Refer to the Performance section of the page HA Operational Notes in the Luna documentation, for more detail.

New Capabilities and Policies – Do Not Use

Commands like `hsm showPolicies` now display three new Capabilities and their attendant Policies. Please ignore these (highlighted below *). They support some upcoming functional changes, currently in development, and are subject to change.

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

Changing policies marked "destructive" will zeroize (erase
completely) the entire HSM.

Description                              Value      Code     Destructive
===========                              =====      ====     ===========
Allow cloning                            On           7        Yes
Allow non-FIPS algorithms                On          12        Yes
SO can reset partition PIN               On          15        Yes
Allow network replication                On          16        No
Allow Remote Authentication              On          20        Yes
Force user PIN change after set/reset    Off         21        No
Allow offboard storage                   On          22        Yes
Allow remote PED usage                   On          25        No
Allow Acceleration                       On          29        Yes
Allow unmasking                          On          30        Yes
*Force Single Domain                     Off         35        Yes
*Allow Unified PED Key                   Off         36        No
*Allow MofN                              On          37        No
```

Compatibility and Upgrade Information

This section describes the upgrade paths for this release, the compatibility of the release with other system components, such as backup HSMs and PEDs, supported operating systems and firmware, and FIPS validation status.

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 5.4.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 SafeNet 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 timeframes involved. Completed CC evaluations: http://www.commoncriteriaportal.org/products/

Component Versions (5.4.7)

The following table lists the supported firmware/software versions for the various components supported in Luna HSM 5.4.7

Component	Version
Luna PCI-E and Luna SA HSM firmware	6.2.1 (upgradable to 6.21.0)
Luna G5 firmware	6.2.5 (upgradable to 6.21.0)
Luna Remote Backup HSM firmware	6.0.8 (upgradable to 6.21.0)
PED Workstation software (requires Remote PED) [optional]	1.0.5
PED II / PED IIr	2.5.0-3
Client software	5.4.1/5.4.2
Luna SA appliance software	5.4.7

Upgrade Paths

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

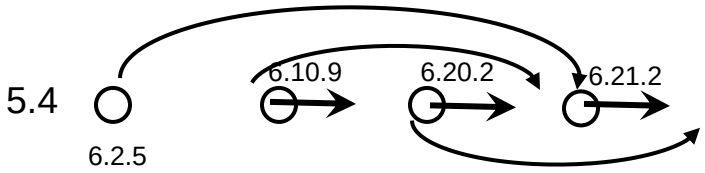
The following upgrade paths are available in this patch. If your HSM is at a lower software or firmware version than those indicated in the “Software Version/Release FW” column, upgrade to an indicated current version, and then apply the secure patch.

Software Version/Release FW	Available FW Releases	Recommended FW	FIPS Target
5.4 / 6.21.0	6.2.1	6.2.5	Validated
	6.10.1	6.10.9	Validated

Software Version/Release FW	Available FW Releases	Recommended FW	FIPS Target
	6.10.2		
	6.10.7		
	6.20.0	6.20.2	Not Planned
	6.21.0	6.21.2	Not Planned

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



These (below) were the upgrade paths supported for Luna 5.4.x **before** the security patch.

Upgrade Notes

These notes apply to the following tables, as indicated.

Note 1: The Luna HSM software version shipped from the factory is now 5.2.4 with firmware 6.2.1 (until firmware 6.10.9 receives FIPS validation).

Note 2: Software 5.3.3 replaced 5.3.0, 5.3.1, and 5.3.2 as the only downloadable 5.3 version, with the only changes being the replacement of firmware 6.10.2 for the Luna SA SSH fix, and the BASH fix.

Note 3: Firmware 6.2.3 applies to Luna G5 only.

Note 4: Firmware 6.10.9 (superseding 6.10.2) replaces firmware 6.10.1 as the in-progress FIPS candidate (at this writing), and includes the SSH fix for Luna SA.

Note 5: Release 5.4.7 supersedes the earlier appliance software versions. Client and firmware versions do not change.

5.4.7 (supersedes earlier releases, below, for Luna SA only)

Component	From version...	To version...
Luna SA appliance software	5.2.4, 5.2.6 5.3.3, 5.3.5 5.4.0, 5.4.1, 5.4.2, 5.4.3, 5.4.4, 5.4.6	5.4.7. Install update 630-010165-024 (includes the previous 5.4.x updates and patches)

5.4.3

See the PatchNote accompanying the patch.
UPDATE: Now included in 5.4.4/5.4.7.

5.4.2 (Windows/Linux/Solaris)

Component	From version...	To version...
Luna SA client software	5.4.1	5.4.2. Install patch 630-010370-001.
Luna SA appliance software	5.4.1	5.4.2. Install patch 630-010165-015

5.4.2 (HP-UX/AIX)

Component	From version...	To version...
Luna SA client software	Any	5.4.2
Luna SA appliance software	5.2.3 (See Note 1), 5.3.0, 5.3.1 (See Note 2), 5.4.0	5.4.1 (included in the 5.4.2 package). Install patch 630-010165-015 to complete the upgrade to 5.4.2
HSM firmware	6.2.1, or 6.2.3 (See Note 3), 6.10.1, 6.10.2 (See Note 4), or 6.20.0	6.21.0

5.4.1 (Windows/Linux/Solaris)

Component	From version...	To version...
Luna SA client software	Any	5.4.1
Luna SA appliance software	5.2.3 (See Note 1), 5.3.0, 5.3.1 (See Note 2), 5.4.0	5.4.1
HSM firmware	6.2.1, or 6.2.3 (See Note 3), 6.10.1, 6.10.2 (See Note 4), or 6.20.0	6.21.0

Supported Operating Systems

This section lists the supported operating systems for the various components of a Luna HSM solution.

Luna Client

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

Operating System	Version	32-bit client	32-bit client on 64-bit OS	64-bit client
Windows	2008 R2	No	Yes	Yes
	2012 and 2012 R2	No	Yes	Yes
	7	Yes	No	No
Redhat Enterprise Linux (includes variants like CentOS)	5.x	Yes	Yes	Yes
	6.x	Yes	Yes	Yes
OpenSuse Linux	10.2	Yes	Yes	Yes
	11.3	Yes	Yes	Yes
Debian	6.x	Yes	No	Yes
Solaris (SPARC/x86)	10	No	Yes	Yes
	11	No	Yes	Yes

Operating System	Version	32-bit client	32-bit client on 64-bit OS	64-bit client
HP-UX	11.31	No	Yes	Yes
AIX	6.1	No	Yes	Yes
	7.1	No	Yes	Yes

Remote PED Server

Windows 2012, Windows 2008 R2, Windows 7 (64-bit only)

Supported APIs

The following APIs are supported on all supported operating systems:

- PKCS#11 2.20
- Java 6
- Java 7
- Java 8
- CAPI (Windows only)
- CNG (Windows only)

Advanced Configuration Upgrades

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

- Korean algorithms
- Maximum memory
- ECIES acceleration
- 5 partitions (Luna SA)
- 10 partitions (Luna SA)
- 15 partitions (Luna SA)
- 20 partitions (Luna SA)

Note The ECIES acceleration upgrade (Luna HSM 5.4) is field-installable, but is not installed at the factory – at time of writing – because the current factory-installed firmware is version 6.2.1 with version 6.10.2 on standby. This is done so that all customers receive the FIPS-validated version installed, with option to upgrade to newer firmware. When firmware 6.10.2 becomes FIPS-validated, and we begin installing that as the default version, then the ECIES upgrade will be a factory-installable option.

PCI-E Server Compatibility

SafeNet tests HSM products on a selection of commonly used servers; however we are unable to test on all possible host systems. A lock-up issue related to a bridge component used in Luna PCI-E was detected on some servers at installation of the driver.

Servers Tested Successfully

The x86 and x64-based servers (Windows 2008R2, Windows 2012, Windows 2012 R2, and RedHat Enterprise Linux 6 (64)) listed in the following table are confirmed to work successfully with Luna PCI-E.

Windows/Linux

Server	Notes
Cisco UCS 210 M1	Single card in any of slots 1, 2, 3, 4, or 5. Passes 3-card test.
Dell R610	Single card in any of slots 1 or 2. Passes 2-card test.
Dell R620	Single card in slot 1 for the two-slot configuration. Not supported in the three-slot configuration (10 drive bays).
Dell R720	Single card in any of slots 2 or 3. Passes 2-card test.
Dell T610	Single card in any of slots 1, 2, or 5. Passes 3-card test. Slots 3 and 4 fail.
HP 360p Gen 8	Single card in slot 1.
HP DL 380 G5	Single card in any of slots 1, 2, or 3. Passes 3-card test.
HP DL 380 G7	Single card in any of slots 1, 2, 3, or 4. Passes 3-card test.
HP DL 380P Gen 8	Single card in any of slots 1, 2, 3, 4, 5, or 6. Passes 3-card test. Slot 3 fails with CKR_Device Error on RHEL 6.2.
IBM x3650 M2	Single card in any of slots 1, 2, or 3. Passes 3-card test. Slot 4 fails.
IBM x3650 M4	Single card in any of slots 1, 2, or 3. Passes 3-card test.

Solaris

The x86 and Sparc based servers (Solaris 10/11) listed in the following table are confirmed to work successfully with Luna PCI-E.

Server	Notes
Sun M4000	Single card in slot 1 with Solaris 11.
Dell R710 x86	Single card in any of slots 1 or 2. Passes 2-card test with Solaris 10/11.
Sun A70	Single card in any of slots 1, 2. Passes 2-card test with Solaris 10.

HP-UX

The HP-UX V3 (11.31) based servers listed in the following table are confirmed to work successfully with Luna PCI-E.

Server	Notes
HP Integrity RX-2800	Single card in any of slots 1 or 2. Passes 2-card test with HP-UX V3 (11.31)

AIX

This release does not support Luna PCI-E HSMs on AIX.

Luna G5 Server Compatibility

SafeNet tests HSM products on a selection of commonly used servers; however we are unable to test on all possible host systems.

Servers Tested Successfully

Solaris

The x86 and Sparc based servers (Solaris 10/11) listed in the following table are confirmed to work successfully with Luna G5.

Server	Notes
Sun A70	Works with 2 G5 HSMs on front USB ports with Sparc 10.
Dell R710 x86	Works with 2 G5 HSMs on front USB ports with Solaris 10/11.
Sun M4000	Works with 1 G5 HSMs on PCI-E USB port with Sparc 11.

HP-UX

This release does not support Luna G5 HSM on HP-UX.

AIX

This release does not support Luna G5 HSM on AIX

Addressed Issues

The following tables list the issues addressed in this release. The addressed issues are categorized by product as follows:

Issue Severity

This table defines the severity of the issues listed in the following tables.

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

Common Luna Addressed Issues

Issue	Severity	Synopsis
(LHSM-11038) OpenSSL TLS heartbeat read overrun vulnerability	C	**Problem:** A vulnerability was discovered in OpenSSL (CVE-2014-0160 - TLS heartbeat read overrun) that affects Luna HSM 5.4.0. (No other Luna product version is affected.) **Resolution:** Luna HSM 5.4.1 or higher fixes the vulnerability.
(LHSM-7035) Cannot change partition password to password	L	**Problem:** On a PED-authorized HSM with firmware 6.20.0, the partition challenge cannot be changed to "PASSWORD". **Resolution:** Working as designed. "PASSWORD" is too insecure and is not allowed to be chosen as a replacement password.
(LHSM-3452) CKLOG help references incorrect DLL name	L	**Problem:** The following line is incorrect: LibNT=c:\Program Files\LunaSA\cryst201.dll The DLL is actually named "cryptoki.dll". **Resolution:** Fixed.

Issue	Severity	Synopsis
(LHSM-3450) HA works by default for single-part encryption	H	**Problem:** Luna HSMs had a default setting PE1746Enabled=1, which favored large-packet encryption (data packet size > 1000 bytes). It makes more sense to optimize performance for the more common usage, which is small data packet encryption, and which also ensures that HA works in the greatest number of customer use cases. **Resolution:** Default setting in configuration file is now PE1746Enabled=0.
(LHSM-3319) Audit logging trace-ability of "who" is broken sometimes	H	**Problem:** Under some circumstances the Luna client's use of the HSM's external log call fails to associate the client process name with the correct access ID. As such, the HSM's audit logs cannot always trace entries all the way back to a client's process name/id. **Resolution:** Fixed.
(LHSM-3142) session handle invalid during failed member recovering while key gen existing	H	**Problem:** During non-interrupt upgrade testing, found session handle invalid:1. In a three-member HA group 2. RSASign traffic and ecdsakeygen traffic co-existing 3. Fail the primary member, no impact 4. Recover the primary member → CKR_CANCEL error in key gen session 5. Continue attempting to recover RSASign, eventually get session handle invalid error on rsasig session. **Resolution:** Fixed.
(186754) **vtl haadmin deleteGroup** command does not remove all HA group related info	L	**Problem:** If you create an HA group, make one member standby, delete the HA group, and then recreate it, **vtl haadmin show** will show the old (deleted) configuration (the standby member). **Resolution:** Invalid – use lunacm.
(186406) Cannot run a Java 7 application on Windows	H	**Problem:** SafeNet recommends that you put **LunaAPI.dll** in the <java install dir>**/lib/ext** folder. However, Java 7 for Windows has removed this directory from the Java library path. As a result, when a Java 7 application on Windows uses the Luna provider, it cannot find the **LunaAPI.dll** library, causing the application to fail. **Resolution:** Documented in the product documentation – See the section "Java Library Path Issue" in the Windows Installation instructions
(181244) SHA384 and SHA512 HMAC sign/verify performance	H	**Problem:** SHA384 and SHA512 HMAC sign/verify performance in Luna HSM 5.2.x is significantly slower than in previous releases. This issue applies to Luna SA and Luna PCI-E only. Luna G5 is not affected. **Resolution:** This was noted in the previous CRN. Customers updating to 5.3 must start at 5.2.1, 5.2.2, or 5.2.3 first, and will see that CRN.

Luna SA Addressed Issues

Issue	Severity	Synopsis
(HSMAN-125 Update for Shellshock vulnerability	C	**Problem:** BASH-related vulnerabilities are reported as CVE-2014-6271, CVE-2014-6277, CVE-2014-6278, CVE-2014-7169, CVE-2014-7186, and CVE-2014-7187 **Resolution:** Luna HSM 5.4.4/5.4.7 fixes the vulnerability as a field update, and in all 5.x versions shipped from the factory.
(LHSM-12955 NTLS service shuts down intermittently	H	**Problem:** NTLS shut down after 7-to-10 days of operation. No errors were found in the lunalogs but messages log reports OOS 20, and LCD on the appliances shows error 20. Recovery from this state required reboot of the Luna appliance or start ntls service and then restart the application. **Resolution:** Fixed in release 5.4.7.

Issue	Severity	Synopsis
(LHSM-10559) OpenSSH 6.2 AES-GCM vulnerability flagged by Qualys scanner in SA 5.4-13	H	**Problem:** Some vulnerability scanners identity CVE-2013-4548 (http://nvd.nist.gov/nvd.cfm?cvename=CVE-2013-4548) as a potential vulnerability. This is flagged due to the use of OpenSSH in Luna SA. However, Luna SA 5.4.1/5.4.2 and previous versions are not vulnerable, as they prevent the use of AES-GCM among the negotiable ciphers. SafeNet will update ssh in future releases, and the alert will no longer appear. **Resolution:** If you run a scanner that flags this as a possible vulnerability, ignore. That potential vulnerability has been blocked in Luna SA.
(LHSM-8678) Audit function - removed yearly rotate option but documentation not updated	H	**Problem:** The selection “yearly” was removed from the Audit log rotation options, but the documentation was not updated. **Resolution:** The page is updated and now says hourly, daily, weekly, monthly, and never.
(LHSM-8581) Documentation implies network interfaces on appliance support 10 and 100 Mbps only	M	**Problem:** The Luna SA documentation page recommended_network_characteristics.htm does not mention gigE, and can leave customers thinking that the appliance supports only 10 and 100 Mbps network interfaces. **Resolution:** The page now says: Bandwidth • Minimum supported: 10 Mb half duplex • Recommended: at least 100 Mb full duplex - full Gigabit Ethernet is supported **Note**: Ensure that your network switch is set to AUTO negotiation, as the Luna appliance negotiates at AUTO. If your network switch is set to use other than automatic negotiation, there is a risk that the switch and the Luna appliance will settle on a much slower speed than is actually possible in your network conditions. Network Latency • Maximum supported: 500ms • Recommended: 0.5ms

(LHSM-3419) Bug in key activation and deactivation command logic in lush	M	**Problem:** Lunash says that Keys in HardWare is not configured/activated, when in fact it is.
		`lunash:>ntls sh`
		`NTLS Keys In HW is NOT configured`
		`The NTLS is NOT activated`
		`NTLS bound to network device: eth1 IP Address: "172.20.13.213" (eth1)`
		`On the HSM:`
		`Misc = { ToolsDir = /usr/lunasa/bin; KeysInHW = Yes; AppIdMajor = 1; AppIdMinor = 2; NtlsSSLOps = All; }`
		Resolution: Fixed.

(LHSM-3392) Salogin displays "Login successful" after closing session	M	**Problem:** After processing cmd "./salogin -o", it shows "Login successful", instead of displaying something like "session closed successfully". **Resolution:** Fixed.
(LHSM-3389) Show crypto operation counts in Luna SA	M	**Problem:** "hsm info show" lunash command output adds these 2 counters: Crypto Operation Requests: 44099950 Crypto Operation Errors: 0 They capture the number of successful crypto operations and failures. **Resolution:** As noted.

Issue	Severity	Synopsis
(LHSM-3333) crash in Linux if ipcheck disabled when using HTL	M	**Problem:** htl server terminates htl session if ipcheck set to disabled and packet received from client with different source IP from the IP in CN of Certificate. **Resolution:** Fixed.
(LHSM-3332) ipcheck not implemented for HTL	M	**Problem:** Disabling ipcheck is desirable for certain client situations, such as when NAT occurs between client and Luna SA. HTL server terminates the HTL session if ipcheck is disabled and a packet is received from a client with a source IP that does not match IP used to create the NTLS certificate. **Resolution:** Fixed.
(161092) Broken pipe error generated by **vtl haadmin -show** when an HA member goes down.	M	**Problem:** An erroneous Broken Pipe error is displayed by the **vtl haadmin -show** command if one of the HA members becomes unavailable. **Resolution:** Fixed with new signal handler.
(161085) Deleting the HA group does not delete HA entries in the client configuration file	M	**Problem:** Deleting the HA group does not delete HA entries in the client configuration file. **Resolution:** Fixed.
(189609) LunaCM does not display other HSM's connected with broken htl client connection	H	**Problem:** LunaCM does not display other HSM's connected with broken htl client connection. **Resolution:** Fixed.

Luna PCI-E Addressed Issues

Issue	Severity	Synopsis
(LHSM-5830) Docs: About Luna PCI-E has bad battery information	M	**Problem:** Luna PCI-E docs still describe sliding the battery switch on the K6 card. This is mentioned in "About Luna PCI-E". The switch is glued in place and does not move. The instructions were correct in the past, but have not been updated. **Resolution:** Fixed in 5.3 docs.

Luna G5 Addressed Issues

No Luna G5-specific issues were fixed in this release.

Known Issues

The following tables list the known issues at time of release. The known issues are categorized into separate tables as follows:

- "Common Luna Known Issues" on page 16
- "Small Form-factor Backup Known Issues" on page 23
- "Luna SA Known Issues" on page 26
- "Luna PCI-E Known Issues" on page 29
- "Luna G5 Known Issues" on page 29

Workarounds are provided where available.

Note In the following tables, some issues are tracked either in our old database (with the six-digit numbers) or in our new database (with Luna product issues preceded by "LHSM-"), or in both, and we mention both numbers where applicable.

Issue Severity

This table defines the severity of the issues listed in the following tables.

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

Common Luna Known Issues

Issue	Severity	Synopsis
(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. **Workaround:** Delete and re-insert the key before changing the AAD. Otherwise, you must reset the HSM before changing the AAD.
(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 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 client with the default Chrystoki.conf file on a Debian OS 1 Uninstall the Luna client: /usr/safenet/lunaclient/bin/uninstall.sh 2 Purge the libcryptoki library: dpkg -P libcryptoki 3 Delete the backup Chrystoki.conf file: rm /etc/Chrystoki.conf.debsave 4 Re-install the Luna client: <path>/install.sh
(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.

Issue	Severity	Synopsis
(LHSM-10594) more documentation needed for CSP and KSP	M	**Problem:** Currently, our documentation explains only basic registration for CSP and KSP. Material not covered includes: CSP commands and usage: register /usagelimit (including how the counter works) register /partition /highavail register /partition /strongprotect register /algorithms register /cryptouser ms2luna keymap KSP commands and usage: ms2luna ksputil ksputil clusterKey ksputil listKey kspcmd kspcmd usagelimit (and how the counter works) kspcmd library kspcmd password kspcmd viewslots Other: - CSP logging - KSP logging - interaction of KSP and CSP **Workaround:** Some assistance is available from the syntax help for utilities and commands.
(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 whatever), or after every renewal, launch ckdemo and manually add the usage limit attribute.

Issue	Severity	Synopsis
(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. **Workaround:** The following workarounds are applicable to Luna HSM release 5.2.1 through 5.4.1/5.4.2 inclusive: SafeNet HTL Client Service 1- If you see “SafeNet HTL Client Service” among Windows services stop it and continue with step 2. 2- Run C:\Program Files\SafeNet\LunaClient\htl\htlc_service.exe uninstall 3- Edit C:\Program Files\SafeNet\LunaClient\htl\htlc_service.xml and remove the following line: <depend>Spooler</depend> 4- Run C:\Program Files\SafeNet\LunaClient\htl\htlc_service.exe install 5- Start “SafeNet HTL Client Service” service if it was running at step 1. SafeNet Remote PED Service 1- If you see “SafeNet Remote PED Service” among Windows services, stop it and continue with step 2. 2- Run C:\Program Files\SafeNet\LunaClient\PedClient_service\pedclient_service.exe uninstall 3- Edit C:\Program Files\SafeNet\LunaClient\PedClient_service\pedclient_service.xml and remove the following line: <depend>Spooler</depend> 4- Run C:\Program Files\SafeNet\LunaClient\PedClient_service\pedclient_service.exe install 5- Start “SafeNet Remote PED Service” service if it was running at step 1. SafeNet Luna SNMP Subagent Service 1- If you see “SafeNet Luna SNMP Subagent Service” among Windows services, stop it and continue with step 2. 2- Run C:\Program Files\SafeNet\LunaClient\ snmp\ luna-snmp_service.exe uninstall 3- Edit C:\Program Files\SafeNet\LunaClient\ snmp\ luna-snmp_service.xml and remove the following line: <depend>Spooler</depend> 4- Run C:\Program Files\SafeNet\LunaClient\ snmp\ luna-snmp_service.exe install 5- Start “SafeNet Luna SNMP Subagent Service” service if it was running at step 1.

Issue	Severity	Synopsis
(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 Luna 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 - Install/configure base Luna 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. **Workaround:** When using the ms2luna.exe utility from the folder c:\Program Files\SafeNet\LunaClient\KSP to migrate, after running ms2luna. - modify this registry entry: HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\CertSvc\Configuration\<CA name>\CSP change the value of "Provider" to "Safenet Key Storage Provider" - go back to CA Management and note that the provider has changed - CA can be restarted If a check with `certutil` shows that the certificate still appears to be associated with the Microsoft provider, but attempts to "repair" it to the Luna provider result in an error that the cert is already with the Luna provider, then there might be a copy in both places. Delete the old copy of the certificate and retry with your application.

(LHSM-10577) ms2luna fails to import software key and cert in Windows 2012	H	**Problem:** ms2luna fails to import software key and cert in Windows 2012
		Steps:
		- create software CA
		- obtain thumbprint of CA cert created
		- run Luna register util
		- run ms2luna and provide thumbprint of CA cert – fails:
		`Please Enter The Certificate Thumbprint Of Required Certificate:`
		`8546093c093c8c3ec7f961681b0c1eec886d2373`
		`ERROR Acquiring Handle Of Key Container!!`
		Workaround: None. Do not use the ms2luna.exe utility from the folder c:\Program Files\SafeNet\LunaClient\CSP to migrate, until further notice.

(LHSM-10402) ms2luna is not working as expected	H	**Problem:** When the Ms2luna utility is run, it asks for the thumbprint of the certificate in software. If the thumbprint is provided, the utility copies the private key, public key and the data object to the Luna partition. But the certificate still shows that it is tied to software Microsoft Enhanced Cryptographic Provider. Using certutil repairstore to fix the certificate association with the Luna provider still gives "ERROR: Could not verify certificate public key against private key". **Workaround:** None. Do not use the ms2luna.exe utility from the folder c:\Program Files\SafeNet\LunaClient\CSP to migrate, until further notice.

Issue	Severity	Synopsis
(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-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.
(190453) RBS host app does not display a message in case of a wrong password.	M	**Problem:** The RBS host application does not display an error message if the user enters a wrong password. **Workaround:** None.
(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. **Workaround:** If using multitoken for RSA sigver against an HSM in FIPS mode, pass the packet parameter with size 32 (or larger), for example: multitoken2 -mode rsasigver -key 2048 -slots 1 -packet 32 View the NIST site for information about similar restrictions with other FIPS approved key sizes and mechanisms.
(LHSM-9418) some content missing from Javadocs on Windows	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. **Workaround:** Replace the incomplete Luna Javadocs on your Windows system with the complete version from the Linux installer, as follows: 1) After installing LunaClient on your Windows computer, delete <luna client dir>/JSP/javadoc 2) On the Luna Client media, got to the “linux” folder. 3) Use a general-purpose archiving/unarchiving utility to open the file lunajsp-5.4.1....rpm 4) In the unarchiving utility, navigate (assuming you started in your \Downloads directory) to: C:\Users\yourname\Downloads\LunaClient_5.4.1-12\linux\64\lunajsp-5.4.1-12.x86_64.rpm\lunajsp-5.4.1-12.x86_64.cpio\.\usr\safenet\lunaclient\jsp\javadoc-5.4.1.tar.gz\javadoc-5.4.1.tar\javadoc\ 5) Extract all the content of that javadoc folder to <luna client dir>/JSP/javadoc >.

Issue	Severity	Synopsis

(LHSM-7032) RBS: client cannot read RBS HSM information if rbs does not already have a partition	M	**Problem:** Remote Backup Service - The client cannot read RBS HSM information if no partition exists in the RBS Backup HSM.
		`[user@myhost bin]# ./lunacm`
		`LunaCM V2.3.3 - Copyright (c) 2006-2013 SafeNet, Inc.`
		`Available HSM's:`
		`Slot Id -> 1`
		`HSM Configuration -> Luna SA Slot (Failed to read information from HSM)`
		`Current Slot Id: 1`
		`lunacm:>exit`
		Workaround: Create a partition on the Backup HSM
		`[user@myhost bin]# ./lunacm`
		`LunaCM V2.3.3 - Copyright (c) 2006-2013 SafeNet, Inc.`
		`Available HSM's:`
		`Slot Id -> 1`
		`HSM Label -> bck1`
		`HSM Serial Number -> 7002333`
		`HSM Model -> G5Backup`
		`HSM Firmware Version -> 6.20.0`
		`HSM Configuration -> Remote Backup HSM (PW) Backup Device`
		`HSM Status -> OK`
		`Current Slot Id: 1`

(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-6968) Windows - cklog is missing when only Luna Remote Backup HSM is installed	M	**Problem:** If only Luna Remote Backup is selected to be installed, the installation directory and the win32 subfolder will not contain cklog. No error message is shown. **Workaround:** If you are installing Luna [Remote] Backup, also select Luna SA. This will ensure that cklog is installed in the install directory and the win32 subfolder.
(LHSM-6967) Windows - cklog and shim are missing in win32 directory when only Luna G5 is installed	M	**Problem:** If only Luna G5 is selected to be installed, the win32 directory will not contain cklog and shim. No error message is shown. **Workaround:** If you are installing Luna G5, also select Luna SA. This will ensure that cklog and the shim are installed in the win32 directory.
(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.. **Workaround:** See special instructions for running 32-bit apps on 64-bit OS, in the Windows installation instructions of the product documentation.

Issue	Severity	Synopsis

(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`
		Workaround: Reboot Windows.

(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. **Workaround:** Just be aware of the numbering discrepancy.
(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. **Workaround:** None.
(LHSM-5790) “lunacm” does not display other HSM’s connected with broken htl client connection	M	**Problem:** “lunacm” does not display other HSM’s connected with broken htl client connection **Workaround:** If you stop the HTL service while lunacm is running, stop lunacm also. Do not try to use HTL in an already-running lunacm session.
(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 don 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.

Issue	Severity	Synopsis
(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-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 pedclient 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.

Small Form-Factor Backup Known Issues

Issue	Severity	Synopsis
(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-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.

Issue	Severity	Synopsis
(LHSM-9710, 9711, 9712, 9713) 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-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 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.

Issue	Severity	Synopsis

(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`
		Workaround: Ensure that the host is connected to UPS, and avoid host reboot while backup is in progress. In the event of an interruption, be aware that the object count could be spurious.

(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`
		`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.

Luna SA Known Issues

Issue	Severity	Synopsis
(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. **Workaround:** 1. Avoid using service restart on snmp. (Instead, use stop and then start) 2. If service restart is used on snmp, the subagent won't automatically reconnect, so to get around this, kick off an snmp service stop command and then follow it up with an snmp service start command. This method will allow the NET-SNMP subagent to reconnect. **Alternative Workaround**: Perform 2 back to back restarts.
(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 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 **Workaround:** The list is not updated, but ECDSA is available; you can still use it.
(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 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.

Issue	Severity	Synopsis

(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-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).`
		Workaround: Be aware that the command is doing exactly what was asked.

(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-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
		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-9883) Lunash fails to shut down certmonitord service	L	**Problem:** Command "ntls certificate monitor disable" in lunash shows that cert monitor was disabled, but in fact the command failed to shut down `certmonitord` service. **Workaround:** Ignore, for the present. This affects only monitoring of certificate expiry, and the current certificates are good for another ten years.

Issue	Severity	Synopsis
(LHSM-9846) sysconf secureKeys broken for PWD-AUTH LunaSA	M	**Problem:** The command to move software NTLS keys into hardware is broken on password-authenticated Luna 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-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. **Workaround:** Ignore, or compare to the output of "package list".
(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-9422) Windows SA 2xHA performance issue: RSA 1024 Sign	M	**Problem:** RSA Sign 1024 with Luna SA 2xHA shows only 8500 operations/second, while Linux multitoken2 reaches 14000 operations/second (the same Luna SA appliance and client machine). **Workaround:** If greater performance under Windows is required, before this can be fixed, consider using a faster client computer (at least four computing cores, 8GB of RAM).
(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.
(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". **Workaround:** Until this is fixed, be aware of the number of bad login attempts since the last successful login.
(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. **Workaround:** If the situation applies to your Luna HSMs, contact SafeNet Technical Support.
(LHSM-5824 MKS161028) SIM key migration to Luna SA 5.1 requires application of a destructive CUF	H	**Problem:** SIM key migration from Luna SA 4.x to Luna SA 5.1 does not work using the standard configuration. **Workaround:** To use SIM key migration on Luna SA 5.1, you must contact SafeNet support to receive a destructive capability update file (CUF) that, once applied, enables unmasking.

Luna PCI-E Known Issues

Issue	Severity	Synopsis
(9819) lunacm “partition archive backup” displays wrong backed up object number	M	**Problem:** If invalid object handles are passed to "`partition archive backup -o`", lunacm responds CKR_OBJECT_HANDLE_INVALID error which is correct, but also displays the objects numbers that were backed up, and that number is not correct. **Workaround:** Ignore the declared number of backed-up objects, or avoid passing invalid object handles.
(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.
(189565) Client tools fail to contact PCI-E card on Solaris 11 Sparc T-5120 server.	M	**Problem:** Client tools fail to contact PCI-E card on Solaris 11 Sparc T-5120 server. **Workaround:** None

Luna G5 Known Issues

Issue	Severity	Synopsis
LUC-630	M	**Problem**: On updating firmware for G5, a Device Error is returned. However, the firmware is found to be updated after reboot. **Workaround**: Before updating the firmware for G5, stop the Pedclient service.
(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-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-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-5797 MKS182827) 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.

Technical Support Information

If you have questions or need additional assistance, contact Technical Support through the listings below:

Contact method	Contact information	
Address	SafeNet, Inc. 4690 Millennium Drive Belcamp, Maryland 21017 USA	
Phone	United States	(800) 545-6608, (410) 931-7520
	Australia and New Zealand	+1 410-931-7520
	China	(86) 10 8851 9191
	France	0825 341000
	Germany	01803 7246269
	India	+1 410-931-7520
	United Kingdom	0870 7529200, +1 410 931-7520
Web	www.safenet-inc.com/Support	
Support and Downloads	www.safenet-inc.com/Support Provides access to the SafeNet Knowledge Base and quick downloads for various products.	
Customer Technical Support Portal	https://serviceportal.safenet-inc.com Existing customers with a Customer Connection Center or Service Portal account can log in to manage incidents, get the latest software upgrades, and access the SafeNet Knowledge Base.	

Trademarks and Disclaimer

Although we have attempted to make this document as complete, accurate, and useful as possible, we cannot guarantee its contents. Errors or omissions will be corrected, as they are identified, in succeeding releases of the product. Information is subject to change without notice.