Luna HSM 5.2.6

CUSTOMER RELEASE NOTES

Document part number: 007-012225-001 Revision N
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_5-2.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

Luna HSM 5.2 Security Patch

This firmware patch, for Luna G5 and Luna PCI-E and Luna SA, to firmware version 6.2.5, and to firmware version 6.10.9, 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 5.2.6

Luna HSM 5.2.6 is a Luna SA-only release, 630-010165-022, which includes the previous 5.2.x releases and patches, as well as firmware 6.10.9 (formerly 6.10.2).

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 5.2.6 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 5.2.5

Limited release.

Luna HSM 5.2.4

Luna HSM 5.2.4 is a Luna SA-only release, 630-010165-019, which includes the previous 5.2.x releases and patches, as well as firmware 6.10.2.

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 5.2.3

Luna HSM 5.2.3 is a full replacement for release 5.2.1, and 5.2.2, meaning that 5.2.3 is complete and does not require any part of 5.2.1 or 5.2.2.

The ONLY change from release 5.2.1 to 5.2.2 was the replacement of Firmware Update Files (FUFs) in the \firmware\PCI and the \firmware\G5 directories in the installation tarball, replacing version 6.10.1 with 6.10.2 (should be 6.10.7). All client software (libraries, tools, drivers, etc.) was completely unchanged. The user documentation was unchanged and is still the 5.2.1 WebHelp.

For release 5.2.3, no change at all was made to the client software, nor to the user documentation. The Client installer still identifies as version 5.2.1, and the documentation identifies as version 5.2.1. The only change is a separately downloadable Appliance Update for Luna SA, which is mandatory for customers updating existing Luna SA systems. If you bought your Luna SA system at version 5.2.3 from the factory, the update was already installed.

Reason for Release 5.2.3

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 5.2.x units already in the field, this is a mandatory update.

This document has been revised to add the following issues to "Addressed Issues" on page 12:

- LHSM 10553: Luna SA HSM Lockup
- LHSM-9897: WebHelp does not work with IE 11 and Chrome 30+
- (MKS 164993) NTLS Crash and Burn

What to Do with Luna HSM 5.2.3 Update

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

All the components are under the Luna 5.2.3 heading on the SafeNet service portal (https://serviceportal.safenet-inc.com).

If your Luna HSM is at version 5.0, 5.1, or 5.2.0, then download all components and update directly to version 5.2.3; there is no need to install 5.2.1 or 5.2.2, since 5.2.3 is a complete, independent replacement for those versions. 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 5.2.1 or 5.2.2, then **only** Luna SA must be updated to version 5.2.3 (urgently). For the other Luna HSMs, no action is needed.

New Features and Enhancements

Luna HSM 5.2.x introduces the following features:

Features that do not require firmware 6.10.7

Host Trust Link (HTL)

HTL provides secure connectivity for VM-based clients to protect against the theft of at-rest virtual clients.

Consolidated Luna Client

The Luna client software is delivered as a single consolidated package that works with all HSM form factors (Luna SA, Luna PCI-E and Luna G5). The Luna firmware is also consistent, ensuring applications work with all HSM form factors.

HSM Driver Timeout Is Now Adjustable

The previously hard-coded timeout, in case the Luna SA HSM failed or lost contact with its appliance, is now configurable with “hsm driver” commands.

HSM Partition and Upgrade Licenses Enforced

All partition licenses and upgrade licenses are now fully locked to individual HSM serial numbers.

Features that require firmware 6.10.9 (formerly 6.10.7)

Crypto Command Center

Crypto Command Center allows service providers or enterprises to easily provision HSM services to consumers using a simple GUI and a pool of Luna SA appliances. Requires HSM firmware 6.10.9

Audit Logging

Secure, signed logs that allow the auditing of all HSM operations. A separate audit role has been created to configure, manage and verify who did what, and when did they do it. This is available with HSM firmware 6.10.9.

New Algorithms

New algorithms are available with firmware 6.10.9, including Rsax931, Rsa186-3keygen, ECIES.

Multiple RemotePED Servers

Multiple RemotePED servers can be used with an HSM. Requires HSM firmware 6.10.9.

RemotePED for USB-Connected HSMs

The RemotePED is now available for Luna G5 and for Luna [Remote] Backup HSM. Requires HSM firmware 6.10.9.

SRK for Backup HSM

The Secure Recovery Key (purple PED Key) feature for Secure Transport and for enforced tamper ackowledgement, is now available for Luna [Remote] Backup HSM. Requires HSM firmware 6.10.9.

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 5.2.6.

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 6.10.7.

SRK Must Be Disabled Before Updating Firmware

If the Secure Recovery Key (SRK) on the HSM is enabled, it must be disabled before you can update the HSM firmware. The SRK is an external split of the HSM's Master Tamper Key (MTK) that is imprinted on the purple PED key. When you disable the SRK, the SRK portion of the MTK is returned to the HSM, so that the MTK is no longer split. It is only in this state that you can update the HSM firmware. After you update the firmware, you can re-enable SRK, if desired, to re-imprint the purple PED with the SRK.

If you attempt to update the firmware without disabling the SRK, the firmware update fails with the following error:

```
Error:  'hsm update firmware' failed. (10A0B : LUNA_RET_OPERATION_RESTRICTED)
```

Connect USB Devices to the Windows Host Computer before Installing Drivers

If your USB devices (Luna G5, Luna Remote Backup HSM or Luna Remote PED) are not connected to the computer on which you are installing the Luna software, the USB drivers do not install successfully. Before installing the Luna software, ensure that any Luna USB-connected devices are connected to the host computer using a USB cable. This issue applies to Windows 2008 only.

Change to Default Chrystoki Library Path May 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
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)

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

In some instances, you may 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**

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.

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.

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.

Remote PED Has Changed

The main Luna HSM Customer Documentation describes the pedClient as it was revised for release 5.2, and gives examples of Remote PED using pedClient at the command line (old way). However, we actually intended for customers to use lunacm commands when configuring and activating Remote PED for Luna PCI-E and Luna G5, and to use Lunash:> when configuring and activating Remote PED for Luna SA. PedClient is installed as part of the Luna Client software (where it runs as a service), and also exists “under the hood” in Luna SA. In both cases, commands are available that present the required functions without invoking pedclient command-line interface.

One difference is how the target HSM is specified for use with Remote PED.

For Luna PCI-E and Luna G5, the command `lunacm:> ped connect –slot <slot>` makes the connection (`ped get` to retrieve pedID). If the slot is not specified in `ped connect`, then the current slot is used by default.

For Luna SA, the `lunash:> hsm ped connect` command uses the serial number of the HSM (could be the onboard K6 HSM card, or any USB-connected PKI-bundle HSM/token). If no serial number is specified, then use of Remote PED, rather than local PED, defaults to the onboard K6 HSM card.

PedClient is still present and can be used by customers who have already been using it directly. Otherwise, pedClient remains available to use in debugging, and as enabling service for audit logging, remote backup and remote PED.

No Dash For vtl haAdmin Sub-Commands

The `vtl haAdmin` command formerly required a leading dash for subcommands. This was changed, but not all instances in the customer documentation were updated. Leading dash is still required for command parameters and options, but is not used with subcommands.

Example: [me@localhost bin]# ./vtl haAdmin HAOnly –enable

“vtl” is the utility

“haAdmin” is the command

“HAOnly” is the subcommand

“-enable” is the parameter or option

Old way: [me@localhost bin]# ./vtl haAdmin -HAOnly –enable

Current way: [me@localhost bin]# ./vtl haAdmin HAOnly –enable

Run vtl commands without sub-commands to see the syntax.

Compatibility and Upgrade Information

This section describes the upgrade paths for this release, compatibility 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 5.2.x 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 in Luna HSM 5.2.6

Component	Version
HSM firmware	6.2.5 (upgradable to 6.10.9)
Luna G5 firmware	6.2.5 (upgradable to 6.10.9)
Luna Remote Backup HSM firmware	6.0.8 (upgradable to 6.10.9)
PED Workstation software (requires Remote PED) [optional]	1.0.5
Luna PED2 / PED2 Remote	2.5.0-3
Luna SA appliance software	5.2.6

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

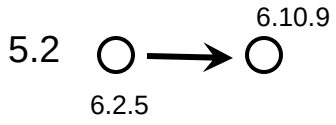
Secure firmware can only be upgraded to higher secure versions. You cannot upgrade to a non-secure version.

The current supported upgrade paths follow. When new firmware is released in the future, please check its associated documentation for upgrade paths.

Software Version/Release FW	Available FW Releases	Recommended FW	FIPS Target
5.2 / 6.10.1	6.2.1	6.2.5 or 6.10.9	Validated
	6.10.1	6.10.9	Validated
	6.10.2		
	6.10.7		

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 version 5.2.6 applies to Luna SA only. Other Luna HSM products are not affected.

Component	From version...	To version...
Luna SA appliance software	5.1.4, 5.1.5 5.2.0, 5.2.1, 5.2.2, 5.2.3, 5.2.4, 5.2.5	5.2.6
HSM firmware	6.0.8 6.1.6 6.2.1 6.2.3 (Luna G5 only) 6.10.1	6.10.9*

(Previous to 5.2.6)
Upgrade to version 5.2.3 from Luna SA 5.1, 5.2.0, or 5.2.1, Luna PCI-E 5.0, 5.2.0, or 5.2.1, or Luna G5 1.3, 5.2.0, or 5.2.1. No upgrade path is provided from previous-generation Luna products, only migration.

Component	From version...	To version...
Luna Client software	Any	5.2.1 (Windows) 5.2.2 (Unix/Linux)
Luna SA appliance software	5.0 5.1, 5.1.1 5.2.0, 5.2.1, or 5.2.2	5.2.3
HSM firmware	6.0.8 6.1.6 6.2.1 6.2.3 (Luna G5 only) 6.10.1	6.10.9*

(* Firmware 6.10.9 replaces all earlier 6.10.x versions for security reasons. Firmware 6.10.9 is validated to FIPS 140-2 Level 2 and Level 3.)

Upgrading From a Luna SA 5.1.x Patch Release

If you are running a Luna SA 5.1.x patch release that is not listed in the table above, you must apply a pre-update patch to revert back to Luna SA 5.1.0 before you can upgrade to Luna SA 5.2.6. The pre-update patch is available for download from the SafeNet Support portal. Contact SafeNet Technical Support for more information.

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 version listed as supporting Luna SA 5.2.6 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 5.2.x client software in a virtualized environment.

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	5.x	Yes	Yes	Yes

variants like CentOS)	6.x	Yes	Yes	Yes
SUSE Linux	10.x	Yes	Yes	Yes
	11.x	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

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 → contact SafeNet Technical Support
- 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.

		Compatibility	
Upgrade Description	**Part number**	**Software**	**Firmware**
Korean non-destructive (See Note 1)	908-000166-001	Luna SA 5.1.0	6.2.1
Korean destructive (See Note 2)	908-000166-002	Luna SA 5.1.0+	6.2.1+
Maximum memory	908-000165-001	Luna SA 5.0.0+	6.0.8+
ECIES acceleration	908-000176-001	Luna SA 5.2.2+	6.10.7+ (See Note 3)
5 partitions	908-000197-001	Luna SA 5.2.2+	6.2.1+

10 partitions	908-000198-001	Luna SA 5.2.2+	6.2.1+
15 partitions	908-000199-001	Luna SA 5.2.2+	6.2.1+
20 partitions	908-000200-001	Luna SA 5.2.2+	6.2.1+

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 is field-installable, but was not installed at the factory – at time of writing – because the then-current factory-installed firmware was 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.
UPDATE!! (2015/07/30) Firmware 6.10.2 must be replaced with 6.10.7 for security reasons. Apply the Security Update Patch according to the Update Sheet instructions that accompany the patch.

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. This section lists the servers that have been tested to work successfully with Luna PCI-E.

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-Fire-V245 Sparc	Single card in slot 1 with Solaris 10.
Dell R710 x86	Single card in any of slots 1 or 2. Passes 2-card test with Solaris 10/11.
Sparc 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 RX2800	Single card in any of slots 1 or 2. Passes 2-card test with HP-UX V3 (11.31)
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. This section lists the servers that have been tested to work successfully with Luna G5.

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-Fire-V245 Sparc	Works with 2 G5 HSMs on front USB ports with Solaris 10.
Dell R710 x86	Works with 2 G5 HSMs on front USB ports with Solaris 10/11.
SPARC-Enterprise-T5120	Works with 2 G5 HSMs on front USB ports with Solaris 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-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.
(187283) C_Finalize won't close socket	H	**Problem:** Either C_Initialize should not open a new socket, or C_Finalize should close the one opened by C_Initialize.. **Resolution:** Close client socket when finalizing..
(187281) Callback server failed to create a PED ID mapping with the error RC_FAILED_TO _CREATE_THREAD	H	**Problem:** [user bin]# ./pedClient -mode setid -id 3 -id_ip 172.20.10.217 -id_port 1503 Ped Client Version 2.0.0 (20000) Ped Client launched in "Set ID" mode. Callback Server is running.. SetID failed with result: 0xc0002000 RC_FAILED_TO_CREATE_THREAD "Set ID" command passed. The problem is due to thread resources (i.e. stack) being leaked. **Resolution:** Fixed – thread objects are affirmatively deleted once they have been terminated.
(187107) LunaProvider ECDH KeyAgreements for AES keys result in a 16 byte key when the convention should be 32 bytes	H	**Problem:** If a key agreement is set up between the LunaProvider and another Java JCA/JCE and attempts to agree on an AES key the LunaProvider will provide a 16 byte (128bit) AES key. The other provider will provide a 32 byte (256bit) AES key **Resolution:** The provider will now return the longest AES key possible from the key agreement shared secret, from the set of 16/24/32 byte keys. All DH key agreements will return 32 byte keys, since the minimum supported DH key size is 1024 bits. EC key agreements will vary depending on the curve: Curve size < 128 bits: error, too small to generate any AES key 128 bits <= curve size < 192 bits: 16 byte (128 bit) AES key 192 bits <= curve size < 256 bits: 24 byte (192 bit) AES key curve size >= 256 bits: 32 byte (256 bit) AES key Note: this is still not entirely compatible with the Bouncy Castle provider, since they seem to return an "AES key" of the same size as the shared secret. Their approach is not compliant to the AES standard.

Issue	Severity	Synopsis
(186542) The audit logger creates a new file every few seconds if the audit log rotation interval is set to **never** or **monthly**	H	**Problem:** If the audit log rotation interval is set to **never** or **monthly**, a new audit log is crested every few seconds, potentially filling the disk and degrading HSM performance. **Resolution:** Fixed time adjustment algorithm for monthly setting; removed support for yearly setting.
(186405) The **sysstat** daemon process is killed if the **lunash** shell used to restart the daemon is closed	M	**Problem:** If you login to a **lunash** session, restart the **sysstat** service, and then exit **lunash**, the **sysstat** service (**sysstatd**) is terminated. **Resolution:** Modified to detach the program from the console, and launch it as a UNIX daemon.
(186404) KSP cannot see slots that appear after an empty slot in the slot list	M	**Problem:** If you add an HA slot to an HSM that does not have a backup device, such as a Luna G5 attached, the HA slot is added after the empty UHD slots reserved for the backup device(s). When KSP encounters an empty slot, it assumes that all of the following slots are empty, and therefore does not find the HA slot. **Resolution:** Fixed the KSP toolchain (KSP/KspConfig/KspCmd) to enumerate slots properly despite slots with token not present.
(186022) SafeNet KSP aliases to refer Luna CSPs (changes made for Microsoft TMG) is not reflecting in Luna SA 5.2	H	**Problem:** After installing and registering CSP and KSP on Windows Server 2012, I found that registry entry for SafeNet Key Storage Provider doesn't register the aliases entry that was made during the Microsoft TMG support. **Resolution:** Value data of registry entry now holds: Aliases REG_MULTI_SZ Luna Cryptographic Services for Microsoft Windows Luna enhanced RSA and AES provider for Microsoft Windows Luna SChannel Cryptographic Services for Microsoft Windows
(185574) 32-bit CSP on 64-bit OS cannot find cryptoki.dll.	M	**Problem:** Attempting to run 32-bit CSP on a 64-bit OS fails because CSP cannot find **cryptoki.dll**. **Resolution:** Fixed in LunaClient installer.
(181030) LunaProvider: RSA-PSS should use non-zero default salt length	M	**Problem:** The Luna provider's RSA-PSS implementation uses a 0-byte salt if no parameters are given. This is a security hazard, since without a salt the PSS algorithm loses the randomness that makes it effective. RFC 4055 recommends using a salt no shorter than the hash length used in the signature. **Resolution:** The default hash used in the signature is SHA-1. The default salt has therefore been set to 20 bytes.
(144528) ECIES does not work	H	**Problem:** ECIES does not work in previous releases. **Resolution:** ECIES is supported in Luna HSM 5.2.
(129980) Documentation: WebHelp search does not match strings that include "_"	L	**Problem:** The WebHelp search function does not match strings that include the "_" (underscore) character. For example, searching for "C_GetFunctionList" will not return any hits, although "GetFunctionList" does. **Resolution:** Searching for terms that include the underscore character now returns all expected hits.

Luna SA Addressed Issues

Issue	Severity	Synopsis

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 5.2.4/5.2.5/5.2.6 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 5.2.6.
(LHSM-10553) Luna SA HSM Lockup	M	**Problem:** A communications issue between the Luna SA appliance software and the embedded K6 HSM may cause any connected Luna clients to appear to be operating normally, although they never complete commands and never time out. If this issue occurs on a Luna SA appliance which is a member of an HA group, the Luna client software does not remove the bad member from the HA group, since it is still able to communicate with the appliance. The only way to recover from this condition is to perform a manual reboot of the appliance. **Resolution:** The appliance software now includes a timeout when a communication issue with the embedded K6 HSM occurs. The 6.10.2 firmware includes several enhancements designed to minimize the chance of this issue occurring.

Issue	Severity	Synopsis

(LHSM-10158) Starting sshd failed after ssh regenKeyPair	H	**Problem:** After update of Luna SA to version 5.2.1 or 5.2.2 (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] lunash:>`
		
		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 5.2.3 update. Upload the update to your Luna SA and apply it immediately.

(MKS190033) HTL server hangs when network connection to client drops	H	**Problem:** The HTL server will hang if it is waiting for a message and the message is late. This is most noticeable when an HTL-connected client experiences a network outage and cannot send its sync beacon in time. Once the HTL server is hung, there is no way to restart it from Luna Shell since it requires a kill -9. **Resolution:** Relevant code adjusted for proper recursion.
(MKS186394) Luna SA doesn't prompt to change audit account password after **sysconf factoryreset**	M	**Problem:** After performing a factory reset of a Luna SA that has an audit account configured, the audit account is retained and the password is reset to the default. However, on first login following the factory reset, you are not prompted to change the password from the default. **Resolution:** Prompt fixed.
(MKS 164993) NTLS Crash and Burn	M	**Problem:** Under certain conditions, NTLS may fail with the following error: `crit  NTLS [14903]: info : 0 : NTLS CRASH AND BURN!` **Resolution:** This issue has been resolved in this release by adding the following fixes: • Buffers are now dynamically allocated if the buffer pool exhausts its resources. • The gethosbyname call has been replaced with a thread-safe version to prevent a NTLS crash when there are numerous client connections that use a DNS host name instead of an IP address.

Issue	Severity	Synopsis
(MKS153052) Typographical error changes meaning of HA log message	M	**Problem:** The word "not" is erroneously inserted into the following HA log message: Mon Feb 6 13:08:06 2012 : [6532] HA group: 2150841010 unable to reach member: 150576010. Manual Recover or Auto Recovery will **not** be able to recover this member **Resolution:** The log message has been corrected.

Luna PCI-E Addressed Issues

Issue	Severity	Synopsis
(140070) Multitoken utility has cosmetic bug in the notes section	L	**Problem:** "Multitoken2 mode rsasign" has been replaced with "multitoken2 mode rsasigver". Although tool works as expected, the notes section still says to run the tool with the old syntax (rsasign instead of rsasigver). **Resolution:** The notes section has been updated with the correct syntax.
(123776) HSM allows login as two different user types simultaneously	H	**Problem:** The HSM currently allows you to log in as both the CRYPTO_OFFICER and CRYPTO_USER (regular and limited users) simultaneously, in the same session. This leads to some confusion as to who is actually logged in, and may be counter to the PKCS11 spec. **Resolution:** Concurrent logins are no longer allowed.

Luna G5 Addressed Issues

Issue	Severity	Synopsis
(164212) Uninstallation does not complete successfully if the driver is in use	H	**Problem:** If you uninstall the Luna G5 software while the driver is in use (for example, if **lunacm** is running), the uninstallation completes with no error message, although it fails to remove the driver. Attempting to reinstall the software causes an error. **Resolution:** The driver is now uninstalled even if in use.
(135461) Firmware rollback command does not provide adequate warning	M	**Problem:** When you use the **hsm rollbackFW** command to roll back G5 HSM firmware, the user and all user objects are destroyed. The message presented by the **lunacm** utility, however, only warns that the HSM will be reset. It gives no indication that objects will be destroyed. **Resolution:** The message has been updated to include appropriate warnings.
(135295) The cklog201.dll.sig file is missing from Windows 64-bit builds	M	**Problem:** The **cklog201.dll.sig** file is missing on Windows 64-bit builds. This file is required to configure KSP with cklog. **Resolution:** This file is now included.
(99275) "haGroup haOnly -disable" not functional	M	**Problem:** With Luna G5s in High Availability Group you can run “haGroup haOnly –enable” to configure "HA Only" mode, but once “HAOnly” mode is established, lunacm does not allow disabling or exit from “HAOnly” mode. **Resolution:** You can now use lunacm to disable "HA Only" mode.
(95860) Luna G5 HA virtual slot not visible in lunacm	M	**Problem:** The Luna G5 virtual slot is not shown by the **show slot list** command in lunacm. The virtual slot ID can still be seen in lunadiag or in ckdemo. **Resolution:** The lunacm utility now displays a message informing the user that the HA slots will not be visible until the application is restarted.

Issue	Severity	Synopsis
(95016) lunacm can't clone objects from old firmware version (Key Migration Issue)	M	**Problem:** Cloning fails with - Error = 0x54 while getting OUID for object handle 6, slot 1. No objects were cloned. The problem is that firmware 4.x (the legacy token HSMs) does not support OUIDs, used by newer versions of lunacm and newer HSM firmware. Attempting to migrate keys from firmware 4 HSMs to firmware 6 HSMs (Luna G5, K6) with lunacm fails. **Resolution:** Cloning objects from firmware 4.x HSMs to firmware 6.x HSMs is now supported.
(80371) "hsm showinfo" doesn't show enough info if SRK is zeroized	L	**Problem:** When the G5's SRK is zeroized, not much can be done with it - and only certain information is query-able. "hsm showinfo" in this state quits almost immediately: lunacm:> hsm si HSM Label -> no label HSM Manufacturer -> Safenet, Inc. HSM Model -> G5 Base HSM Serial Number -> 655123 Token Flags -> CKF_RNG CKF_LOGIN_REQUIRED CKF_RESTORE_KEY_NOT_NEEDED CKF_PROTECTED_AUTHENTICATION_PATH Firmware Version -> 6.0.0 Command Result : 0x80000026 (CKR_MTK_ZEROIZED) lunacm:> "hsm si" should be modified to show all that it is allowed to when the HSM is in this state. **Resolution:** The lunacm messages have been corrected.
(80363) Can't regenerate SRK when Luna G5 is zeroized	L	**Problem:** In this case, if SRK generate is not permitted in the zeroized state, it should error out immediately with "srk_zeroized", and not present a PED prompt and then device error. lunacm:> srk generate Please attend to the PED. SRK failed to regenerate. Command Result : 0x30 (CKR_DEVICE_ERROR) **Resolution:** You can regenerate the SRK/MTK in any state.

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 HSM Known Issues" on page 19
- "Luna SA Known Issues" on page 22
- "Luna PCI-E Known Issues" on page 24
- "Luna G5 Known Issues" on page 26

Workarounds are provided where available.

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 HSM Known Issues

Issue	Severity	Synopsis
(LHSM-8414) Synchronization issue after performing a firmware update on Luna G5 or Luna PCI-E	H	**Problem:** After updating the firmware on a Luna G5 or Luna PCI-E HSM, the hardware and firmware are not synchronized. **Workaround:** After updating the firmware on a Luna G5 or Luna PCI-E HSM, you must use the lunacm **hsm reset** command to reset the HSM to synchronize the firmware with the hardware.
(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.
(LHSM-3319) Audit logging trace-ability of “who” is broken sometimes	H	**Problem:** Used a standard client (win64) registered to a single HSM with NO app Id settings, but the log messages are not properly bound to the access ID, so there is no traceability to the “who”. **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).

Issue	Severity	Synopsis
(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.
(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.
(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). **Workaround:** None.
(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. **Workaround:** Use one of the following methods to add **LunaAPI.dll** to the Java 7 search path: • Put **LunaAPI.dll** in an arbitrary folder and add that folder to the system path. Java 7 will search the system path for **LunaAPI.dll.** • Put **LunaAPI.dll** in the Windows system folder. This folder varies by operating system and DLL type, as follows: - 32-bit Windows: **C:\Windows\System32** **-** 64-bit Windows, 64-bit LunaAPI.dll: **C:\Windows\System32** **-** 64-bit Windows, 32-bit LunaAPI.dll: **C:\Windows\SysWOW64**
(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.
(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 may 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.

Issue	Severity	Synopsis
(182201) JCPROV HALogin API does not work	M	**Problem:** The JCPROV HALogin API does not work. **Workaround:** None.
(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. **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.
(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 may 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.

Issue	Severity	Synopsis
(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.
(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
(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

Issue	Severity	Synopsis
(LHSM-3332, 3333) HTL feature and disabling of ip checking are not compatible	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 may be displayed: **EncryptInit() using PE1746 failed, disabling PE1746.: Cannot allocate memory** You can ignore this message. **Workaround:** None.
(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** 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 may 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.
(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. **Workaround:** None. This error message can be ignored.
(161085) Deleting HA group does not delete HA entries in client configuration file	M	**Problem:** Deleting the HA group does not delete HA entries in the client configuration file. **Workaround:** None.
(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
(187108) Slot 1 driver crash on HP DL 380P Gen8 with RHEL 6.2 x64	H	**Problem:** A driver crash may occur for a Luna PCI-E card inserted into slot 1 on an HP DL 380P Gen8 server running RHEL 6.2 x64. The crash was observed after about 6 or 7 HSM resets, when you running a multitoken script which resets the HSM and performs a multitoken operation in a loop. **Workaround:** Do not use slot 1 on an HP DL 380P Gen8 server running RHEL 6.2 x64.
(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.

(182827) HA autorecovery does not work	H	**Problem:** If you enable HA autorecovery on Luna G5, members of the HA group that go down may 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.

Documentation Addendums

This section addresses errors or omissions in the documentation.

Lunacm and lunash audit config command

The documentation indicates that the **audit config** command allows you specify that the audit logs can be rotated on a yearly basis. This is incorrect.

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.	
Technical Support Customer Portal	https://serviceportal.safenet-inc.com Existing customers with a Technical Support Customer Portal account can log in to manage incidents, get the latest software upgrades, and access the SafeNet Knowledge Base.	

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.