Luna HSM 5.3.5

CUSTOMER RELEASE NOTES

Document part number: 007-012225-002 Revision H
Release notes issued on: 17 November 2015

The most up-to-date version of this document is at:
http://www.securedbysafenet.com/releasenotes/luna/crn_luna_hsm_5-3.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 several form factors, offering multiple levels of performance and functionality, as follows:

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

Luna HSM 5.3 Security Patch

This firmware patch for Luna G5 and Luna PCI-E and Luna SA to firmware versions 6.2.5, 6.10.9, and 6.20.2, 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.

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.

Luna HSM 5.3.5

Luna HSM 5.3.5 is a Luna SA-only release, 630-010165-023, which includes the previous 5.3.x releases and patches, as well as firmware 6.20.0.

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.

Fixing NTLS lockout (intermittent shutdown)

Release 5.3.5 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 5.3.4

Limited release.

Luna HSM 5.3.3

Luna HSM 5.3.3 is a Luna SA-only release, 630-010165-020, which includes the previous 5.3.x releases and patches, as well as firmware 6.20.0.

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 5.3.2

Limited release.

Luna HSM 5.3.1

Luna HSM 5.3.1 is a replacement for release 5.3.0, meaning that 5.3.1 is complete, and does not require any part of 5.3.0. The only change is the addition of a fix for an SSH issue in Luna SA (see Issue LHSM-10158, in Addressed Issues, later in this document). If you are updating from release 5.3.0, your only mandatory action is to download the Luna SA software update from the SafeNet Service Portal and install it on every 5.3.0 Luna SA.

However, the full release with all components is provided for customers wishing to update from a version older than 5.3.0.

The main user documentation is still the 5.3.0 document set (WebHelp).

Reason for Release 5.3.1

An issue in the appliance software of Luna SA 5.2.x and 5.3.0 causes SSHD to become inoperable after the command `sysconf ssh regenKeyPair` is run from the administrative shell, `lunash`. If that is allowed to happen, then the appliance can no longer be accessed via SSH, and you cannot transfer files to the appliance. The appliance must then be returned to SafeNet for repair, via the RMA process.
This update pro-actively fixes the issue for customers who have not yet run the command.

Shipping of affected units was halted as soon as the problem was discovered, and resumed only after the fix was in place at the SafeNet factory. For Luna SA 5.3.0 units already in the field, this is a mandatory update.

This document has been revised to address issue **LHSM-9897: WebHelp does not work with IE 11 and Chrome 30+**. See "Addressed Issues" on page 12 for more information.

What to Do with Luna HSM 5.3.1 Update

If you have any Luna HSM before 5.0, there is no update path, only migration of key material.

All the components are under the Luna 5.3 heading on the SafeNet service portal (https://serviceportal.safenet-inc.com).

If your Luna HSM is at version 5.0 or 5.1, then upgrade to version 5.2.3, first.

If your Luna HSM is at version 5.2.0, or 5.2.1, or 5.2.2, or 5.2.3, then download all components and update directly to version 5.3.1; there is no need to install 5.3.0, since 5.3.1 is a complete, independent replacement for those versions. If you are coming from Luna SA 5.2.1 or 5.2.2, upload the Luna SA Appliance Update to all of your affected Luna SA appliances and apply the update immediately after you upload it.

If your Luna HSM is already at version 5.3.0, **only** Luna SA must be updated to version 5.3.1 (urgently). For the other Luna HSMs (Luna PCI-E and Luna G5), no action is needed.

New Features and Enhancements

Luna HSM 5.3.5 introduces some new features and improvements since release 5.2, as follows:

Features that do not require firmware 6.20.0

Crypto Command Center Improvement

Crypto Command Center has improved installation, and now automatically populates HSM/appliance attributes when the HSM is added. A “refresh” option is included for the situation where an HSM’s capabilities are upgraded after it has been added in CCC.

Enhanced Update/Upgrade Process for HSMs in HA

The update process has been enhanced to minimize or eliminate any disruption of availability when members of an HA group are updated one at a time.

Portions of Enhanced HSM and Appliance Monitoring Via SNMP

Introduction of the SAFENET-HSM MIB and the SafeNet subagent extends the scope and granularity of information available va SNMP. Many of the SNMP improvements will work without upgrading from firmware 6.2.1, but see below.

Features that require firmware 6.20.0

HSM Usage Monitoring

New HSM Monitor commands now supply some statistics such as, HSM up-time, command counts, and utilization counters.

Enhanced HSM and Appliance Monitoring Via SNMP

Introduction of the SAFENET-HSM MIB and the SafeNet subagent extends the scope and granularity of information available va SNMP. Most of the SNMP improvements will work without upgrading from firmware 6.2.1, but reporting of some functions, such as operational counters, requires firmware version 6.20.x or newer.

Improved Performance for ECDSA Signing and Verification

ECDSA P192/256/384 signing speeds have improved:

- ECC P192: from 740 to 3000 operations/second
- ECC P256: from 1000 to 2000
- ECC P384: from 800 to 1000

SHA224 or 256 ECDSA sign/verify speeds have improved:

- P192: from 90 to 1000
- P256: from 60 to 670
- P384: from 32 to 340

For ARIA ECB/CBC/OFB encryption of small data size, our testing has shown an average 100% increase in performance (there are too many sub-mechanisms and key sizes to list here – contact SafeNet Sales or Technical Support).

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 5.3.5.

Firmware update is required for 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 6.20.0.

HSM Firmware 6.20.0 and FIPS 140-2

Firmware 6.20.0 implements some features of release 5.3, but will not be a FIPS-validation candidate.

Luna HSMs with HSM firmware version 6.10.2 (from Luna HSM 5.2.5 release) are in the evaluation process for FIPS validation. Until firmware version 6.10.2 achieves validation, the validated firmware for Luna PCI-E and Luna SA is f/w 6.2.1; the validated firmware for Luna G5 is f/w 6.2.3. If you currently require FIPS validation, your HSM firmware must remain at those versions. The Luna Backup HSM continues to ship with firmware 6.0.8 with the same possibility to upgrade to newer firmware.

For Luna SA, if you update to Luna 5.3 software on the appliance (which includes the option to update the HSM firmware to 6.20.0), that would displace the standby firmware update option 6.10.2. When firmware 6.10.2 achieves FIPS validation, you would not have that upgrade option available on your Luna SA – having displaced it with firmware 6.20.0 as the standby upgrade option. Please plan ahead, with that in mind.

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

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
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)

Chrystoki.conf File Issues When Uninstalling the Luna Client on a Debian OS

In some instances, you might wish to perform a complete re-install of the Luna client, including replacing your **Chrystoki.conf** file with the default version. If you want to do this on a Debian OS, after you uninstall the client you must purge the **libcryptoki** library **before** you delete your old **Chrystoki.conf.debsave** backup file.

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**

Luna SA integration with Oracle WebLogic

Currently, Luna SA is not integrated with Oracle WebLogic because of a key verification problem that developers from the two companies are working to resolve.

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.

New Capabilities and Policies – Do Not Use

Commands like **hsm showPolicies** now display three new capabilities and their attendant policies. Please ignore these (*). 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
```

jMultitoken Has a Few Issues That Could Cause Confusion

If you are using the jMultitoken demonstration utility, be aware of the following:

- Perform any operation that does not use digest or curve (ie. RSA or DSA), run it, then stop it. Digest and curve drop-boxes are now selectable and any value can be chosen but the HSM does not support digest or curve operations. No error occurs when this is run, though the curve and digest are ignored.
- DSA has a 2048-bit option, though it only supports 512 and 1024. When this is selected and run, an error occurs. The 2048 option should be removed.
- Depending on the Digest chosen, RSAwithDigest (SHAx) might not support 256-bit or 512-bit keys. An error is generated. If the algorithm/digest does not support a given key size, it should not be an option.
- ECC (NOT ECCwithDigest) has the same problem as listed above: run an operation, stop it, then Key Size and Digest are selectable. These are ignored, and no error is generated, but results could be confused with ECCwithDigest.

"Paper" licenses vs. software-enforced licenses for HSM Partitions.

For Luna SA, multiple partitions can be deployed within the HSM, the number determined by purchased licenses. In the past, each HSM was capable of the full complement of 20 partitions, with customers agreeing to use only the number for which they had paid, per Luna SA HSM. These were called "paper" licenses, or contract licenses. In recent versions SafeNet has changed the partition licensing system, placing it under software control, keyed to the individual HSM's serial number. On behalf of customers who already own Luna SA 5.x units, SafeNet has implemented the following transition strategy:

- Customers with Luna SA 5.0 and 5.1 received from the factory continue to use paper licenses for upgrades.
- Customers with older versions upgraded to Luna SA 5.2.1, or subsequent releases, also continue to use paper licenses for upgrades.
- Partition upgrades enforced by software start with Luna SA 5.2.1 shipped from the factory.

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 this release at the time of this document's 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

The following table lists the supported firmware/software versions for the various components supported in Luna HSM 5.3.5 (Luna SA now 5.3.5, all other Luna HSMs and components remain at 5.3.1 equivalents

Component	Version
HSM firmware	6.2.5 (upgradable to 6.20.2)
Luna G5 firmware	6.2.5 (upgradable to 6.20.2)
Luna Remote Backup HSM firmware	6.0.8 (upgradable to 6.20.2)
PED Workstation software (requires Remote PED) [optional]	1.0.5
Luna PED2 / PED2 Remote	2.5.0-3 or newer
Client software	5.3.0
Luna SA appliance software	5.3.5

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.

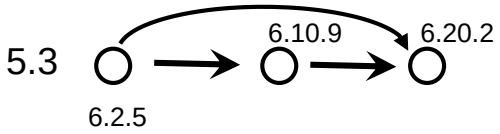
Upgrade Paths for Secure Firmware

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 “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 FW Releases	Recommended FW	FIPS Target
5.3 /6.20.0	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

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



Earlier

Upgrade to this version from previous versions shown in the table.

Component	From version...	To version...
Luna Client software	Any	5.3.0
Luna SA appliance software	5.2.4, 5.2.6 5.3.0, 5.3.1, 5.3.3, 5.3.4	5.3.5
HSM firmware	6.2.1, or 6.2.3*, 6.10.1, or 6.10.2	6.20.0**

*Luna G5
** Superseded by version 6.20.2

Supported Operating Systems

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

Luna Client

Any Windows or Linux or version listed as supporting Luna SA 5.3.x in the following table is also supported if used under VMWare, XEN, or Microsoft HyperV virtualization environments. Other operating systems are not currently tested with Luna SA 5.3.x client software in a virtualized environment.

The 32-bit client will run on a 64-bit OS for all supported operating systems.

Operating System	Version	32-bit client	32-bit client on 64-bit OS	64-bit client
Windows	2008 R2	No	Yes	Yes
	2012	No	Yes	Yes
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)	10	No	Yes	Yes
	11	No	Yes	Yes
Solaris (x86)	10	No	Yes	Yes
	11	No	Yes	Yes
HP-UX	11.31	No	Yes	Yes
AIX	6.1	No	Yes	Yes
	7.1	No	Yes	Yes

Crypto Command Center

Operating System	O/S kernel architecture	32-bit library	64-bit library
CentOS 6	32 bit	Yes	No
	64 bit	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
- OpenSSL 0.9.8x
- 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. (The part numbers below are for the field-installable version.)

Upgrade Description	Part number	Compatibility	
		Software	Firmware
Korean non-destructive (See Note 1)	908-000139-001	Luna SA 5.1.0	6.2.1
Korean destructive (See Note 2)	908-000166-002	Luna SA 5.1.0+	6.2.1+
	908-000138-002	Luna PCI-E 5.1.0	6.2.1
	908-000156-002	Luna G5 5.1.0	6.2.1
Maximum memory	908-000086-001	Luna SA 5.0.0+	6.0.8+
	908-000154-001	Luna PCI-E 5.0.0+	6.0.8+
ECIES acceleration	908-000175-001	Luna SA 5.2.1+	6.10.2+ (See Note 3)
	908-000177-001	Luna PCI-E 5.2.1+	6.10.2+ (See Note 3)
	908-000179-001	Luna G5 5.2.1+	6.10.2+ (See Note 3)
5 partitions	908-000201-001	Luna SA 5.2.1+	6.2.1+
10 partitions	908-000202-001	Luna SA 5.2.1+	6.2.1+
15 partitions	908-000203-001	Luna SA 5.2.1+	6.2.1+
20 partitions	908-000204-001	Luna SA 5.2.1+	6.2.1+

Upgrade Description	Part number	Compatibility	
		Software	Firmware

Note 1: Deprecated.

Note 2: The destructive version is the preferred version, which enforces compliance with standards – your auditors will prefer that you add the ability to use Korean algorithms by means of the destructive version of the upgrade.

Note 3: This upgrade (Luna HSM 5.3.1) 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 (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.

The symbol " + " after a software or firmware version means that the Configuration Upgrade can be applied to Luna products with the indicated software or firmware version, or newer.

Luna 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

Windows/Linux

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

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.
Dell R710	Single card in any of slots 1, 2, 3, 4, or 5. Passes 3-card test.
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.
Fujitsu Primergy RX 200 S6	Single card in slot 1.
HP DL 380 G2 AMD-based	Single card in any of slots 1 or 2. Passes 2-card test.
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 Server RX2660	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:

- “Common Luna Addressed Issues” on page 13
- Luna SA Addressed Issues” on page 14
- “Luna PCI-E Addressed Issues” on page 15

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-9897) WebHelp does not work with IE 11 and Chrome 30+	M	**Problem:** The product documentation (WebHelp) is displayed incorrectly, or not at all, when browsed using Internet Explorer 11 or Google Chrome 30 and higher. **Resolution:** The documentation has been rebuilt to fix this issue, and is available for download. Contact SafeNet Technical Support for more information.
(LHSM-5788) Circumvention of Vaudenay CBC Padding Oracle Attack Fix	C	**Problem:** An exploit was fixed to prevent a Vaudenay CBC padding oracle attack. The customer later found a variant of the original attack that circumvented the fix. CBC Padding is inherently insecure, but some customers need/want to use it nevertheless. **Resolution:** The latest fix adds the HSM capability/policy to “Enable CBC-PAD (un)wrap keys of any size”. If this is DISabled, then CBC-PAD (un)wrapping is restricted to keys that are multiples of 64-bits. The policy is worded this way (enabled by default) for benefit of customers with legacy applications.
(LHSM-3452) Documentation Error: 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.
(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 main product documents – See the section “Java Library Path Issue” in the Windows Installation instructions

Issue	Severity	Synopsis
(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 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 5.3.5 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 5.3.5.

(LHSM-10158) Starting sshd failed after ssh regenKeyPair	H	**Problem:** After update of Luna SA to version 5.2.1 or 5.2.2 or 5.3.0 (incorporating newer version of OpenSSH), SSH fails following command "sysconf ssh regenKeyPair".
		`[local_host] lunash:>sysc ssh regenkeypair`
		`WARNING !! This command regenerates SSH keypair.`
		`WARNING !! SSH will be restarted.`
		`If you are sure that you wish to proceed, then type 'proceed', otherwise type 'quit'.`
		`> proceed`
		`Proceeding...`
		`Stopping sshd: [ OK ]`
		`Starting sshd: [FAILED]`
		`Command Result : 65535 (Luna Shell execution)`
		`[local_host] lunash:>sysc fi s`
		`SSH Server Public Keys`
		`Type Bits Fingerprint`
		`------------------------------------------------------------`
		`Error: SSH server RSA public key file not found. Please contact customer support.`
		`Error: SSH server DSA public key file not found. Please contact customer support.`
		`Command Result : 65535 (Luna Shell execution) [local_host]`
		Resolution: All shipments were halted until the fix was applied at the factory. Customers with Luna SA 5.x were alerted. The fix is released as Luna HSM 5.3.1 update. Upload the update to your Luna SA and apply it immediately.

Issue	Severity	Synopsis
(LHSM-3389) Show crypto operation counts in Luna SA	M	**Problem:** "hsm info show" lunash command output adds these 2 counters, which capture the number of successful crypto operations and failures: Crypto Operation Requests: 44099950 Crypto Operation Errors: 0 **Resolution:** As noted.
(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.
(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 HA group does not delete HA entries in client config file	M	**Problem:** Deleting the HA group does not delete HA entries in the client configuration file. **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.

Known Issues

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

- “Common Luna Known Issues” on page 16
- "Luna SA Known Issues” on page 21
- “Luna PCI-E Known Issues” on page 23
- “Luna G5 Known Issues” on page 25

Note In the following tables, some issues are tracked either in our old database (MKS, with the six-digit numbers) or in our new database (JIRA, 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-7035) Can't 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". **Workaround:** n/a.

(LHSM-7032) RBS: client can't read RBS HSM information if rbs doesn't 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`
		`lunacm:>`

(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 G5, 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.

Issue	Severity	Synopsis
(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 don't 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 main documentation.

(LHSM-5827) pedserver can't 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-5812, MKS#176840) Crypto-User cannot create objects when using an HA group	M	**Problem:** Some customers prefer operating as the Crypto User rather than Crypto Officer. When operating in java the provider needs to create certificate and public key objects, which are used ephemerally. Typically this works, but when operating with an HA group the Crypto User receives a failure message indicating it does not have permissions to perform the CreateObject operation. This is due to the Crypto User not having permission to perform network replication / cloning. The Crypto User should have permissions to replicate any object it is able to create. **Workaround:** Perform these operations as Crypto Officer.
(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 not being transfered to host. **Workaround:** None.
(LHSM-5790) “lunacm” doesn’t display other HSM’s connected with broken htl client connection	M	**Problem:** “lunacm” doesn’t 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.

Issue	Severity	Synopsis
(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. **Workaround:** None.
(LHSM-2864) HA Key gens don't 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.
(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, in case the user enters a wrong password. **Workaround:** None.
(190048) 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.
(188646) Windows "remove" from msi installer doesn't remove client	L	**Problem:** Windows "remove" from the LunaClient.msi installer should allow customer to remove Luna HSM client completely. Currently, it takes you through the menus, runs through the motions, and results in no changes for installed client. **Workaround:** Invoke Start > Control Panel > Programs > Uninstall a program (or the equivalent sequence in your version of Windows).
(188269) Windows "repair" does not work from msi installer	L	**Problem:** In Windows, the Repair option from the LunaClient.MSI installer does nothing. **Workaround:** From Control Panel, go to Programs and Features, and select the Repair option.
(188266) Windows "modify" does not modify the installed Luna Client	L	**Problem:** Windows Modify (in Windows Programs and Features) should allow you to add/remove Luna HSM components. Currently, it takes you through the menus, runs through the motions, and results in no changes to your configuration. **Workaround:** Using Programs and Features (accessed via Windows Control Panel, or other means), uninstall LunaClient software completely, and then re-install it with the required components.

Issue	Severity	Synopsis
(187000) 32-bit JVM Java on 64-bits CentOS does not run if SELinux is enabled	L	**Problem:** If SELinux is enabled, you cannot run a 32-bit JVM on a 64-bit OS. **Workaround:** Disable SELinux.
(186046) The **-p** and **-password** options for the **partition login** command are not recognized for HA slots	M	**Problem:** If you use the **-p** <password> or **-password** <password> options for the **partition login** command when logging into an HA slot, the option is not recognized and you are prompted to enter the password. **Workaround:** Do not use the **-p** or **-password** options when logging into an HA slot. You will be prompted for the password instead.
(LHSM-5795 MKS185978) Cannot use **lunacm** to restore a backup partition	M	**Problem:** If you attempt to use **lunacm** to restore a partition from a Luna backup HSM, **lunacm** is unable to find the partition and the backup fails. **Workaround:** Use **vtl** to restore backup partitions.
(183503) LunaProvider: ECDH with KDF does not work in some situations	M	**Problem:** ECDH with KDF provide interoperability between the Luna provider and the BC provider, when performing CMS operations, by including shared information, such as key length and algorithm with, each request. However, this information is not included for non-CMS operations, which might cause secret key derivations to fail. **Workaround:** None.
(183431) Crypto Command Center fails to initialize a device if only 1 HSM admin login attempts is left before zeroization	M	**Problem:** If you enter the wrong password twice on the Crypto Command Center Initialize Device page, the device will not be initialized if the correct password is entered on the third attempt. It will also not be zeroized. **Workaround:** Ensure that you enter the correct password on the first or second attempt.
(182201) JCPROV HALogin API does not work	M	**Problem:** The JCPROV HALogin API does not work. **Workaround:** None.
(180921) Drivers install incompletely when devices are not connected - Luna G5, Luna Remote Backup HSM and Luna Remote PED drivers	M	**Problem:** On both Windows 2003 32-bit and Windows 2008 R2 when installing the USB drivers (Luna G5, Luna Remote Backup HSM and Luna Remote PED products), with the devices not connected, the drivers are partially installed as the .inf files are installed but not the .sys files. If the devices are connected before installing the drivers, they are installed properly and work fine. **Workaround:** 1) Connect the devices before installing LunaClient. 2) If LunaClient software (which includes the drivers) is installed before devices are connected, then connect the device(s), reboot the computer, and allow Windows to discover the new devices and complete the driver install.
(180345) 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.

Issue	Severity	Synopsis
(179677) Ambiguous LunaProvider error message when libLunaAPI incorrect or not found	L	**Problem:** When the LunaProvider cannot find the libLunaAPI library, or if the libLunaAPI library is incorrect, the following message is displayed: `Failed to load LunaAPI and LunaAPI_64 libraries` This message is ambiguous in that it is displayed on both 32 and 64-bit operating systems, potentially causing confusion. **Workaround:** None.
(176696) Unable to use cmu to import p12/PFX files	M	**Problem:** If you attempt to use the **cmu importkey** command to import a p12/PFX file, the operation fails with an error message. **Workaround:** None.
(176594) Java 7 library path issues on Windows 2008 R2	H	**Problem:** When installed in the default location, Java 7 might not find and load LunaAPI.dll on Windows 2008 64. **Workaround:** If the JSP does not work, copy LunaAPI.dll to the current directory (or any directory in the path such as C:\windows\system32) to resolve the issue.
(173299) jMultiToken does not support rsa186 -3 keygen	M	**Problem:** There is no option for rsa186 -3 keygen when you run jMultitoken. **Workaround:** None.
(172230) jMultitoken does not support ECIES and KCDSA	M	**Problem:** jMultitoken does not support ECIES and KCDSA **Workaround:** Use multitoken.
(168352) LunaProvider fails to sign with RSA keys that have a modulus that is not evenly divisible by 8	M	**Problem:** The LunaProvider.jar (all versions) fails when performing a sign operation with an RSA key that has a modulus which is not evenly divisible by 8. The provider uses the key modulus (size) to determine how to construct the buffer for the signature value, but in the case of a key with a leading 0, or a non-standard sized key (we do not generate those keys, but they are allowed) a buffer will be generated which is too short. **Workaround:** None.
(161087) The **sysconf ntp deleteserver** command allows deletion of the NTP pseudo IP (127.127.1.0)	M	**Problem:** If NTP loses synchronization with the remote server, it will synchronize against itself using pseudo IP address 127.127.1.0 until it can start synchronizing with the remote server again. Although you should be prevented from deleting this pseudo IP address, deletion is allowed using the **sysconf ntp deleteserver** command. **Workaround:** None. Use caution when using the **sysconf ntp deleteserver** command to ensure that you do not delete the NTP pseudo IP address (127.127.1.0).
(161075) SunPKCS11 Provider: Bad DSA Signature returns CKR_DEVICE_ERROR	M	**Problem:** When the Java SunPKCS11 Provider validates the DSA signatures on the providers listed in the **java.security** file it encounters a bad signature (S is greater than Q). As a result, the HSM returns a CKR_DEVICE_ERROR, causing a Java exception. **Workaround:** None.
(161071) LunaProvider does not fully support third-party created double length DESede keys	M	**Problem:** DESede keys created using a third-party Java provider are assumed to be 24 bytes long, although 16-byte keys are also possible. Attempting to unwrap a 16-byte DESede key onto the HSM using the LunaProvider causes the operation to fail. **Workaround:** Create a new DESede key which repeats the first 8 bytes in the last 8 bytes. For example, a key with the value 12345678ABCDEFGH becomes 12345678ABCDEFGH12345678.
(161067) IIS server cannot bind with lunaCSP (Windows 2008 R2 64-bit)	M	**Problem:** IIS server cannot bind with lunaCSP (Windows 2008 R2 64-bit) **Workaround:** None.

Issue	Severity	Synopsis
(161059) G5 PKI bundle HA feature does not recover from USB unplug	L	**Problem:** If the USB cable connecting a Luna G5 and Luna SA in a PKI bundle HA configuration is disconnected, traffic does not recover when the USB cable is reconnected. **Workaround:** Restart the client applications.
(161045) RADIUS authentication currently unsupported	M	**Problem:** Although RADIUS user authentication is available in this release, it has not been adequately tested and is therefore not officially supported. **Workaround:** None. Although you can use the feature, it is unsupported. SafeNet is working to complete verification of the feature in the post-GA timeframe.

Luna SA Known Issues

Issue	Severity	Synopsis
(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 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-3845, MKS#182861) Incorrect Message Authentication error in Weblogic and Luna SA Integration	H	**Problem:** Problem integrating Luna SA 5.x with Oracle WebLogic. Message Authentication Error. Currently, Luna SA is not integrated with Oracle WebLogic because of a message authentication problem that developers from the two companies are working to resolve. **Workaround:** None.

(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; }`
		Workaround: Ignore.

Issue	Severity	Synopsis
(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". **Workaround:** Ignore.
(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. **Workaround:** Use without HTL when ipcheck is disabled.
(186997) Erroneous message displayed during firmware upgrade	M	**Problem:** During a firmware upgrade, the following error message might be displayed: **EncryptInit() using PE1746 failed, disabling PE1746.: Cannot allocate memory** You can ignore this message. **Workaround:** None.
(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. **Workaround:** If you stop the HTL service while lunacm is running, stop lunacm too. Do not use HTL in an already-running lunacm session
(184186) The number of retries specified in the **vtl haadmin autoRecovery -retry** command is ignored	M	**Problem:** If you use the **vtl haadmin autoRecovery -retry** <retries> command to specify an explicit number of retries for a failed HA member, the specified value is ignored, and an unlimited number of retry attempts are performed instead. **Workaround:** None.
(171722) lunacm **slot partitionList** command displays incorrect name for Luna SA network slots	M	**Problem:** Rather than displaying the correct slot name, the slot partitionList command displays the name of the partition configured for client use with the **crystoki.ini** (Windows) or **Chrystoki.conf** (Linux) file. **Workaround:** None.
(161105) Intermittent faults when stopping or starting NTLS on an HA member	M	**Problem:** Very rarely, a segmentation fault, broken pipe, or application exit might occur when stopping or starting NTLS on an HA member. **Workaround:** None.
(161104) Extraneous information displayed by ckdemo HA Status option (option 52)	M	**Problem:** The ckdemo HA Status option (option 52) displays extraneous information. For example: Enter your choice : 52 HA group 1150485010 status **HSM 224213213691 - CKR_UNKNOWN** (extraneous information) HSM 150485010 - CKR_OK HSM 150576010 - CKR_OK Status: Doing great, no errors (CKR_OK) **Workaround:** Ignore the extraneous information.
(161028) 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 CUF that, once applied, enables unmasking.

Issue	Severity	Synopsis
(161002) Luna SA client unable to access more than 16 appliances	M	**Problem:** When adding more than 16 appliances to a client, only the first 16 are seen in **vtl verify** or in **ckdemo**'s list of available slots. In addition, if you add appliances number 17 and 18, and then delete some of the first 16 appliances the additional appliances are still not seen by the client. If those same appliances (17 and 18) are deleted and then re-added after deleting lower slot appliances they will be re-added at lower slot numbers and then be able to be accessed by the client. **Workaround:** None.

Luna PCI-E Known Issues

Issue	Severity	Synopsis
(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
(160971) lunacm unable to read information from the K6	M	**Problem:** Intermittent issue where lunacm reported that it was not able to read information from the HSM. **Workaround:** Use **vreset** to get the HSM responding again.

(160856) The function GetConfigurationEntry() in the ChrystokiConfiguration class does not work properly	M	**Problem:** The function GetConfigurationEntry() in the ChrystokiConfiguration class does not work properly.
		This function is used on Linux/Unix to parse the .conf file.
		If your conf file contains the following
		Chrystoki2 = {
		LibUNIX64=/dummy;
		LibUNIX=/usr/lib/libCryptoki2.so;
		}
		GetConfigurationEntry() will incorrectly try to use the LibUNIX64 entry because it only tries to match "LibUNIX" and ignores the rest.
		This function should be more specific when it is comparing strings.
		Workaround: Use one or the other entry in .conf file, or adjust the order of the entries so that the desired entry is found first.

(160806) setlegacy domain does not accept default domain in ckdemo	L	**Problem:** During key migration testing from PCM to PCI5.0, it was found that there is no way to input default which is an empty string for setlegacydomain in ckdemo. In this case, there is no way to do key migration with ckdemo if PCM PW-Auth was using default domain. **Workaround:** Use lunacm.
(160774) **cmu generatekeypair** for DSA does not accept subprime in interaction mode	M	**Problem:** **cmu generatekeypair** for DSA does not accept subprime in interaction mode while it has been accepted in command line mode. **Workaround:** Use command-line mode.

Issue	Severity	Synopsis
(160765) Adding or removing a member to an HA group using HSM serial number is broken	L	**Problem:** Cannot add/remove a member from an HA group using the serial number of the HSM. lunacm:> ha r -se 753951 -g myHA -p userpin Error: Failed to open a user session on slot 0. Command Result : 0x3 (CKR_SLOT_ID_INVALID) lunacm:> **Workaround:** Add/remove with the slot number. lunacm:>ha r -slot 3 -group myHA -password userpin Member 753951 successfully removed from group myHA. New group configuration is: HA Group Label: myHA HA Group Number: 150031 Group Members: 150024, 150031 Needs sync: no Command Result : No Error lunacm:>
(160754) Timeout sometimes occurs during remote backup with append option	M	**Problem:** During appended remote backup, sometimes got timeout (depending on operator speed) when attempting to re-size a partition on the backup HSM. Looks like this: lunacm:>partition backup backup -slot remote -hostname 172.20.11.130 -port 2222 -debug -partition backuppartition1 -append The partition backuppartition1 will be resized. recv(): timed-out setContainerSize_Client(): failed to read cmd result (-110) Error: failed to resize partition backuppartition1 on remote device. Command Result : 0x5 (CKR_GENERAL_ERROR) lunacm:> **Workaround:** Specify a longer commandtimeout setting when issuing the remote backup command from lunacm. Here is a workaround example specifying -ct as 20 seconds: lunacm:>partition backup backup -slot remote -hostname 172.20.11.130 -port 2222 -partition backuppartition1 -append -commandtimeout 20 The partition backuppartition1 will be resized. Verifying that all objects can be backed up... 4 objects will be backed up. 17 objects will not be backed up because they are duplicates. Backing up objects... Cloned object 43 to partition backuppartition1 (new handle 256). Cloned object 44 to partition backuppartition1 (new handle 257). Cloned object 47 to partition backuppartition1 (new handle 260). Cloned object 48 to partition backuppartition1 (new handle 261). Backup Complete. 4 objects have been backed up to partition backuppartition1 on remote device. Command Result : No Error lunacm:>

Issue	Severity	Synopsis
(160731) Driver errors when clearing full partition on HSM	M	**Problem:** After filling up a partition with small key objects (88 byte AES keys), and clearing the partition using the par clear command, these errors appear in syslog. n 7 16:45:10 harvey kernel: ERR: viper0: _rx: user rsp buf 2 small rxhdr cmd=00, msb(00000035) lsb(0000009c) rxoffset(000035a0) dataleft(00000040) Jan 7 16:45:10 harvey kernel: ERR: viper0: _rx: too small user's response buffer, cmd=0x16(?), size (00006b40) > rxmaxsize (00004408) Jan 7 16:45:10 harvey kernel: ERR: viper0: _rx: user rsp buf 2 small cmd=0x16(?), rxcount(000035a0) rxoffset (000035a0) insize (00000040) blksize (0000359c) Jan 7 16:45:11 harvey kernel: ERR: viper0: _rx: user rsp buf 2 small rxhdr cmd=00, msb(00000035) lsb(0000009c) rxoffset(00006b40) dataleft(00000040) **Workaround:** The driver and HSM card are still working so the reported errors don't appear to have consequences - ignore.
(160728) RSA with MGF1 is missing from jMultitioken	M	**Problem:** During performance testing on jMultitoken, we found RSA with MGF1 algorithms were missing from jMultitoken cross all supported clients. We don't support RSA with MGF1 for small key sizes (256 and 512), but the HSM does support key size 1024 and larger. **Workaround:** None.
(160721) **lunacm** command syntax summary not consistent	L	**Problem:** The command syntax summary that is presented when the user types a **lunacm** command followed by "**?**" is not consistent for all **lunacm** commands. **Workaround:** None.
(160706) 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.

Luna G5 Known Issues

Issue	Severity	Synopsis
(190597) 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.

Issue	Severity	Synopsis
(190451) Client tools fail to recognize attached G5 and Backup G5 on Dell R710.	M	**Problem:** Client tools do not recognize the attached G5 and back up G5 HSMs on Dell R710, until system is rebooted. **Workaround:** Reboot the system.
(190450) Client tools fail to detect G5 on 'unplug and re-plug' operations.	H	**Problem:** When 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
(190409) 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

(188376) trace messages every 5 seconds for G5 - lunauhd1	M	**Problem:** When Luna G5 is connected to a Windows client with audit logging NOT configured, then trace messages, similar to the following, appear every 5 seconds.
		`53 0x80000d02 00271 SOURCE/LUNA2/LOG_MOD/log_gen.c`
		`54 0x80000d02 00271 SOURCE/LUNA2/LOG_MOD/log_gen.c`
		`55 0x80000d02 00271 SOURCE/LUNA2/LOG_MOD/log_gen.c`
		`56 0x80000d02 00271 SOURCE/LUNA2/LOG_MOD/log_gen.c`
		`57 0x80000d02 00271 SOURCE/LUNA2/LOG_MOD/log_gen.c`
		After audit log is enabled and the audit log path is properly configured, the messages cease.
		For a Linux client, if a "fresh" Luna G5 HSM is connected, the messages do not appear. However, if the connected Luna G5 HSM was configured for audit logging using Windows, before moving the HSM to the Linux client, then messages like the following occur every 5 seconds.
		`Apr 22 11:28:20 localhost kernel: lunauhd1: TRACE: 20 0x80000d02 00271 SOURCE/LUNA2/LOG_MOD/log_gen.c`
		`Apr 22 11:28:25 localhost kernel: lunauhd1: TRACE: 21 0x80000d02 00271 SOURCE/LUNA2/LOG_MOD/log_gen.c`
		`Apr 22 11:28:30 localhost kernel: lunauhd1: TRACE: 22 0x80000d02 00271 SOURCE/LUNA2/LOG_MOD/log_gen.c`
		`Apr 22 11:28:35 localhost kernel: lunauhd1: TRACE: 23 0x80000d02 00271 SOURCE/LUNA2/LOG_MOD/log_gen.c`
		Workaround: Ignore the messages, or configure audit log correctly for the current system, to stop the messages.

(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.
(161131) Rollback from FW 6.2.x to 6.0.8 is destructive	L	**Problem:** Although firmware rollback is supported, rolling back the firmware from 6.2.x to 6.0.8 will reset the HSM and remove the existing partition. Any objects created under firmware 6.2.x will no longer exist after the rollback. **Workaround:** None. If you perform the rollback, the lost objects are not recoverable. Always backup the data on your HSMs.

Issue	Severity	Synopsis
(160504) Unplugging/plugging back in G5 will eventually fails to reset it correctly	M	**Problem:** Repeatedly disconnecting and reconnecting the USB cable between Luna G5 and your computer can put the Luna G5 into an "undefined" state that shows in lunacm as firmware 0.0 and "undefined" mode. **Workaround:** Power-cycle the Luna G5, waiting 30 seconds before reconnecting the power cord.

Support Contacts

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 Connection Center	https://serviceportal.safenet-inc.com Existing customers with a Customer Connection Center 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.

Copyright 2015. All rights reserved.

Luna and the SafeNet logos are registered trademarks of SafeNet, Inc.